جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY
Amman - Jordan

الحماية الجزائية للبيانات الشخصية في التشريع الأردني (دراسة مقارنة)

Penal Protection for Personal Data in Jordanian Legislation (A Comparative Study)

إعداد

عبد السلام أحمد خلف العرمان

إشراف

الأستاذ الدكتور أحمد محمد اللوزي

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير
في القانون العام

قسم القانون العام

كلية الحقوق

جامعة الشرق الأوسط

تشرين الثاني، 2022

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرٗا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡمٞۖ وَلَا تَجَسَّسُواْ وَلَا يَغۡتَب بَّعۡضُكُم بَعۡضًاۚ أَيُحِبُّ أَحَدُكُمۡ أَن يَأۡكُلَ لَحۡمَ أَخِيهِ مَيۡتٗا فَكَرِهۡتُمُوهُۚ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ تَوَّابٞ رَّحِيمٞ ١٢ ﴾

[سورة الحُـجُـرات, ١٢]

تفويض

أنا **عبد السلام أحمد خلف العرمان**، أفوّض جامعة الشرق الأوسط بتزويد نسخٍ من رسالتي ورقياً وإلكترونياً للمكتبات أو المنظمات أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: عبد السلام أحمد خلف العرمان.

التاريخ: 19 / 11 / 2022.

التوقيع: 

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها: "الحماية الجزائية للبيانات الشخصية في التشريع الأردني".

وأجيزت بتاريخ : يوم السبت الموافق 19 / 11 / 2022 م

للباحث: عبد السلام أحمد خلف العرمان.

أعضاء لجنة المناقشة

الاسم	الصفة	المكان	التوقيع
أ.د أحمد محمد اللـــــوزي	المشرف	جامعة الشرق الأوسط	.....
د. محمد علي الشباطـــــات	رئيس اللجنة	جامعة الشرق الأوسط	.....
د. منذر عبدالرزاق العمايرة	العضو الداخلي	جامعة الشرق الأوسط	.....
أ.د. صالح أحمد حجـــــازي	العضو الخارجي	جامعة عمان الأهليـــة	.....

شكر وتقدير

أشكر **الله عز وجل** أولاً، ثم أشكر الأستاذ المشرف على البحث؛ لما قدَّمه لي من دعم **أ. د. أحمد محمد اللوزي** الذي لم يألُ جهدًا في مدِّ يد العون والمساعدة؛ لِتخرج هذه الأُطروحة للنور.

كما أتقدم بجزيل الشكر إلى **أعضاء لجنة المناقشة** بقبولهم مناقشة رسالتي؛ فهم أهل لتدارك النقص والخلل فيها.

وأتوجَّه بخالص الشكر إلى **جميع أعضاء هيئة التدريس في كلية الحقوق في جامعة الشرق الأوسط** الذين استفدتُ من علمهم.

الباحث

عبدالسلام أحمد خلف العرمان

الإهداء

إلى من أحمل اسمه بكل فخر...إلى من يرتعش قلبي لذكره...إلى من أرجو الله يسكنه فسيح جناته ...**والدي الحبيب**

إلى رمز الحب ...وبلسم الشفاء

والدتي العزيزة

إلى القلوب الطاهرة والرقيقة

أخواتي

إلى من هم أقرب إلى من روحي

إخواني

إلى رفيقة روحي

زوجتي

إلى زينة حياتي وبهجتها

أولادي

إلى من لم يتوانوا في مدِّ يد العون لي **أساتذتي الكرام**

أهدي هذه الرسالة

فهرس المحتويات

الموضوع **الصفحة**

الفصل الأول: الإطار النظري للدراسة

الفصل الثاني: ماهية البيانات الشخصية

الفصل الثالث: النموذج القانوني لمعالجة البيانات الشخصية

الفصل الرابع: الحماية الجزائية للبيانات الشخصية

الفصل الخامس: الخاتمة، النتائج، التوصيات

الحماية الجزائية للبيانات الشخصية في التشريع الأردني (دراسة مقارنة)

إعداد: عبد السلام أحمد خلف العرمان

إشراف: الأستاذ الدكتور أحمد محمد اللوزي

الملخَّص

تناولت هذه الدراسة موضوع الحماية الجزائية للبيانات الشخصية في التشريع الأردني، وذلك من خلال بيان ماهية هذه البيانات، والآثار التي تترتَّب على معالجتها، وحمايتها ضمن نطاق الحق في الخصوصية، والأساس القانوني لانعقاد المسؤولية الجزائية في حال انتهاكها، فتطرقت الدراسة لماهية المعالجة، وضوابطها وحقوق الشخص المعني بالمعالجة، والتزامات المسؤول عن المعالجة، بالإضافة إلى ذكر أشكال أو صور الجرائم التي تقع عليها، والحماية الجزائية المقررة لها، وذلك من خلال استخدام الباحث المنهج الوصفي التحليلي بالإضافة إلى المنهج المقارن، وذلك من خلال التطرق لبعض التشريعات المقارنة.

وفي النهاية، توصَّل الباحث من خلال هذه الدراسة إلى بعض النتائج والتوصيات التي يوصي بها، يوصي الباحث المشرِّع الأردني بضرورة توفير حماية لهذه البيانات في ظل التطورات التقنية المتزايدة، والتي تهدِّد أمن وسرية الأفراد في حال تم انتهاكها، فالطرق التي يتم بها الاعتداء عليها عديدة، وذلك يرجع إلى التقدم التقني الذي ساهم في ظهور العديد من الأساليب الجُرمية، وبالتالي يوصي الباحث المشرِّع الأردني بضرورة تعديل مسودَة القانون الخاصة بحماية البيانات الشخصية لتوفير حماية اكبر، وذلك من خلال إعادة النظر بتشكيلة مجلس حماية البيانات الشخصية، بأن يتم اختيار رئيس المجلس بطريق الانتخاب، وأن لا يتكون المجلس من السلطة التنفيذية، فمن المعلوم أن السلطة التنفيذية هي المسؤولة عن معالجة البيانات الشخصية، فلا يعقل أن تكون الجهة المعالجة هي ذات الجهة التي تراقب وتحمي البيانات، والإسراع بإصدارها أُسوةً بباقي الدول، فضلاً عن جملة من التوصيات ذيَّلها الباحث في الفصل الأخير من هذه الدراسة.

الكلمات المفتاحية: البيانات الشخصية، الحماية الجزائية، معالجة البيانات.

Penal protection for personal data in Jordanian legislation

(A comparative study)

Prepared by: Abdul Salam Ahmed Khalaf Al -Arman

Supervision: Prof. Dr. Ahmed Mohamed Al –Lawzi

Abstract

This study to shed light on Penal protection for personal data in Jordanian law by showing the nature of the data and the effects of processing it and also protecting with in right of privacy at the legal basis of establishing penal responsibility in case of violation.

Its controls, the rights of the person concerned with the treatment, the obligations of the person responsible for the treatment, in addition to mentioning the forms or forms of crimes that fall on it, and the penal protection prescribed for them, through the use of the researcher descriptive analytical approach in addition to the comparative approach, by addressing some comparative legislation.

The study also shed a light on the nature of handling (processing) and its restriction and the rights commitments of the responsible person. It also shed a light on the forms and pictures of the crimes that falls on it and the penal protection for it by using the descriptive analytic approach al comparative approach, Finally, the researcher got some results and recommendations.

The necessity putting greater data protection specially because of the speed of technical developments that threatens the security and the privacy of families in case of violation and that also created different penal ways and methods>

Amending the law of personal data employing an elected president (manager) and forming a committee for personal data protection without having an executive authority which will be responsible for watching and protecting data.

Issuing this law as soon as possible following the countries that seriously protect personal data and secure it and I also wrote some other recommendations in the last chapter of this study.

Keywords: personal data, penal protection, data processing.

الفصل الأول
الإطار النظري للدراسة

أولاً: مقدمة الدراسة

إن حماية البيانات الشخصية حقٌّ من حقوق الأفراد، التي ترتبط ارتباطاً وثيقاً في الحياة الخاصة للفرد واحترام حدوده الشخصية، التي يجب أن يكتنفها الكتمان والسرية وعدم إتاحتها للجمهور، كونها تكرِّس مبدأً من المبادئ التي حثَّت عليها الشريعة الإسلامية وهي احترام آدميته وكرامته، وعدم التطفل على حياته الخاصة، فضلاً عن الخصوصية التي حثَّت عليها أغلب الدول في دساتيرها، ونظَّمت حماية قانونية لها [1]، فحق الفرد في احترام سرية بياناته الشخصية وتوفير الحماية القانونية التي تضمن حمايتها –ضمن إطار قانوني جزائي شامل متكامل يوائم معطياتِ العصر– أَلا وهي التكنولوجيا التي أصبحت تهدِّد البياناتِ الشخصيةَ للأفراد، فمن هنا تأتي أهمية الحماية الجزائية للبيانات الشخصية؛ وذلك لأن خصوصية وسرية بيانات المرء أصبحت مرتعاً سهلاً يقتحمه الآخرون ذوو الأفعال الجُرمِية التي تنال منها؛ وذلك لعدم وجود عائق يحول دون هذه الاعتداءات، وعدم توفير الحماية الكافية لهذه البيانات في ظل التطورات التقنية وظل التطبيقات الذكية والمواقع الإلكترونية التي تزداد يوما بعد يوم، والتي وفَّرت بيئة خصبة لارتكاب جميع الأفعال التي تنال من أمن واستقرار الأفراد، وزعزعة أمنهم من خلال العبث في بياناتهم ذات الطابع الشخصي.

فمعظم الدول نظمت حماية خاصة للبيانات الشخصية؛ منها الاتحاد الأوربي الذي طبَّق اللائحة الأوروبية لحماية البيانات الخاصة بالأشخاص الطبيعيين في 25 مايو 2018 على جميع الدول الأعضاء في الاتحاد الأوروبي، بالإضافة الى قانون حماية البيانات الشخصية لمملكة البحرين رقم

---

(1) محمد، محمود عبد الرحمن، نطاق الحق في الحياة الخاصة دراسة مقارنة، دار النهضة العربية، القاهرة، ص5.

(30) لسنة 2018، وقانون رقم 45 لسنة 2021 الخاص بحماية البيانات الشخصية لدولة الإمارات، وفي ظل حداثة موضوع البحث وظهور العديد من التجاوزات غير المشروعة على بيانات المرء ستتمحور الدراسة حول الحماية الجزائية للبيانات الشخصية في التشريع الأردني.

ثانياً: مشكلة الدراسة

تكمن مشكلة الدراسة في مدى توفير نظام قانوني لحماية بيانات الأفراد الشخصية من عدمه في التشريع الجزائي الأردني في ظل التطورات المتزايدة لاستخدامات المواقع الإلكترونية والتطبيقات الذكية، التي لا يمكن ولوج أيٍّ منها دون التعرف على الهُوية الشخصية، وأخذ جميع المعلومات التي تتعلق بشخص الفرد ومدى مسؤولية الشخص المسؤول عن إدارة وإدخال ومعالجة هذه البيانات، ومدى مسؤولية الدولة في توفير الحماية الجزائية للبيانات ذات الطابع الشخصي، التي تُعدُّ حقًّا من حقوق الأفراد؛ بأن تبقى بعيدةً عن الأفعال المشبوهة، بالإضافة إلى أن مسالة وضع إطار قانوني لمعالجة البيانات الشخصية تتضمَّن عدة مشكلات يجب أن يتناولها أيٌّ تنظيم قانوني، وبناءً على ما تقدَّم فمشكلة الدراسة تتمحور حول وجود تنظيم قانوني لحماية البيانات الشخصية من عدمه في التشريع الأردني.

ثالثاً: أهداف الدراسة

1. توضيح ماهية البيانات الشخصية.
2. بيان حقوق الأفراد لحماية بياناتهم الشخصية، وبيان الالتزامات التي تقع على عاتق الشخص المسؤول عن معالجة البيانات الشخصية.
3. بيان المبادئ العامة التي ترد على معالجة البيانات الشخصية.
4. بيان صور الجرائم التي تقع على البيانات الشخصية.

5. بيان العقوبات الجزائية المترتبة على الشخص المسؤول في المعالجة، في حال أخَّل بالتزاماته في حماية البيانات الشخصية.
6. بيان التنظيمات القانونية في تشريعات بعض الدول؛ لغرض المُقارنة.

رابعاً: أهمية الدراسة

حماية البيانات الشخصية هي أساسٌ لحماية الأفراد، وبناءً على ما تقدَّم فإن أهمية الدراسة تكمن في نقطتين جوهريتين:

الأولى: توضيح المقصود بالبيانات الشخصية؛ لتمييزها عن غيرها من البيانات التي تخرج عن نطاق كونها شخصية، وذكر ماهي تلك البيانات والتفريق بينها وبين الحق في الخصوصية، من خلال عرض النصوص القانونية الخاصة فيها.

الثانية: وهي تحليل النصوص القانونية المتعلِّقة بالبيانات الشخصية، والبحث في مدى الحماية الجزائية في التشريع الأردني للبيانات الشخصية، بالإضافة إلى التطرُّق لخطة بعض الدول لحماية البيانات ذات الطابع الشخصي؛ للاستفادة منها لسدِّ النقص التشريعي في الحماية الجزائية للبيانات، من خلال المقارنة بينها وبين التشريع الأردني.

خامساً: أسئلة الدراسة

1. مدى مشروعية معالجة البيانات الشخصية؟
2. هل للشخص الذي تتم معالجة بياناته الشخصية حقوق ترد على هذه البيانات؛ يمارسها في مواجهة الشخص الذي يقوم بالمعالجة وماهي التزامات المعالج؟
3. إذا حدث وخرق المسؤول عن معالجة بيانات الأفراد الالتزامات التي تقع على عاتقه ماهي العقوبات التي تترتَّب عليه؟

4. ماهي أشكال الاعتداءات التي تقع على البيانات الشخصية؟

5. هل يوجد تشريع في القانون الأردني يكفل حماية البيانات الشخصية؟

سادساً: حدود الدراسة

1- الحدود الموضوعية: إن هذه الدراسة تقتصر على توضيح البيانات الشخصية للأفراد من خلال بيان ماهيتها وطبيعتها، وحقوق الأفراد في حماية بياناتهم الشخصية، والتزامات الشخص المعني بمعالجة البيانات، والجزاء المترتِّب على إخلاله بتلك الالتزامات، والحماية الجزائية لتلك البيانات، والتنظيم القانوني لها في بعض التشريعات المقارنة.

2- الحدود المكانية: الأصل في الدراسة أنها ستتناول التنظيم الجزائي لحماية البيانات الشخصية في التشريع الأردني.

3- الحدود الزمانية: قانون العقوبات الأردني واخر تعديلاته، مسوَّدة حماية البيانات الشخصية الأردنية لسنة 2016، قانون حماية البيانات الشخصية لمملكة البحرين لسنة 2018، قانون حماية البيانات الشخصية لدولة الإمارات رقم 45 لسنة 2021.

سابعاً: مصطلحات الدراسة

- **البيانات:** هي "معلومات تفصيلية حول شخص أو شيء ما يمكن من خلالها الاستدلال عليه[1]".

(1) https://ontology.birzeit.edu/term (on-line) available: تمت الزيارة الساعة الرابعة عصرا تاريخ 2022/5/1

- **البيانات الشخصية:** هي "كلُّ معلومة تتعلَّق بشخص طبيعي معين أو يمكن تعيينه بصورة مباشرة أو غير مباشرة؛ عن طريق الرجوع إلى رقم الهوية، أو إلى واحد أو أكثر من العناصر المميِّزة له[1]".
- **الشبكة المعلوماتية:** هي "شبكة الاتصالات العالمية التي تربط الملايين من الحاسبات بعضها ببعض، إما عن طريق خطوط الهواتف، أو عن طريق الأقمار الصناعية التي يستخدمها مستخدمو الحواسيب حالياً على مدار الساعة في معظم أنحاء العالم، وخاصة في الجامعات، ومعاهد البحث العلمي والشركات الكبرى، والبنوك والمؤسسات الحكومية"[2].
- **الحق في الخصوصية:** هو " الحق الذي يكون للأفراد والجماعات والهيئات والمؤسسات متى وكيف وبأيِّ قدرٍ يمكن إيصال المعلومات الخاصة بهم إلى غيرهم"[3].
- **الحماية الجزائية:**" مجموعة الأحكام أو بالأحرى القواعد القانونية الجنائية الموضوعية والإجرائية التي يتوسَّل بها المشرِّع؛ لوقاية شخصٍ أو مالٍ أو مصلحة معينة بوجهٍ عامٍ، ضدَّ المساس الفعلي أو المحتمل، ولفرض جزاءٍ جنائيٍّ على من يخالف ذلك، أو جزاءٍ إجرائيٍّ على العمل الإجرائي الذي على هذا الأساس، أو إذا اتصل بهذا المساس بشكل أو بآخر[4]".

---

(1) جابر، أشرف (2015)، استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصية، مجلة العلوم الإنسانية جامعة الاخوة منتوري، الجزائر :available (on-line) :استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصيةavailable (mandumah.com) تمت الزيارة الساعة الرابعة عصرا تاريخ 2022/5/1

(2) الخلايلة، عايد رجا (2011)، المسؤولية التقصيرية الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع الطبعة الثانية، ص 49.

(3) محمد، محمود عبد الرحمن، نطاق الحق في الحياة الخاصة، مرجع سابق، ص 107.

(4) العادلي، محمود صالح (2006). الحماية الجنائية لأسرار المحامي للمحافظة على أسرار موكليه، دراسة مقارنة، الإسكندرية دار الفكر الجامعي ص 8.

ثامناً: الإطار النظري والدراسات السابقة

أ: الإطار النظري للدراسة

لقد تم تقسيم هذا البحث إلى:

الفصل الأول: ويتضمَّن الإطار العام للدراسة محلِّ البحث؛ حيثُ سيقوم الباحث ببيان أهداف الدراسة، وأهميتها، وإشكاليات الدراسة، والمنهجية المتَّبعة في الدراسة، وحدود الدراسة الموضوعية المكانية والزمانية، وأهمّ المصطلحات وأيضا الدراسات السابقة، وما يُميِّز هذه الدراسة عن غيرها، وأقسام فصول الدراسة.

الفصل الثاني: سيتمحور هذا الفصل حول ماهية البيانات الشخصية من حيثُ مفهومُها وصورُها وطبيعتُها، ومدى حمايتها ضمن نطاق الحق في الخصوصية.

الفصل الثالث: يرتكز هذا الفصل على ماهية معالجة البيانات الشخصية، ومدى مشروعية معالجة البيانات الشخصية والقيود التي ترد على معالجتها، والآثار المترتبة على المعالجة من حقوق والتزامات، تحت عنوان النموذج القانوني لمعالجة البيانات الشخصية.

الفصل الرابع: يتناول الباحث فيه أساس الحماية، وانعقاد المسؤولية الجزائية في التشريع الأردني والتشريع المقارِن.

الفصل الخامس: يتناول الباحث فيه الخاتمة وما توصَّل إليه من نتائج الدراسة، مع تقديم أهم التوصيات.

ب. الدراسات السابقة ذات الصلة

فيما يلي الدراسات ذات الصلة في موضوع الدراسة:

1- **السكر، سلطان فياض محمد (2022)**، جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني، جامعة الشرق الأوسط.

تناولت هذه الدراسة جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني وتوصلت الدراسة الى عدة نتائج ان النصوص التي تعالجها نصوص عامة وان ملاحقة جريمة انتهاك سرية المعلومات تتصل بالصعوبة لأنها جريمة تقنية لا تتصل بالواقع المادي وأوصت الدراسة بضرورة تعديل قانون الجرائم الإلكترونية رقم 27 لسنة 2015 من خلال إيجاد نصوص قانونية واضحة لمعالم جريمة انتهاك سرية المعلومات عبر الوسائط الإلكترونية، واتبعت الدراسة المنهج الوصفي التحليلي، وقد استفاد الباحث من الدراسة في مبحث الحق في الخصوصية، وما يميز الدراسة محلُّ البحث انها تناولت موضوع الحماية الجزائية للبيانات الشخصية.

2- **التهامي، سامح عبد الواحد**، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية.

هذه الدراسة تناولت القيود أو الضوابط التي تخضع لها البيانات عند المعالجة، حيث اتبعت المنهج المقارن بين التشريع الفرنسي والكويتي، وتوصلت الدراسة إلى عدة نتائج أهمها وضع عقوبة جنائية في حال مخالفة معالج البيانات لالتزامه بتأمين البيانات الشخصية أثناء المعالجة، أما الدراسة محلُّ البحث فتناولت الحماية الجزائية للبيانات الشخصية في التشريع الأردني، وقد استفاد الباحث منها في بعض الأمور التي تخص معالجة البيانات الشخصية.

3- **شقير، يحيى (2012)**. مدى توافق قانون ضمان حق الحصول على المعلومات في الأردن مع المعايير الدولية، جامعة الشرق الأوسط.

إن هذه الدراسة تتحدث عن قانون ضمان حق الحصول على المعلومات، ومقارنته مع المعايير الدولية، بينما الموضوع محلُّ الدراسة فتناول البيانات الشخصية؛ من حيثُ حمايتُها جزائياً في التشريع الأردني.

تاسعاً: منهجية الدراسة

ستتبع هذه الدراسة المنهج الوصفي والتحليلي لبيان أهمية الحماية الجزائية للبيانات الشخصية، بالإضافة إلى اتباع المنهج المقارن؛ من خلال الحديث عن المنظومة القانونية للحماية الجزائية للبيانات الشخصية، لبعض التشريعات المقارنة.

الفصل الثاني
ماهية البيانات الشخصية

أثارت مشكلة حماية البيانات الشخصية مؤخرا قلقاً بين أفراد المجتمع والمشرِّعين والقانونيين؛ وذلك لكثرة استخدامها في الفضاء الإلكتروني، وازدادت إشكالية حمايتها مع جهل المستخدِم للمواقع والتطبيقات الإلكترونية، التي لا يمكن دخول أيٍّ منها دون التعرف على هُوية المستخدِم، وأخذ معلوماته الشخصية، حيث تنحدر أهمية حماية البيانات الشخصية في كونها لم تقتصر على الاسم والصورة؛ بل تخطَّت ذلك واشتملت على بياناتٍ حيويةً للمستخدِمين؛ كبصمة العين والوجه والإصبع، بالإضافة إلى الموقع الجغرافي والعديد من المعلومات الحساسة [1].

فالعالم الرقميُّ ساهم بشكل واضح في تآكل الخصوصية فيما يخصُّ البياناتِ الشخصيةَ للأفراد؛ وذلك يرجع إلى كون الحواسيب أصبحت بمثابة بنوك للمعلومات والبيانات، وذلك بسبب الإقبال الكبير والمتزايد من قبل الهيئات والشركات والأفراد نحو تبادل وتخزين ونشر البيانات عبر الفضاء الإلكتروني، الذي أصبح يحوي العديد من الأسرار والخصوصيات التي تخصُّ الأفراد والشركاتِ والبنوك؛ وذلك بسب الاعتماد على الفضاء الإلكتروني في شتى مجالات الحياة، ويرجع ذلك الاعتماد؛ لسهولة نقل وتبادل ونسخ واسترجاع وتخزين أعدادٍ هائلةٍ من البيانات [2].

---

(1) شمس الدين، أشرف توفيق (2007). الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية، دار النهضة العربية، بحث منشور، ط2، ص61.

(2) عثمان، طارق (2007). الحماية الجنائية للحياة الخاصة عبر الانترنت، دراسة مقارنة، كلية الحقوق، جامعة محمد خيضر، ص 81. تمت زيارة الموقع الساعة 2 بتاريخ 8/ 5/2022، https://boubidi.blogspot.com/: on- available (line)

إن نقل البيانات وتبادلها عبر شبكات الإنترنت يكون من خلال عنوان بروتوكول الإنترنت (Internet Protocol)، و" هو عنوان رقمي منطقي يتم تعيينه لكل كمبيوتر، أو طابعة، أو محمول، أو جهاز توجيه، أو أي جهاز آخر يشكل جزءًا من شبكةTCP / IP ، ويُعدُّ عنوان IP المكوِّن الأساسي الذي بُنيِت عليه بُنية الشبكات؛ حيث لا توجد شبكة إنترنت دون عنوان IP، وهو عنوان يُستخدم لتعريف كل عقدة في الشبكة بشكل فريد، ويربط شبكة الإنترنت العالمية ببعضها البعض مهمّته هي تحديد عنوان للأجهزة المذكورة؛ لتتمكّن من التواصل مع الأجهزة الأخرى في شبكةIP ، ويحمل كلّ جهاز عنوان IP مختلف عن غيره من الأجهزة، وبمعنى آخر يمكن القول بأنّه مماثل لعنوان الشارع أو رقم الهاتف؛ حيث يُستخدم لتمييزه عن غيره من الأجهزة [1]".

إن المخاوف تزداد مع ازدياد أعداد المستخدمين للمواقع الإلكترونية والتطبيقات الذكية ومواقع التواصل الاجتماعي، بالإضافة إلى الاستخدام غير الواعي لها، فالعالم الرقمي يكشف ويُعرّي الحياة الخاصة للأفراد، كما أنه بيئة خصبة للانتهاكات التي تمسُّ الخصوصية، فالأمر لم يعد يقتصر على بيانات شخصية؛ كالاسم والموطن، بل تعدَّى إلى بصمات الشخص؛ كبصمة الإصبع والوجه والعين وبصمة الصوت، وتسمى بالبيانات البيرمترية، وهي التي تستطيع تحديد هُوية المستخدِم بطريقة تقنية فنية من خلال تحويل سمة من سمات الشخص إلى بصمة رقمية تستطيع من خلالها إثبات انفراد الشخص بمظاهر غير قابلة للتغيير ذاتية على جسده [2].

---

(1) https://mawdoo3.com/ (on– line)available: تمت زيارة الموقع الساعة الخامسة تاريخ 2022/5/15

(2) المعداوي، محمد احمد، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص1944: https://search.mandumah.com/. –available(on– line) تمت زيارة الموقع الساعة 11 صباحا، تاريخ 6/ 2022/6.

فحماية البيانات ذات الطابع الشخصي في غاية الأهمية؛ كونها تحقق مبدأ الشرعية التي تقوم عليها الدولة القانونية، ومن هذا المنطلق فإنه يتوجّب على الدولة أن تكفل حق حماية البيانات الشخصية باعتبار أي تعدِّي عليها هو تعدِّي على حياة الأفراد الخاصة.

لا سيما أنها أصبحت في الوقت الحالي بضاعة العصر المتاحة، ولذلك أصبحت قواعد البيانات تمثِّل قطاعًا مهمًّا، وذات أهمية كبرى في الاقتصاد[1]،وذلك يرجع إلى أنَّ حجم مستخدمي موقع فيس بوك يتجاوز المليارين شخص، وتطبيق إنستقرام يصل عدد المستخدمين 800 مليون تقريبا، وتطبيق واتساب أكثر من مليار، فهذه التطبيقات أصبحت مصدرًا من مصادر إنتاج البيانات، فالناظر للتطبيقات والمواقع الإلكترونية يفسِّر سبب اتجاه الشركات الكبرى؛ لاستثمار تلك البيانات[2]؛كما ظهر ما يسمَّى ببنوك المعلومات – التي ظهرت بالتزامن مع انتشار التكنولوجيا – والتي مُهمَّتها إنشاء قاعدة بيانات تختصُّ في موضوع معين ولغرض محدَّد، ومن ثم معالجتها عبر أجهزة الحاسب الآلي، ويتمُّ إخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة، فالحاسب يقوم بجمع البيانات وتخزينها وبعد ذلك يقوم بمعالجتها ونشرها، فيصبح الفرد أسيرًا للمعلومات التي تمَّ جمعها[3]؛ لأن الانتهاكات أو ما يسمى بالجرائم الإلكترونية أو الإنترنت أو جرائم السيبر[4]، التي قد تقع عليها

---

(1) بوعمرة، آسيا، الحماية المزدوجة لقواعد البيانات، المجلة الجزائرية للعلوم القانونية، بحث منشور، ص248: available.https://www.asjp.cerist.dz/en/article/ (on– line) تمت زيارة الموقع الساعة 4 مساء تاريخ 2022/6/10.

(2) الأشقر، د. منى جبور، الجبور، د. محمود، 2018، البيانات الشخصية والقوانين العربية، مرجع سابق، ص12، available (on– line) .pdf (archive.org) الساعة 11 مساءً تاريخ 2022/7/14.

(3) لامي، بارق منتظر عبد الوهاب، (2017)، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ص 20.

(4) عمر، رشاد خالد، (2013)، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليله مقارنة، المكتب الجامعي الحديث، ص 18.

عديدة؛ كاختراقها والاطلاع عليها دون علم صاحبها، فتلك الأفعال عامل تهديد لحياة الشخص الخاصة.

وبناءً عليه فلا بدَّ من التطرق إلى طبيعة البيانات الشخصية، وتوضيح مفهومها والتعريف بها؛ لتمييزها عن غيرها من البيانات، وذلك لنتمكن من إسقاط صفة الشخصية عليها، وعليه سيتناول هذا الفصل الحديث عن مفهومها والفرق بينها وبين المعلومات وطبيعتها، وذلك ضمن المبحث الأول، ويتصل الحديث عن هذه البيانات حيث إنه يجب التطرق لموضوع مدى نطاق حماية البيانات الشخصية ضمن الحق في الخصوصية أو بمعنى آخر: هل الحق في حماية البيانات الشخصية حقٌّ مستقِلٌّ عن الحق في الخصوصية أم لا؟ وذلك ضمن المبحث الثاني.

المبحث الأول: مفهوم البيانات الشخصية.

المبحث الثاني: نطاق حماية البيانات الشخصية (الحق في الخصوصية).

المبحث الأول
مفهوم البيانات الشخصية

إن تمييز أو اعتبار البيانات شخصية أم لا، هو إذا كان بإمكانها أن تحدِّد هُوية الشخص من عدمه، فكلُّ بيان يكشف عن شخص المستخدِم يعتبر بياناً ذا طابع شخصي، أو بإمكانه أن يكشف عن هُويته، وبناءً على ما تقدم فإن أيًّا من البيانات التي يتمُّ استخدامها في إحدى المواقع الالكترونية، أو خدمات الإنترنت فهي تُعدُّ بياناتٍ ذاتَ طابع شخصي، فعلى سبيل المثال مستخدمو موقع (فيس بوك) يلزم للتسجيل فيه الاسم واسم العائلة والبريد الالكتروني ونوع الجنس وكلمة المرور، وذلك ينطبق على أغلب التطبيقات الذكية وأغلب المواقع الالكترونية، وكما قد تتطلب بعض المواقع إضافة معلومات حساسة وأكثر خصوصية؛ كالعقيدة الدينية والأفكار السياسية [1].

فلا بدَّ من أن تبقى هذه البيانات سرية لا يطَّلع عليها أحد إلا بإذن صاحبها، فالبيانات التي تتصل بشخص صاحبها يجب أن تكتنفها السرية بحيث لا يُسمح اختراقها والاطلاع عليها؛ لأن من حق أصاحبها أن تُحفظ، وتبقى بعيدة عن أي سلوكيات تُسيء لأصحابها بالاطلاع عليها.

فالأصل أن الشخص ذاته هو من يقوم بالإفصاح عن بياناته، أو معلوماته التي يُعرف بها عن نفسه، أو من خلال الهيئات في الدولة التي تتوصل إليها بطريقة أو بأخرى، لذا فإن حمايتها تُصبح واجبًا وضرورةً قصوى في حال تمَّ نشرها دون أخذ إذن صاحب الشأن أو إذا أُفشيَت دون موافقته[2].

إن أهمية حمايتها تكمن بكون أي اعتداء عليها سيتم ببيئة من الصعوبة إثبات الشخص المعتدي، وسهولة إخفاء معالم الأفعال السلبية التي تتم في فضاء تقني من الصعب فيه تتبُّع المرتكِب للجريمة،

---

(1) جابر، أشرف، استهداف مستخدمي الانترنت بالإعلانات التجارية وحماية الحق في الخصوصية، مرجع سابق، ص 18:available (on-line) تمت زيارة الموقع الساعة 9 مساءً تاريخ 2022/7/15.

(2) الشوابكة، محمد أمين، (2011)، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، ص71.

وكما أن كشف معالمها يتطلب قدراً من المعرفة بالتقنيات والعالم الرقمي، وكما أن الشخص الذي قد يعتدي على هذه المعلومات هو شخص غير عادي، وشخص على قدر عالٍ من الذكاء والمعرفة التقنية. [1]

فالأفعال غير المشروعة عبر التقنيات الحديثة نتيجة أي تقدُّم تقني وعلمي، فالتطور جعل من الفضاء الإلكتروني مرتعا للتخطيط الجرمي بعيداً عن رقابة الجهات الأمنية. [2]

وسيتم تقسيم المبحث إلى ثلاثة مطالب، هي:

المطلب الأول: مفهوم البيانات الشخصية.

المطلب الثاني: الفرق بين المعلومات والبيانات.

المطلب الثالث: طبيعة البيانات الشخصية.

المطلب الأول
مفهوم البيانات الشخصية

لا بدَّ من الإحاطة بتعريف البيانات ذات الطابع الشخصي، من خلال الاطلاع على تعريفها ضمن المشرِّع الأردني والتشريعات المقارنة، والخروج بتعريف شامل لها، فالمشرِّع الأردني عرَّف البيانات بشكل عام في قانون الجرائم الإلكترونية في نص المادة الثانية منه على النحو الآتي: "البيانات: هي الأرقام أو الحروف أو الرموز أو الأشكال أو الأصوات أو الصور أو الرسومات التي ليس لها دلالة بذاتها".

---

(1) عبد الله، عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، ص32.

(2) السكر، سلطان فياض محمد، (2022)، جريمة انتهاك سرية المعلومات عبر الوسائل الالكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط كلية الحقوق، ص 19.

كما ان المشرع الأردني عرَّفها في مشروع قانون حماية البيانات الشخصية الذي لم يصدر بعد، بأنها: " أي بيانات أو معلومات تتعلَّق بشخص طبيعي مهما كان مصدرها أو شكلها، والتي من شأنها التعريف به بطريقة مباشرة أو غير مباشرة من خلال العديد من المعلومات أو الرموز، بما في ذلك البيانات المتعلِّقة بالحالة الشخصية أو وضعه العائلي، أو بيانات تحديد الموقع الجغرافي أو بيانات تعريف الإنترنت الخاضعة لقواعد الحماية المقرِّرة بموجب أحكام هذا القانون".

كما عرَف المشرع الأردني في مسوَّدة القانون البيانات الحسَّاسة بأنها: " هي التي تشكِّل معالجتها مخاطرَ أو تمييزا بالنسبة إلى حماية الحياة الخاصة للشخص؛ كأن تبين الأصل العرقي، أو الآراء والاتجاهات السياسية والمعتقدات الدينية، أو أي بيانات تتعلق بحالته الصحية أو الجسدية، أو العقلية أو الاقتصادية، أو انتماءاته الحزبية أو سجلِّه الجُرمي".

كما عرَّف قانون حماية البيانات الشخصية **البحريني** البيانات الشخصية في قانون رقم (30) لسنة 2018 في المادة الأولى منه: أنها" أية معلومات في أية صورة تخصُّ فردا معرَّفا، أو قابلا بطريق مباشر أو غير مباشر لأن يُعرَّف، وذلك بوجه خاص من خلال رقم هويته الشخصية أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية، ولتقرير ما إذا كان الفرد قابلا لأن يُعرَّف، تراعى كافة الوسائل التي يستخدمها مدير البيانات أو أي شخص آخر، أو التي قد تكون متاحة له".

وعرَّف المشرِّع البحريني البيانات الشخصية الحسَّاسة بأنها: أية معلومات شخصية تكشف على نحو مباشر أو غير مباشر؛ عن أصل الفرد العِرْقي أو الإثْنِي أو آرائه السياسية أو الفلسفية أو معتقداته الدينية أو انتمائه النقابي أو سِجِل السوابق الجنائية الخاص به أو أية بيانات تتعلَّق بصحته أو حالته الجنسية.

أما المشرِّع **الإماراتي** فعرَّفها بقانون حماية البيانات الشخصية رقم45 لسنة 2021 في المادة الأولى منه على النحو الآتي: " أي بيانات تتعلَّق بشخص طبيعي محدد، أو 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 المعرِّف الإلكتروني 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".

كما عرَّف أيضاً في نفس القانون البيانات الحساسة على أنها: " أي بيانات تكشف بشكل مباشر أو غير مباشر، عن عائلة الشخص الطبيعي أو أصله العرقي أو آرائه السياسية أو الفلسفية أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به، أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحة هذا الشخص وتشمل حالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية له التي تكشف عن وضعه الصحي".

ولم يكتفِ المشرِّع الإماراتي بتعريف البيانات الحساسة، فعرَّف أيضا البيانات الحيوية البيومترية بأنها: "البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلَّق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات، والتي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات، مثل صورة الوجه، أو بيانات البصمة".

عرف المشرع القطري البيانات الشخصية في نص المادة الأولى من قانون حماية البيانات الشخصية:" بيانات عن الفرد الذي تكون هويته محددة، أو يمكن تحديدها بصورة معقولة، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى".

ولا بد من الإشارة إلى إن بريطانيا من أوائل الدول التي اهتمَّت بحماية البيانات الشخصية، ففي عام 1948 أصدرت قانون حماية البيانات، ثم أصدرت في عام 1998 قانون حماية البيانات الشخصية، وعرَّفها بانها البيانات المتعلقة بالشخص الحي الذي يمكن تعريفه بها أو بضمِّها لمعلومات أخرى في حوزة المسؤول عن معالجة البيانات، أو من المحتمل أن تكون في حوزته[1].

كما عرفتها اللائحة العامة للاتحاد الأوربي بأنها: "أي معلومات تتعلَّق بشخص طبيعي محدد أو يمكن التعرف عليه (موضوع البيانات)؛ الشخص الطبيعي الذي يمكن التعرف عليه هو الشخص الذي يمكن التعرف عليه، بشكل مباشر أو غير مباشر، ولا سيما بالإشارة إلى معرِّف مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرِّف عبر الإنترنت أو إلى عامل أو أكثر من العوامل المحددة للهوية الجسدية أو الفسيولوجية أو الوراثية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص الطبيعي[2]".

أيضا عرَّفت اللائحة في المادة الرابعة "البيانات الوراثية" تعني البيانات الشخصية المتعلقة بالخصائص الوراثية الموروثة أو المكتسبة للشخص الطبيعي والتي تعطي معلومات فريدة عن فسيولوجيا أو صحة ذلك الشخص الطبيعي والتي تنتج على وجه الخصوص عن تحليل عينة بيولوجية من الشخص الطبيعي المعني؛

---

(1) الحسيني، محمد يحيى، الحماية القانونية للبيانات الشخصية، دراسة مقارنة بين القانون البريطاني والاماراتي، دار القضاء، بحث منشور، ص11.

(2) General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu)-

و"البيانات البيومترية" تعني البيانات الشخصية الناتجة عن معالجة تقنية محددة تتعلَّق بالخصائص الفيزيائية، أو الفسيولوجية، أو السلوكية للشخص الطبيعي، والتي تسمح أو تؤكد التعريف الفريد لذلك الشخص الطبيعي، مثل صور الوجه أو البيانات بالمنظار".

و"البيانات المتعلقة بالصحة" تعني البيانات الشخصية المتعلقة بالصحة البدنية، أو العقلية للشخص الطبيعي، بما في ذلك توفير خدمات الرعاية الصحية، التي تكشف عن معلومات عن حالته الصحية".

كما نصت المادة 16 من قانون البيانات الشخصية القطري على البيانات الشخصية ذات الطبيعة الخاصة، حيث ان النص جاء كالاتي:" تعد بيانات شخصية ذات طبيعة خاصة، البيانات المتعلقة بالأصل العرقي، والأطفال، والصحة أو الحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقة الزوجية، والجرائم الجنائية.

وللوزير أن يضيف أصنافاً أخرى من البيانات الشخصية ذات الطبيعة الخاصة، إذا كان من شأن سوء استخدامها أو إفشائها إلحاق ضرر جسيم بالفرد.

ولا يجوز معالجة البيانات الشخصية ذات الطبيعة الخاصة، إلا بعد الحصول على تصريح بذلك من الإدارة المختصة، وفقاً للإجراءات والضوابط التي يصدر بتحديدها قرار من الوزير.

وللوزير، بقرار منه، فرض احتياطات إضافية لغرض حماية البيانات الشخصية ذات الطبيعة الخاصة".

وبناءً على ما سبق فإن الباحث يرى بأن المشرِّع الاماراتي عرَّف البيانات الشخصية بشكل قريب جدا لما جاء باللائحة الأوربية حيث إن التعريف اشتمل على جميع أشكال البيانات ذات الطابع

الشخصي، فعرَّف كلًّا من البيانات الحساسة والصحية والوراثية والانتمائية في نصِّ القانون في حين المشرِّع الأردني في مسوَّدة قانون حماية البيانات الشخصية اكتفى بتعريف البيانات الشخصية، وبتعريف البيانات الحساسة بدون تعريف أشكالها، وبالتالي المشرِّع الأردني لم يذكر البيانات البيرمترية في مسوَّدة القانون.

ويمكن أن نستخلص من التعاريف السابقة التعريف الآتي: إن أي معلومة أو بيان من شأنها التعريف بالشخص أو قابله للتعريف به بحيث تكشف عنه بشكل مباشر او غير مباشر؛ بحيث تكون قادرة على تحديد هويته على وجه الخصوص، سواء كانت عناصر متعلِّقة بشخصه، أو بسماته النفسية أوالجينية أو بأعماله الاقتصادية أو الثقافية وبمعلوماته النفسية والصحية والاجتماعية والدينية والعرقية.

المطلب الثاني
الفرق بين المعلومات والبيانات

شاع في مطلع الستينات استخدام مصطلح المعلوماتية، وكان العالم الروسي (ميخائيلوف) أوَّل من استخدمها، والذي كان مديرًا للمعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفيتي سابقاً، ثم شاع استخدامها على مستوى جغرافي واسع، فكان لها العديد من التعريفات، فكلمة معلوماتية اختصار لكلمتي معلومة وآلية، وتعني المعالجة الآلية للمعلومات، وعليه فإن المعلوماتية تعني المعلومات التي تمَّت معالجتها بوسائل آلية، فالمعلومات أثمن ما يمتلكه الإنسان عبر العصور، لذا سعى لحفظها وجمعها وسائل عدة، وكان أول محاولة حفظها على يد المصريين الذين سجَّلوا حضارتهم على جدران المقابر والمعابد وأوراق البردي، وهذا ساعد على حفر حضارتهم في ذاكرة التاريخ، بالمقابل يوجد حضارات عظيمة اندثرت بسبب عدم جمعها وحفظها، وذلك يعني أن المعلومة

رمز الحضارة وفقدان المعلومة تعني ضياع حضارة [1]، لقد عرَّف الأستاذ (Parte) المعلومات بأنها: "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال أو التفسير والتأويل أو للمعالجة، سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها، أو نقلها بوسائلَ وأشكالٍ مختلفة [2]".

كما عرَّف المشرِّع الأمريكي المقصود بالمعلومات في قانون المعاملات الإلكترونية الصادر سنة 1990 بالفقرة العاشرة من المادة الثانية بأنها: تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر، والبرامج الموضوعية على الأقراص المرنة وقواعد البيانات، أو ما شابه ذلك [3].

المعلومات: من حيثُ مدلولها اللُّغوي مشتقة من المادة اللغوية "علم" وهي مادة غنية بالكثير من المعاني كالعلم والإحاطة بباطن الأمور والوعي والإدراك واليقين والإرشاد والإعلام والشهرة والتمييز والتيسير وتحديد المعالم والمعرفة والتعليم والتعلم والدراية ...الى آخر ذلك من المعاني المتصلة بوظائف العقل [4].

وعرَّفت البيانات بأنها: "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة، سواء بواسطة الأفراد أو الأنظمة

---

(1) الرابحي عزيزة، رابحي عزيزة (2018)، الاسرار المعلوماتية وحمايتها الجزائية رسالة دكتوراه منشورة، جامعة أبو بكر بلقايد، تلسمان، كلية الحقوق، ص21 وص23. الأسرار المعلوماتية وحمايتها الجزائيةSajPlus.com | : available: (on– line) تمت زيارة الموقع الساعة 3 مساءً تاريخ 2022/7/17.

(2) الحسيني عمار عباس (2017)، جرائم الحاسوب والانترنت والجرائم المعلوماتية، منشورات زين الحقوقية، بيروت، لبنان، ص 79.

(3) إبراهيم، خالد ممدوح (2008)، أمن المعلومات الالكترونية، الدار الجامعية، ص31.

(4) السكر، سلطان فياض محمد، مرجع سابق، ص32.

الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها، أو نقلها بوسائل وأشكال مختلفة [1]".

عرف المشرع الإماراتي البيانات:" مجموعة منظمة او غير منظمة من المعطيات، او الوقائع او المفاهيم او التعليمات او المشاهدات او القياسات تكن على شكل ارقام او حروف او كلمات او رموز او صور او فيديوهات او إشارات او أصوات او خرائط او أي شكل اخر، يتم تفسيرها او تبادلها او معالجتها، عن طريق الافراد او الحواسيب، والتي ينتج بعد معالجتها او تداولها ما يطلق عليه مصطلح معلومات."

عرف المشرع البحريني البيانات بأنها:" كل ما يمكن تخزينه ومعالجته وتوليده ونقله باستخدام وسائل تقنية المعلومات وبوجه خاص الكتابة والصور الثابتة والمتحركة والصوت والأرقام والحروف والرموز والإشارات وغيرها ".

عرف المشرع الأردني البيانات في قانون الجرائم الإلكترونية في المادة الأولى منها، " فالبيانات: هي الأرقام، أو الحروف، أو الرموز، أو الأشكال، أو الأصوات، أو الصور، أو الرسومات التي ليس لها دلالة بذاتها".

البيانات بوصفها العام فتعني: "مجموعة من الأرقام والكلمات والرموز والحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للاستخدام، والتي تخلو من المعنى الظاهر في أغلب الأحيان، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات [2]"، وأيضا عُرِّفت بأنها: "مجموعة من البيانات التي قد تمَّت معالجتها وتحليلها وتجريبها؛

(1) قورة، نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، مصر، ص97.

(2) الحسيني، عمار عباس (2017)، جرائم الحاسوب والأنترنت والجرائم المعلوماتية، مرجع سابق، ص 81.

لتحقيق الأهداف المرجوَّة منها، واستخدامها في المجالات المختلفة، أي أنها البيانات المجهزة في شكل منظم ومعين بتسلسل منطقي [1]".

يميِّز الكثير من الباحثين بين المعلومات والبيانات، فالمعلومة مطلب أساسي للتعامل مع الحاسوب، ومن أجلها يتم إعداد البرامج فيتم التوصُّل إلى المعلومات من خلال الحاسوب، من ثم يتم البحث عن البيانات؛ لتخزينها على الحاسوب، ومن ثم معالجتها وتحويلها إلى معلومات، وعليه فإن كلَّ البيانات معلومات، وليس كلُّ المعلومات بيانات [2]، في حين ذهب اتجاهٌ آخرُ إلى أن المصطلحَيْن يؤدِّيان إلى مفهومًا واحدًا، فلم يفرِّق المشرِّع العراقي في قانون التوقيع الإلكتروني، والمعاملات الإلكترونية العراقي لسنة 2012، وقانون المعاملات الإلكترونية الأردني لسنة 2019 بين المصطلحَيْن [3].

أما فيما يخصُّ طبيعتها القانونية، فقد انقسم الفقه إلى اتجاهين: فالاتجاه الأوَّل وهو الاتجاه التقليدي يرى بأن المعلومات ليس لها أي قيمة مادية وغير قابلة للتملك، ومن ثم فهي لا تدخل ضمن الحقوق المحمية قانوناً إلا إذا كانت متصلة بالملكية الأدبية أو الفنية أو الصناعية، فالمعلومات بنظرهم ليس لها طبيعة مادية وليست محسوسة التي لا يجعلها محلَّ حقٍّ للحماية، أما الاتجاه الآخر وهو الاتجاه الحديث الذي تبنَّاه الفقه الفرنسي (الفقيه PIRRE CATALK) أن المعلومات لها قيمة مالية كالسلعة بكونها نتاجًا بشريًّا وأسند رأيه إلى حُجَّتين، أولهما القيمة الاقتصادية للمعلومات وثانيهما العلاقة اللصيقة بين المعلومة وصاحبها [4].

---

(1) رابحي، عزيزة، (2018)، الأسرار المعلوماتية وحمايتها الجزائية، مرجع سابق، ص 25.

(2) رابحي عزيزة، مرجع سابق، ص 28.

(3) الحسيني عمار عباس، جرائم الحاسوب والأنترنت والجرائم المعلوماتية، مرجع سابق، ص82.

(4) قورة، نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، مرجع سابق، ص120، وأشار اليه الحسيني عمار عباس، مرجع سابق، ص78 وص 88.

فالمعلومات أصبحت أقرب ما يكون للسلعة، فالمعلومات تكون على عدة صور كالاتي:

1. المعلومات الاسمية.
2. المعلومات متعلقة بالمصنفات الفكرية.
3. المعلومات المباحة. [1]
4. المعلومات السرية.
5. المعلومات التجارية والصناعية.
6. المعلومات العسكرية. [2]

المطلب الثالث
طبيعة البيانات الشخصية

في الوقت الراهن يتم تبادل العديد من البيانات كل يوم، وذلك تبعاً لكثرة المواقع والتطبيقات وهذه البيانات بيانات ذات طابع شخصي حيث إنها تتعلَّق بحياته الخاصة، كما إن تبادلها لا يقتصر على حدود جغرافية معينة، بل في جميع أنحاء العالم، وإن هذا يخلق حالة من الخوف؛ لصعوبة السيطرة عليها وحفظها.

فمستخدمو المواقع الإلكترونية في ازدياد؛ وذلك بدوره يؤدي إلى تدفُّق كبير للبيانات التي هي عرضة للانتهاك، فالوضع لم يقتصر على الفيس بوك مثلا، فلقد ظهرت في الآونة الأخيرة العديد من غرف الدردشة، والتطبيقات الكثيرة التي لا تقتصر فقط على الدردشة بين الأصدقاء، بل ظهرت مواقع أخرى لها أغراض مغايرة؛ مثل الإعلانات التجارية التي تستهدف البيانات الخاصة بالمستخدمين

---

(1) المضحكي، حنان ريحان (2014). الجرائم المعلوماتية "دراسة مقارنة"، ط1، منشورات الحلبي الحقوقية، بيروت، ص 45.

(2) الحسيني، عمار عباس، مرجع سابق، ص83.

للقيام بإعلانات تثير اهتماماتهم، ومقابل ذلك فإن المستخدمين على جهل في هذه الأمور، واستخدام المواقع على غير وعي فلا بدَّ من تسليط الضوء على طبيعتها؛ لتمييزها عن غيرها من البيانات.

إن المتمعِّن في تعاريف أغلبية الدول العربية للبيانات الشخصية يجد أنه تمَّ تعريفها على أنها بيانات من شأنها التعريف به، وتمييزه عن غيره من الأشخاص، كما أن السمة الأساسية في هذه البيانات أنها تتصل بأشخاص طبيعيين[1]، بينما من يتمعَّن في تعريف القانون البريطاني للبيانات الشخصية، يجد أنه خصَّ الحماية للشخص الحي، هذا يعني أن التشريعات العربية أكثر توفيقا، حيث نجد أنها جعلت الحماية للشخص سواء كان حيًّا أو ميتًا؛ وذلك تكريساً لمبدأ الكرامة الإنسانية، وأن موت الإنسان لا يعني أن يتمَّ انتهاك خصوصيته؛ فالتشريع البريطاني يرفع الحماية بموت الشخص[2]، بالإضافة إلى أنها بيانات مخفية فإن أيَّ بيانات مكشوفة للجمهور وظاهرة للعلن لا تُعدُّ ذات طابع شخصي، فتعتبر مباشرة حين تتصل بشخص المستخدم؛ مثل اسمه ولقبه، وتكون غير مباشرة؛ مثل بريده الإلكتروني وكلمة المرور[3].

ولا بدَّ من الإشارة إلى أن البيانات المجهولة وهي التي لا تدلُّ ولا يُستدلُّ منها على شخص تعلَّقت به، إذ إن المجهول لا خصوصية له[4] فهي لا تتمتَّع بالخصوصية؛ لأن من شروط المعلومات

---

(1) التهامي، سامح عبد الواحد، ضوابط معالجة البيانات الشخصية، دراسة مقارنة، مجلة كلية القانون الكويتية العالمة، بحث منشور، ص402. https://journal.kilaw.edu.kw/ / available (on- line) تمت زيارة الموقع 5 مساءً، تاريخ 2022/7/18.

(2) الحسيني، محمد يحيى، الحماية القانونية للبيانات الشخصية، مرج سابق ص8.

(3) المداوي، محمد احمد، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص1942.

(4) أحمد، خالد حسن (2020). الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية، دراسة مقارنة، ص 49، ON-LINE Available الحق في خصوصية البيانات الشخصية بين الحماية القانونية (ebscohost.com) تمت زيارة الموقع الساعة 9 مساءً، تاريخ 19/ 7/2022.

الشخصية أن تعرف بالشخص، وكذلك الحال للمعلومات الموضوعية؛ فهي تتعلق بالحياة العامة للأفراد، وتختلف عن المعلومات الشخصية؛ كالاسم والحالة المدنية المخزَّنة في بنوك المعلومات التي تمسُّ الحياة الخاصة للأفراد [1]، ويظهر مما سبق أن البيانات تكون شخصية عندما تكون معرِّفة عن الفرد، وليست مجهولة، وعندما يكون من حقِّ صاحبها فقط الكشف عنها، فالأصل أن تكتنفها السرية، وأن تبقى بمأمن عن الغير.

وقد حرصت جميع الأنظمة القانونية على إخضاع البيانات الصحية للحماية، من خلال السرية المهنية، أي مبدأ "السرية الطبية[2]."

وإن من أهم البيانات الشخصية والأكثر عرضة للانتهاك معرفة أرقام بطاقات الائتمان من الحصول عليها عن طريق الاحتيال الإلكتروني أو السرقة الإلكترونية [3].

ويظهر مما سبق أن المعطيات تكتسب الصفة الشخصية بمجرد ارتباطها في الشخص، سواء كانت بطريقة مباشرة أو غير مباشرة، وتبقى العناصر التي تُعرِّف بالشخص كثيرة ومتعددة، ويدخل فيها كل العناصر الخاصة بشخص معين، متى كانت تُفرِّقه عن غيره، ومُميِّزة لهُويته البدنية، أو الفيزيولوجية، أو الجينية، أو النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية [4].

---

(1) الشوابكة، محمد امين، جرائم الحاسوب والانترنت، مرجع سابق، ص63، انظر أيضا أحمد حسن خالد، مرجع سابق، ص 50.

(2) الأشقر، منى الجبور، محمود جبور، البيانات الشخصية والقوانين العربية، مرجع سابق، ص 84.

(3) الشوابكة / محمد أمين، جرائم الحاسوب والأنترنت، مرجع سابق، ص 69.

(4) يحي، تومي (2020)، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء قانون رقم 18-07، مجلة الأستاذ الباحث للدراسات القانونية والسياسية مجلد 4 عدد 2، available (on- line) الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07 دراسة تحليلية (cerist.dz) ASJP |، تمت زيارة الموقع الساعة 2 مساءً، تاريخ 2022/7/20،ص1521

ويبدو مما سبق أن البيانات ذات الطابع الشخصي تتصل بشخص الفرد بشكل مباشر؛ مثل حالته النفسية، والعقلية التي لا يجب أن يطَّلع أيُّ أحد عليها، ولإدراك المشرِّع بأهميتها أطلق عليها مصطلح حساسة؛ دلالة على أهمية حمايتها من الآخرين، ويمكن تعريفها على النحو الاتي:

- بيانات بيومترية: وهي التي تُعنى بالسمات الخاصة بشكل مباشر بالفرد؛ كبصمة العين وبصمة الإصبع، والتي عَرَّفتها اللائحة العامة الأوربية في نص المادة الثانية منها: " تعني البيانات الشخصية الناتجة عن معالجة تقنية محددة تتعلَّق بالخصائص الفيزيائية، أو الفسيولوجية، أو السلوكية للشخص الطبيعي، والتي تسمح أو تؤكِّد التعريف الفريد لذلك الشخص الطبيعي؛ مثل صور الوجه أو البيانات بالمنظار".
- بيانات جينية: وهي التي تتصل بالصفات الموروثة والمكتسبة بالوراثة للشخص المعني الطبيعي.
- بيانات الائتمانية: وهي التي تكون بهدف الحصول على تمويل نقدي.

وأخيرا يرى الباحث بأنَّ البيانات ذات الطابع الشخصي لها عدة سمات:

كونها بيانات سرية، تتصل بأشخاص طبيعيين، فهي لا تتصل بشخص معنوي، تكشف عن هوية الفرد سواء بشكل مباشر مثل اسمه ولقبه، أو غير مباشر؛ مثل بريده الإلكتروني، الحق في الكشف عنها يكون لصاحبها فقط وأخذ موافقته، وبإذنه.

المبحث الثاني
نطاق حماية البيانات الشخصية (الحق في الخصوصية)

إن الحديث عن موضوع حماية البيانات ذات الطابع الشخصي يخلق التساؤل الآتي: هل الحق في حماية البيانات الشخصية يدخل في إطار الحق في الخصوصية، أم هو حق مستقل؟

إن مصطلح الخصوصية ليس حديث النشأة، وهو من أقدم الحقوق الشخصية، حيث وُجد بوجود الإنسان، والخصوصية تعني السرية بما تحمله من تعابير؛ كالعزلة، والخلوة، والانطواء، فالإنسان حقه أن تُحاط حياته الخاصة بالسرية والكتمان، ونظرا للتغيرات التي طرأت على العصر الذي نعيشه من تقدم تقني، لا بدَّ من إحاطة خصوصية الأفراد بحماية تعمل على الحدِّ من التطفل عليها[1].

فالتطور التقني نتج عنه العديد من الإيجابيات، لكنه في المقابل أحدث نافذة يُقتحَم من خلالها الآخرين حياةُ المرء الخاصة، والتي تعدَّت الشكل التقليدي؛ كخرق حرمة منزل دون استئذان، إلى مكان لا حدود له ولا جدران ولا حواجز.

فمن حق الفرد أن تبقى حياته الخاصة بعيدة عن أنظار المتطفلين، والفضوليين، وذوي السلوكيات السيئة، بحيث يحفظ نفسه من انتهاك أسراره، وكل أمور حياته التي ليس من حق أحد معرفتها، فأغلب التشريعات أوردت أحكام تقليدية؛ مثل الأحكام الخاصة بالجوار والمناور[2].

لكن التشريعات الخاصة بالحماية القانونية لحق الخصوصية عالجت انتهاك الخصوصية بشكلها التقليدي في الواقع المادي، وبعض الدول أوردت قوانين خاصة بانتهاك الخصوصية في الواقع

---

(1) الزعبي، علي احمد عبد، 2006، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، طرابلس، لبنان، ص13.

(2) محمود، عبد الرحمن محمد، نطاق الحق في الحياة الخاصة، مرجع سابق، ص5، ص6.

الافتراضي، حيث يرى الأستاذ **ويستن** أن الأجهزة التقنية الحديثة تهدِّد الحياة الخاصة للأفراد في ثلاث حالات؛ وهي المراقبة البدنية، والمراقبة النفسية، وأخيرا رقابة البيانات وتجمعيها وتبادلها والتعامل بوثائق المعلومات حول الأفراد بواسطة آلات تجهيز البيانات[1].

وعليه سيتم تقسيم هذا المبحث على النحو الآتي:

المطلب الأول: تعريف الحق في الخصوصية.

المطلب الثاني: وسائل حماية الحق في الخصوصية.

المطلب الثالث: الحق في حماية البيانات الشخصية؛ كحق مستقل عن الحق في الخصوصية.

المطلب الأول
تعريف الحق في الخصوصية

الخصوصية لغة: يُقصد بها حالة الخصوص، والخصوص نقيض العموم، وقال: خصَّه الشيء، ما يختص به دون غيره؛ أي يتميز به، ويقال: اختص فلان بالأمر وتخصَّص له إذا انفرد وخصَّ غيره ببِرِّه، ويقال: فلان يخصُّ فلان؛ أي خاصٌّ به، وله به خصيصة، والخاصة ما تخصُّه لنفسك[2].

الخصوصية اصطلاحاً: "عرَّف معهد القانون الأمريكي الخصوصية: كلُّ شخص ينتهِك بصورة جدية وبدون وجه حقَّ شخص آخر في أن لا تصل أموره وأحواله إلى علم الغير، وألا تكون صورته عرضة لأنظار الجمهور، و يعتبر مسؤولاً أمام المعتدى عليه، وعرَّفها الفقيه هشام محمد فريد رستم

---

(1) – مرنيز، فاطمة، حرمة الحق في الخصوصية للعامل في ظل الوسائل التكنولوجية الحديثة، رسالة دكتوراه منشوره، ص2،

أطروحة دكتوراه : الاعتداء على الحق في الحياة الخاصة عبر شبكة الأنترنت PDF علوم قانونية وادارية (boubidi.blogspot.com) تمت زيارة الموقع الساعة 11 صباحا، تاريخ 2022/7/22.

(2) – ابن منظور، لسان العرب، (2000)، المجلد الخامس ط 1، دار صادر للطباعة والنشر، بيروت، ص80.

بأنها: " قيام مفهوم الحق في الخصوصية بتوافر وجهين أحدهما مادي؛ وقوامه عدم اقتحام الشخص في خصوصيات الآخرين، والثاني إعلامي؛ مقتضاه ألا تكون الشؤون الخاصة بالفرد محلاً للحق في الإعلام بالنسبة للآخرين، مما يُستتبع معه عدم استغلال الآخرين لتلك المعلومات بالنشر أو التشهير.[1]

إن الفقيه بيرو من أوائل الفقهاء الفرنسيين الذين تحدَّثوا في كتاباتهم عن الحق في الخصوصية حيث تحدث عنه في المجلة الفصلية عام 1909 وأشار إلى أن " من حق الشخص أن يعيش في هدوء وسكينة إذا رغب في ذلك، كما أن قيام الغير بنشر أمور متعلِّقة بحياة المرء الخاصة دون موافقته الصريحة أو الضمنية اعتداء على حقه في الخصوصية "[2].

كما عرَّفت : بأنها الحق في حماية الحياة الشخصية للأفراد، وضمان عدم الاعتداء عليها واستغلالها[3].

وعُرِّفت الخصوصية بأنها: " حرص الفرد على الاحتفاظ بجانب من حياته، وأفكاره، وميوله وأنشطته في مجال الحرمات الشخصية لنفسه، أو لمن يختارهم من أعضاء عائلته وأصدقائه وعدم الإفشاء غير المصرَّح به[4] ".

---

(1) – الدهبي خدوجه، حق الخصوصية في مواجهة الاعتداءات الإلكترونية، مرجع سابق، ص145.

(2) – د. أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق، ص 52.

(3) – الدهبي خدوجة، حق الخصوصية في مواجهة الاعتداءات الإلكترونية، مرجع سابق، ص145.

(4) – السكر، سلطان فياض محمد، جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني، مرجع سابق، ص29.

كما عُرفت الخصوصية بأنها: "ليست مجرد التحرر من إنشاء المعلومات من غير مقتضى، أو التحرر من التطفل في أمور تتطلب الخصوصية، ولكن المعنى يمتد أبعد من ذلك، حتى يمكن القول إنها تعني أن يعيش المرء كما يحلو له، وأن يعيش مُستمتعًا باحترام أنشطة خاصة معينة[1]".

وعرَّف جانب من الفقه خصوصية المعلومات بأنها: " قدرة الأفراد على التحكم بدورة المعلومات التي تتعلَّق بهم[2]".

جانب من الفقه الفرنسي عرَّفها أيضا بأنها: "كل ما ليس له علاقة بالحياة العامة، أو هي كل ما لا يعتبر من قبيل الحياة العامة[3]".

إن ما يراه أفرادُ مجتمعٍ معينٍ خصوصيةً، قد لا يكون خصوصيةً لدى مجتمعٍ آخر، فالتعريف بالخصوصية مختلفٌ من بلد لآخر، فأغلب الشعوب تعترف بحق المرء بخصوصية مسكنه، وعدم الاطلاع على مراسلاته، فقد يندرج العديد من الحقوق تحت مضمون الخصوصية؛ ففي فرنسا الذمة المالية أهم خصوصيات الفرد، لكن الوضع مختلف في أمريكا، فيتم نشر معلومات الذمة المالية بشكل منتظم فلم تعتبرها خصوصية، لذلك من الصعوبة تخصيص تعريف معين للخصوصية لاختلافها من بلد لآخر[4]".

في 6 يونيو 2013، " نشرت صحيفة الجارديان قصة باستخدام الأدلة التي قدَّمها سنودن، والتي تؤكد أن وكالة الأمن القومي قد حصلت على أوامر محكمة سرية غير قانونية تتطلب من Verizon،

---

(1) الزعبي، علي احمد عبد، (2006)، حق الخصوصية في القانون الجنائي، مرجع سابق، ص 135.

(2) أبو سريع، أحمد عبد الرحمن، 2011، حقوق الأنسان الرقمية بين الأطلاق والتقييد، ص82.

(3) محمود، عبد الرحمن محمد، نطاق الحق في الحياة الخاصة، مرجع سابق، ص 98.

(4) المعمري، مسعود بن حميد، نطاق الحماية الجزائية للحق في الخصوصية، دراسة مقارنة، مجلة كلية القانون الكويتية العالمية، ص659. available (on-line): مارك: نطاق الحماية الجزائية للحق في الخصوصية (mandumah.com)

وغيرها من شركات الهواتف المحمولة جمع وتسليم سجلات الهاتف لملايين عملائها الأمريكيين إلى الحكومة، ومن ثم كشف سنودن عن معلومات حول برنامج مراقبة يتبع لوكالة الأمن القومي، سمح للحكومة الفيدرالية بجمع وتحليل البيانات الخاصة المخزنة على خوادم يديرها مقدِّمو خدمات الإنترنت، وتحتفظ بها شركات؛ مثل Microsoft و Google و Facebook و AOL و YouTube دون أمر قضائي. فبمجرد اكتشافها، ناضلت هذه الشركات من أجل شرط أن تكون الحكومة الأمريكية شفافة ونزيهة تماما في طلبها للحصول على البيانات، وفازت به، في عام 2015، حيث أقرَّ الكونغرس قانونا لإنهاء المجموعات كبيرة من سجلات هواتف ملايين الأمريكيين بشكل نهائي[1]".

المطلب الثاني
وسائل حماية الحق في الخصوصية

إن الخصوصية لم تقتصر في الوقت الحالي على الخصوصية المادية؛ وذلك لأن التطور التقني ساهم في كشف خصوصيات وحرمات الإنسان بشكل أكبر[2]، فالانفتاح الكبير على شبكة الإنترنت من قِبل الأفراد أدَّى الى إيجاد الكثير من المخاطر التي لا يُدركون حجمها ونتائجها، فالغالبية ليس

---

(1) Tome-head/ constitutional merits and congressional acts/ published article/ 2019. For more look at the following link: (on-line) available /The Origins and History of the Right to Privacy (thoughtco.com) تمت زيارة الموقع الساعة 2 مساءً تاريخ 2022/7/23.

قاعدة حماية خصوصية الأطفال على الإنترنت (COPPA)، 1998 " كانت الخصوصية عبر الإنترنت مشكلة منذ أن تم تسويق الإنترنت بالكامل في الولايات المتحدة في عام 1995. في حين أن البالغين لديهم مجموعة من الوسائل التي يمكنهم من خلالها حماية بياناتهم، فإن الأطفال معرضون للخطر تماما دون رقابة، يفرض COPPA، الذي سنته لجنة التجارة الفيدرالية في عام 1998 ، متطلبات معينة على مشغلي مواقع الويب والخدمات عبر الإنترنت الموجهة للأطفال دون سن 13 عاما. وهي تشمل طلب إذن الوالدين لجمع المعلومات من الأطفال، والسماح للوالدين بتحديد كيفية استخدام هذه المعلومات، وتسهيل الأمر على الآباء لإلغاء الاشتراك في المجموعات المستقبلية".

(2) لامي، بارق منتظر عبد الوهاب (2017). جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، ص 22.

لديهم علم بما قد يحدث من آثار سلبية تمَسُّ حياتهم الخاصة، فالانتهاكات التي تقع على حياة الأفراد الخاصة بشكلها الافتراضي لا تقل خطورة عن الانتهاكات التقليدية، بل قد تكون أكثر خطورة كون الأفراد يتعاملون مع عالم شفاف، وسهل الانتهاك خلاله، وقد يكون هناك صعوبة كبيرة في الإثبات كونه لا يوجد أدلة مادية [1].

فالتشريعات الدولية والاتفاقيات تعمل جاهدة للتصدِّي لهذه الانتهاكات، سواء بصورتها التقليدية أو الافتراضية، فالعديد من الدول تتصدَّى للانتهاكات التي أفرزها العالم الرقمي، كما أن العديد من الدول الأجنبية والعربية أوجدت قوانين للحدِّ من الانتهاكات التي تمسُّ خصوصية المرء.

فوسائل الحماية على الصعيد الدولي؛ ما جاء في اتفاقية بوادست لعام 2001 تُعدُّ هذه الاتفاقية أول اتفاقية ذات طابع دولي يتبنَّاها المجلس الأوروبي في هذا المجال، بحيث ضمَّت العديد من الدول الأوروبية وغير الأوروبية، وقد دخلت حيِّز التنفيذ في سنة 2004، وهي الاتفاقية الأوربية لمكافحة الجرائم المعلوماتية حيث تكوَّنت من مقدِّمة وأربعة فصول، فبعد أن استعرضت المقدِّمة، وأهداف الاتفاقية ومنطقها ومرجعتها، وما تقوم عليه من جهود إرشادية إقليمية ودولية، فقط كان الفصل الأول منها يضمُّ المصطلحات في المادة الأولى، والفصل الثاني كان عنوانه الإجراءات المتعيِّن اتخاذُها المستوى الوطني، وينقسم إلى ثلاثة أقسام:

القسم الأول: يحتوي على المواد من 2-13 وهذه النصوص تعالج النصوص الموضوعية لجرائم الكمبيوتر، القسم الثاني يحتوي على المواد من (14-21) والتي تتعلَّق بالمواد الإجرائية، أما القسم

---

(1) الزعبي، جلال محمد، المناعسة، أسامة احمد (2010). جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، ص91.

الثالث يحتوي على المادة 22 التي تتعلَّق بالاختصاص، والفصل الثالث كان تحت عنوان التعاون الدولي وقُسِّم الى قسمين:

القسم الأول من المادة (23–28) تحت عنوان المبادئ العامة والقسم الثاني من المادة (29–35) يتعلَّق بالنصوص الخاصة، أما الفصل الرابع من المادة (36–48) فضمَّ الأحكام الختامية للاتفاقية.

إن الأسباب التي دعت إلى إبرام هذه الاتفاقية جاء للحرص على التصدِّي لجرائم الكمبيوتر، فأكدَّت مقدِّمة الاتفاقية على اتخاذ التدابير التشريعية والتقنية؛ لضمان ملاحقة مرتكبي الجرائم الإلكترونية، وتوفير خطط للكشف، والتحري والإثبات التي تخصُّ الجريمة التقنية، كما هدفت وحدة التدابير التشريعية بين الدول الأوربية وغير الأوربية، وجاءت للتأكيد على أهمية التعاون الإقليمي والدولي لمكافحة الجرائم الإلكترونية، بالإضافة إلى تحقيق التوازن بين حماية حقوق الانسان الأساسية المعترف فيها بالعهد الدولي للحقوق المدنية والسياسية، وخصوصا الحقوق المتعلِّقة بحرمة الحياة الخاصة [1].

والاتفاقية الأوربية التي نصَّت في المادة الثامنة على" 1– لكل إنسان الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته [2].

---

(1) الحسيني، عمار عباس (2017)، التصوير المرئي والتسجيل الصوتي وحجيتهما في الاثبات الجنائي، دراسة مقارنة المركز العربي للنشر والتوزيع، ط 1، ص125وص 127

(2) اتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا في 4 نوفمبر 1950
hrlibrary.umn.edu/arab/euhrcom.html

الإعلان العالمي لحقوق الإنسان لعام 1948 في نص المادة الثانية عشر على الحق في الخصوصية والنص كان كالآتي: " لا يعرض أحد لتدخل تعسُّفي في حياته الخاصة، أو أسرته، أو مسكنه، أو مراسلاته. ولكل شخص الحق في الحماية القانونية إزاء مثل هذه التدخلات.

العهد الدولي للحقوق المدنية والسياسية الصادر عام 1966 حيث أكدَّت الفقرة الأولى من المادة السابعة عشر على احترام الخصوصية بمختلف صورها، ومنع كل أشكال التدخُّل في الحياة الخاصة للإنسان، وأسرته، ومسكنه، وسريَّة مراسلاته، حيث مُنِع التدخُّل فيها بشكل تعسُّفي، أو غير قانوني[1].

الاتفاقية الأوربية لحقوق الإنسان لسنة 1950 تمَّ إبرامها في العاصمة الإيطالية روما على أن تنفِّذ في 1953 وقد اهتمت بالحقوق والحريَّات، وجاء في نصِّ المادة الثامنة منها: " لكل شخص الحق في احترام حياته الخاصة والعائلية، وحرمة مراسلاته ومسكنه، ولا يجوز للسلطة العامة التدخَّل في مباشرة هذا الحق إلا إذا كان هذا التدخُّل ينصُّ عليه القانون [2]".

كما ورد الحق في الخصوصية في **المادة الحادية عشر من الاتفاقية الأمريكية لحقوق الإنسان لعام** 1969 على النحو التالي:

1. لكل إنسان الحق في أن يُحترمَ شرفُه، وتُصانُ كرامتُه.

---

(1) العهد الدولي للحقوق المدنية والسياسية الصادر عام 1966، *المادة 17* لا يحوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته .2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس، https://www.ohchr.org/ar/instruments-mechanisms/instruments/. تمت زيارة الموقع الساعة 4 مساءً تاريخ 2022/7/21.

(2) نصوص ومواد الاتفاقية الأوروبية لحقوق الإنسان (mohamah.net).

2. لا يجوز أن يتعرَّض أحدٌ لتدخُّلٍ اعتباطي، أو تعسُّفي في حياته الخاصة، أو في شؤون أسرته أو منزله أو مراسلاته، ولا أن يُتعرَّض لاعتداءاتٍ غير مشروعة على شرفه أو سمعته.

3. لكل إنسان الحق في أن يحميه القانون من مثل ذلك التدخل، أو تلك الاعتداءات[1].

أما على صعيد الحماية الدستورية فأغلب دساتير الدول نظَّمت الحقَّ في الخصوصية؛ فالدستور المصري نص في المادة (99) منه على حرمة الحياة الخاصة، والدستور الإماراتي في نص المادة (36): أن للمساكن حرمةً لا يجوز دخولها بغير إذن أهلها، وفي المادة (31): نصَّت على حرية المراسلات البريدية والبرقية. [2]

والدستور البحريني نص في المادة 25 على ما يلي: "للمساكن حرمة، فلا يجوز دخولها أو تفتيشها بغير إذن أهلها إلا استثناء في حالات الضرورة القصوى التي يعينها القانون، وبالكيفية المنصوص عليها فيه"، ونص في المادة 26 على:" حرية المراسلة البريدية والبرقية والهاتفية والإلكترونية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها إلا في الضرورات التي يبينها القانون، ووفقًا للإجراءات والضمانات المنصوص عليها فيه".

أما فيما يخصُّ الدستور الأردني فقد نص على الحق في الخصوصية في نص المادة السابعة: أن كل اعتداء على حرمة الحياة الخاصة جريمة يعاقب عليها القانون.

وعلى صعيد الحماية الجزائية، نص المشرِّع الأردني في قانون العقوبات على حماية الخصوصية، وجَرَّم انتهاك الخصوصية في المادة (347)، والمادة (348)، فجريمة خرق حرمة المسكن تقع بمجرد الدخول غير المشروع؛ فالدخول غير المشروع الذي ليس مسوِّغ قانونا مُجَرَّمٌ حتى

---

(1) الاتفاقية الامريكية لحقوق الانسان لعام 1969 hrlibrary.umn.edu/arab/am2.html.

(2) دستور دولة الإمارات العربية المتحدة (1971).

لو لم يعارِض صاحب المسكن، وإذا كانت الغاية من الدخول هو لقصد معين لو علِم به المجنيُّ عليه لما سمح له بالدخول، فالأصل أن يأذن له صاحب المسكن بالدخول، فالجريمة هنا تقوم على الدخول غير المشروع، فلو كان الدخول مشروعًا لانتفت الجريمة [1].

وقام المشرِّع بتعريف السكن في المادة الثانية، وفي الفقرة الثانية من المادة **(347)** جرَّم المشرِّع الدخول غير المشروع في ظروف مشدَّدة، والمادة **(348)** مكرر من قانون العقوبات، نصت على أنه يعاقب بناء على شكوى المتضرر بالحبس مدة لا تتجاوز ثلاثة أشهر كل من خرق الحياة الخاصة للآخرين باستراق السمع او البصر باي وسيلة كانت بما في ذلك التسجيل الصوتي او التقاط الصور او استخدام المنظار وتضاعف العقوبة في حال التكرار.

كما صدر قانون الجرائم الإلكترونية الأردني لعام (2015) لم يتضمَّن الخصوصية بشكلها التقني، ولم يرد ذكر للبيانات الشخصية فيه.

أما فيما يخص المشرِّع الاماراتي فنصَّ في قانون العقوبات في المادة رقم 434 ما يلي: "يُعاقب بالحبس مدة لا تزيد على سنة، أو بالغرامة التي لا تجاوز خمسة آلاف درهم كلَّ من دخل مكانا مسكونا، أو مُعدًّا للسكنى، أو أحد ملحقاته، أو محلا معدًّا لحفظ المال، أو عقارًا خلافًا لإرادة صاحب الشأن، وفي غير الأحوال المبينة في القانون، وكذلك من بقي فيه خلافا لإرادة من له الحق في إخراجه، أو وُجد متخفيًّا عن أعين من له هذا الحق، وتكون العقوبة الحبس مدةً لا تزيد على سنتين إذا وقعت ليلاً، أو بوساطة العنف على الأشخاص، أو الأشياء، أو باستعمال سلاح، أو من

---

(1) قانون العقوبات الاردني واخر تعديلاته حتى 2022.

شخصين فأكثر، أو بانتحال صفة كاذبة، وإذا كان القصد من الدخول أو البقاء منع الحيازة بالقوة، أو ارتكاب جريمة عُدّ ذلك ظرفاً مشدداً " [1].

اما المشرع البحريني فقد نص على الحق في الخصوصية في نص المادة 361 على النحو الاتي: " يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بالغرامة التي لا تجاوز خمسين دينارا من دخل مكانا مسكونا أو معدا للسكن أو أحد ملحقاته أو محلا معدا لحفظ المال أو عقارا، خلافا لإرادة صاحب الشأن وفي غير الأحوال المبينة في القانون وكذلك من بقي فيه خلافا لإرادة من له الحق في إخراجه، أو وجد مختفيا عن أعين من له هذا الحق.

وتكون العقوبة الحبس مدة لا تزيد على سنتين إذا وقعت الجريمة ليلا أو بواسطة العنف على الأشخاص أو الأشياء أو باستعمال سلاح أو من شخصين فأكثر، أو بانتحال صفة عامة أو ادعاء القيام أو التكليف بخدمة عامة أو الاتصاف بصفة كاذبة، وإذا كان القصد من الدخول أو البقاء منع الحيازة بالقوة أو ارتكاب جريمة، عد ذلك ظرفا مشددا. [2]

كما أن المُتمعِّن في أغلب التشريعات سيلاحظ أنها اكتفت بإيجاد نصوص قانونية، تكفل حماية الحق في الخصوصية، ولم تضع تعريفا لها، والواضح أيضا أنه ليس بالأمر السهل وضعُ تعريفٍ جامع مانع؛ ويرجع ذلك لمرونة المصطلح وتطوُّره؛ كونه مرتبطاً بالعادات والتقاليد، والثقافات والقيم الدينية السائدة في كل مجتمع [3]، فهو مصطلح يختلف من دولة إلى أخرى بالإضافة إلى اختلافه حسب الظروف الخاصة لكلِّ شخص.

---

(1) قانون العقوبات الاتحادي لدولة الامارات العربية (1987).

(2) قانون العقوبات البحريني مرسوم بقانون رقم (15) لسنة 197.

(3) العابدين، مروة زين، 2016، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت، بين القانون الدولي الاتفاقي والقانون الوطني، رسالة دكتوراه، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر، ص 55، ON-Lain available: http// تمت الزيارة الساعة الثامنة تاريخ 2022/7/22.

المطلب الثالث

الحق في حماية البيانات الشخصية كحق مستقل

لقد انقسمت الآراء إلى اتجاهين في مسألة نطاق حماية البيانات الشخصية ضمن الحق في الخصوصية بشكلها التقليدي، فذهب الاتجاه الأول بأن الحق في الخصوصية تطوَّرَ خلال ثلاث مراحل: المرحلة التقليدية وهي الحق في حماية الأفراد من أي شكل من أشكال الاعتداء المادي على حياتهم وممتلكاتهم، وهي الخصوصية المادية، أما الثانية فكانت حماية العناصر المعنوية للشخص، وهي الخصوصية المعنوية، وأخيرا الخصوصية التي ارتبطت ارتباطًا وثيقًا بأثر التقنية المعلوماتية على بيانات الأشخاص ومعلوماتهم، وهي الحق في حماية البيانات الشخصية في مواجهة التقنية، حيث تلخَّص هذا الراي إلى أن حماية البيانات الشخصية هي فرعٌ من الخصوصية، وتتعلَّق بحماية بيانات المرء الشخصية في عصر المعلوماتية، فالخصوصية بالعموم تنطوي على حماية بيانات مادية، ومعنوية، ومعلوماتية، وهذا يعني أن الخصوصية قد تطوَّرت تبعًا للتطور التكنولوجي، وهي تتخذ صورًا عديدةً، وتندرج جميعها تحت مسمَّى الحياة الخاصة [1].

أما الاتجاه الثاني فذهبت إليه محكمة العدل الأوربية في أول سابقة سنة (2008) في ميثاق الاتحاد الأوربي المادة السابعة والثامنة منه؛ كمصدر مباشر لاعتبار الحق في حماية البيانات الشخصية حق من حقوق الأفراد، ومنفصل عن الحق في الخصوصية، وعلى خلاف الحماية التي نصَّت عليها المواثيق، وأكَّدتها في تقاريرها، فإن الحماية التي جاء بها الاتحاد الأوروبي عام 2009،

---

(1) أيوب، بولين أنطونيوس، 2009، الحماية القانونية للحياة الخاصة في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، ص10، ص66 وص67.

وذلك بتاريخ نفاذ معاهدة لشبونة، أصبحت حماية البيانات الشخصية قانونا ملزما، بعدما اتضح أن كلًّا من الحق في الخصوصية والحق في حماية البيانات رغم ترابطهما إلا أنهما حقان منفصلان.

إن حقَّ حماية البيانات الشخصية حقٌّ أساسيٌّ تمَّ التأكيد عليه عام 1981 اتفاقية مجلس أوروبا بشأن حماية الأشخاص اتجاه المعالجة الآلية إلى أن تمَّ اليوم الوصول إلى قانون موحَّد على مستوى اللائحة العامة التي دخلت حيِّز النفاذ عام 2018، إن الاتحاد الأوربي قبل 2000 كان يعتبر احترام الحياة الخاصة يشمل حماية البيانات الشخصية، أما بعدُ فأصبح حقًّا مستقلا؛ لأن من منظوره أن حقَّ الخصوصية أوسع نطاقا من حق حماية البيانات الشخصية [1].

بناءً عليه؛ فإن الاتحاد الأوربي تدَرَّج في حماية البيانات الشخصية على النحو الآتي:

- صدرت الاتفاقية الأوربية لحقوق الإنسان عام 1950 التي نصَّت على الحق في الخصوصية في المادة.
- اتفاقية مجلس أوروبا بشأن حماية الأشخاص اتجاه المعالجة الآلية لعام 1981.
- صدر ميثاق الحقوق الأساسية عام 2000.
- صدور التشريع الأوربي الموحَّد تحت عنوان القواعد العامة لحماية البيانات (GDPR) سنة 2016 ودخل حيِّز النفاذ عام 2018.

---

(1) الشافعي، آمال، ام السعد شافعي، التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوربي، بحث منشور، مجلة الباحث القانوني، مجلد 1 عدد2، جامعة الحاج لخضر، باتنه، 2022، ص 122 وص118. available (on-line): التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوربيASJP | تمت الزيارة الساعة 1 مساء تاريخ 2022/8/22.

وفي هذا الإطار يرى الباحث أن البيانات الشخصية محلَّ اهتمام كبير، كونها لصيقةً بالشخص وتُعرِّف به، ويتفق مع الرأي الثاني؛ فالحق في حماية البيانات الشخصية لا يندرج تحت مُسمَّى الحق في حماية الخصوصية؛ خاصة لما يشهده العالم من تطورات تقنية هائلة، فإن الدساتير لم تنصَّ بشكل صريح على الحق في حماية البيانات الشخصية، ولم يتمَّ ذكرها، فكانت الحماية تتركَّز على الحق في الخصوصية بشكلها التقليدي، والتي تتمثَّل بخرق حرمة منزل دون إذن صاحبه، وحرية المراسلات، وقد تبيَّن من تعريفات الدول للخصوصية أنها لم تُشِر إلى حماية البيانات الشخصية لا سيَّما بعد التطور التقني، واستعمالها ضمن الفضاء الإلكتروني بشكل كبير، لذلك تذهب الدراسة إلى أن الحق في الخصوصية كان على اتصال كبير بالانتهاكات بشكلها التقليدي، ولم يتطرَّق إلى الانتهاكات في العالم الرقمي، كما أن غالبية الدول أصدرت قوانين خاصة بالحق في حماية البيانات الشخصية كالقانون الإماراتي والبحريني، حيث يمكن معه القول بأنه حقٌّ مستقلٌّ عن الخصوصية رغم ترابطهما إلا أنهما حقّان مستقلان؛ ذلك لأن البيئة التي تُرتكَب فيها الانتهاكات التي تقع على البيانات الشخصية تفتقر لعنصر الأثر المادي على عكس البيئة التي تُرتكَب فيها الانتهاكات التي تقع على الخصوصية بشكلها التقليدي، فالاعتداءات التي تقع على البيانات الشخصية تقع في بيئة رقمية افتراضية.

الفصل الثالث

النموذج القانوني لمعالجة البيانات الشخصية

إن العالم الرقمي يشهد زخما كبيرا من الانتهاكات، والاعتداءات التي تقع على المعطيات الشخصية، حيث إن الفضاء الإلكتروني يكشف عن بيانات الأفراد الخاصة التي لا يحقُّ لغيره معرفتها، كما أنه في الوقت الحالي أشعل فتيل القلق لما يحمله من مخاوف وسلبيات؛ غايتها انتهاك خصوصية معطيات الأفراد؛ لأهدافَ وغاياتٍ غيرِ مشروعة.

فحماية البيانات ذات الطابع الشخصي في غاية الأهمية؛ كونها تحقِّق مبدأ الشرعية التي تقوم عليها الدولة القانونية، ومن هذا المنطلق فإنه يتوجَّب على الدولة أن تكفل حق حماية البيانات الشخصية، باعتبار أيِّ تعدٍّ عليها هو تعدٍّ على حياة الأفراد الخاصة.

إن الفرد يفقد سيطرته على بياناته في مواجهة ثلاثة أطراف، أوَّلُها الحكومات، والشرطة، والأجهزة الاستخبارية والشركات التجارية، فمن خلال أجهزة الكمبيوتر المنتشرة يتم مراقبة الملايين أثناء ممارسة الوظائف، بالإضافة إلى الشركات الموجودة في العالم الافتراضي القادرة على أخذ ملفات تعريفية لمستخدميها، وحفظها لأغراض تسويقية، ولغرض بيعها، ولأغراض أخرى، علاوة على انتشار الأشخاص الافتراضيين، وهم الفضوليون الذين يريدون التعرف أكثر على أصدقائهم أو جيرانهم عبر الوسائل التقنية [1].

ففي الاتحاد الأوربي تم تفعيل اللائحة العامة لحماية البيانات (GDPR)؛ وذلك لاهتمام الأوربيين في حماية بياناتهم الشخصية، وأدراكهم للمخاوف التي تحيط بيناتهم الشخصية نظرا لما أحدثته

---

(1) الشافعي، آمال، الشافعي، أم السعد، مرجع سابق، ص120.

التكنولوجيا من أثار سلبية، وكذلك الحال قام الفرنسيين، فرضت غرامة مالية على شركة جوجل وقدرها 150 الف يورو بواسطة اللجنة الوطنية لتكنولوجيا المعلومات والحريات لعام 2014 ؛ وذلك لرفضها الالتزام بما جاء فيه القانون الفرنسي في ضرورة احترام خصوصية البيانات الشخصية، حيث تبين انهم ينتهكوا خصوصية بيانات المستخدمين بالرجوع إلى بياناتهم بهدف القيام بإعلانات تتعلق باهتماماتهم، فالوقت الذي كان فيه المستخدمون على غير علم باستخدام بياناتهم الشخصية [1].

تم تقسيم هذا الفصل إلى مبحثين على النحو الآتي:

المبحث الأول: ماهية معالجة البيانات الشخصية.

المبحث الثاني: الآثار التي تترتَّب على المعالجة.

المبحث الأول
ماهية معالجة البيانات الشخصية

إن الحصول على بيانات المستخدمين يُمثِّل سمة العصر التقني، مقابل خدمات مجانية، أو شبه مجانية، فالمستخدم في الظاهر يعتقد أنه يستفيد من منصات إعلامية مجانية، لكنه في الحقيقة يدفع لمشغِّل الخدمة عن طريق إعطائه الحق في الوصول إلى بياناته الشخصية التي ستستخدمها فيما بعد بحرية، كما أنها تدرك القيمة الاقتصادية للبيانات الشخصية [2]، إن أغلب الدول ضمَّت ضمن قوانينها الخاصة بحماية البيانات الشخصية شروطا ومبادئ خاصة لمعالجة تلك البيانات، وبالتالي

---

(1) المعداوي، محمد احمد، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مرجع سابق، ص1935.

(2) الصالحين محمد، التنظيم القانوني لاستخدام البيانات الشخصية في الاعلام الجديد، كلية الحقوق، جامعة بن غازي، مجلة الحقوق، مجلد13، عدد2، ص13، available (on-line)، الوصف: التنظيم القانوني لاستخدام البيانات الشخصية في الإعلام الجديد(mandumah.com) تمت الزيارة الساعة 1 مساءً تاريخ 2022/8/2.

فأي مخالفة لتلك الشروط والمبادئ تُعدُّ انتهاكًا وتعدٍّ على البيانات، ويعتبر فعلًا غيرَ مشروع، فيترتَّب عليه العقوبات، فالمعالجة قُيِّدت بنص القانون، وذلك لضمان توفير الحماية لها.

وبناءً عليه، سيتم تقسيم هذا المبحث على النحو الآتي:

المطلب الأول: تعريف معالجة البيانات الشخصية.

المطلب الثاني: المبادئ العامة للمعالجة.

المطلب الأول
تعريف معالجة البيانات الشخصية

المعالجة بصفة عامة: هي تحويل شيء ما من صورته الطبيعية إلى صورة أخرى تعبِّر عن نتيجة ما يمكن الاستفادة منها [1].

المعالجة الإلكترونية للبيانات وفق المجال التقني: " مجموعة من العمليات المترابطة والمتسلسلة بدءًا من جمع المعطيات، وإدخالها إلى نظام المعالجة الآلية، وصولاً إلى تحليلها وإخراجها بصورة معلومات [2].

عرَّفت اللائحة الأوربية المعالجة كالآتي: تعني أي عملية أو مجموعة من العمليات التي يتم تنفيذها على البيانات الشخصية، أو على مجموعات من البيانات الشخصية، سواء كان ذلك بوسائل آلية أم لا؛ مثل الجمع، أو التسجيل، أو التنظيم، أو الهيكلة، أو التخزين، أو التكييف، أو التغيير، أو الاسترجاع، أو التشاور، أو الاستخدام، أو الكشف عن طريق الإرسال، أو النشر، أو الإتاحة، أو الموائمة، أو الدمج، أو التقييد، أو المحو، أو التدمير [3]".

---

(1) **رابحي** عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، مرجع سابق، ص 57.

(2) رابحي، عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، مرجع سابق، ص 57.

(3) General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu).

أما فيما يخص **المشرِّع الأردني** فعرَّفها في نص المادة الثانية من مسوَّدة قانون حماية البيانات الشخصية: "عملية واحدة أو أكثر يتم إجراؤها بأي شكل أو وسيلة؛ بهدف جمع البيانات، أو الاطلاع عليها، أو تسجيلها أو نسخها، أو حفظها، أو تخزينها، أو تنظيمها، أو تنقيحها، أو استغلالها، أو استعمالها، أو إرسالها، أو توزيعها، أو نشرها، أو ربطها ببيانات أخرى، أو إتاحتها، أو نقلها، أو عرضها، أو إخفاء هويتها، أو ترميمها، أو إتلافها".

عرَّف **المشرِّع الإماراتي** المعالجة:" بأنها أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية باستخدام أي وسيلة من الوسائل الإلكترونية، بما فيها وسيلة المعالجة، وغيرها من الوسائل الأخرى، وتمثِّل هذه العملية جمع البيانات الشخصية، وتخزينها، أو تسجيلها، أو تنظيمها، أو تكييفها، أو تعديلها، أو تداولها، أو تحويرها، أو استرجاعها، أو تبادلها، أو مشاركتها، أو استعمالها، أو توصيفها، أو الإفصاح عنها عن طريق بثِّها، أو نقلها، أو توزيعها، أو إتاحتها، أو دمجها، أو تقييدها، أو حجبها، أو محوها، أو إتلافها، أو إنشاء نماذج لها".

وتضمَّن القانون الإماراتي المادة الأولى من قانون حماية البيانات الشخصية منه على تعريف آخر للمعالجة في ذات القانون، وهو المعالجة المؤتمنة:" المعالجة التي تتم باستخدام برنامج أو نظام إلكتروني يعمل بطريقة آلية وتلقائية؛ إما بشكل مستقل كليا دون أي تدخُّل بشري، أو بشكل جزئي بإشراف وتدخُّل بشري محدود".

وعرَّف **المشرِّع البحريني** المعالجة في نص المادة الأولى: "أية عملية أو مجموعة عمليات يتم إجراؤها على بيانات شخصية بوسيلة آلية أو غير آلية، ومن ذلك جمع تلك البيانات، أو تسجيلها، أو نقلها، أو إتاحتها للغير، أو دمجها، أو حجبها، أو مسحها، أو تدميرها [1]".

---

(1) قانون حماية البيانات الشخصية البحريني رقم 30 لسنة 2018.

كما عرف المشرع القطري المعالجة في نص المادة الأولى من قانون حماية البيانات الشخصية:" إجراء عملية أو مجموعة عمليات على البيانات الشخصية، كالجمع والاستلام والتسجيل والتنظيم والتخزين والتهيئة والتعديل والاسترجاع والاستخدام والإفشاء والنشر والنقل والحجب والتخلص والمحو والإلغاء".

كما عرَّفتها اللائحة العامة لحماية البيانات (GDPR) في **المادة الرابعة** منها: "**المعالجة**" تعني أي عملية أو مجموعة من العمليات التي يتم تنفيذها على البيانات الشخصية، أو على مجموعات من البيانات الشخصية، سواء كان ذلك بوسائل آلية أم لا، مثل الجمع، أو التسجيل، أو التنظيم، أو الهيكلة، أو التخزين، أو التكييف، أو التغيير، أو الاسترجاع، أو التشاور، أو الاستخدام، أو الكشف عن طريق الإرسال، أو النشر، أو الإتاحة، أو الموائمة، أو الدمج، أو التقييد، أو المحو، أو التدمير[1]".

ويبدو للمتأمِّل في التعاريف السابقة أن أمر المعالجة يندرج تحته العديد من العناصر المكونة له، وأغلب القوانين نصَّت عليها في صلب القانون، وذلك يجسِّد أهمية وخطورة معالجة بيانات الأشخاص، فبياناتهم عرضة للنشر، والنقل، والإتلاف ...الخ، وتلك السلوكيات تناقض مبدأ الخصوصية، وتتجاوز الحدود الشخصية التي من حق الأفراد عدم الاقتراب منها.

---

(1) General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu) تمت زيارة الموقع الساعة الثالثة مساءً تاريخ 24/ 8/2022.

المطلب الثاني
المبادئ العامة في المعالجة

إن منظمة التعاون الاقتصادي والتنمية **(OECD)** أرست مبادئ حماية الخصوصية فيما يخص البيانات الشخصية، حيث اتخذت الحماية شكل قواعد إرشادية، حيث تمَّ تبنِّيها رسمياً من قبل مجلس المنظمة في أيلول 1980، ولا بدَّ من الإشارة إلى أنها لا تتخذ الصيغة الإلزامية، وتشمل الأشخاص الطبيعيين فقط، وتسري على القطاع العام والخاص. [1]

كما نصَّت اللائحة الأوربية **(GDPR)** على مبادئ معالجة البيانات الشخصية في المادة الخامسة منها على النحو الآتي:

- مشروعية المعالجة: بمعنى أن تتم بطريقة عادلة ومشروعة وبطريقة شفافة.
- تحديد الهدف من المعالجة: بمعنى أن يكون تجميعها ومعالجتها لأغراض محددة وصريحة.
- ملائمة ومحددة: بمعنى أن تقتصر المعالجة فيما يتعلق بغرض المعالجة فقط.
- الدقة: أن تكون البيانات دقيقة، مع التأكد من صحتها.
- قيود التخزين: يتم الاحتفاظ بها بشكل يسمح بتحديد هوية المعنيين بالبيانات لمدة أطول من اللازم؛ للأغراض التي تتم معالجة البيانات الشخصية من أجلها.
- الحماية من المعالجة غير المصرَّح بها وغير القانونية. [2]

---

(1) الشوابكة، محمد أمين، جرائم الحاسوب والانترنت، مرجع سابق، ص75.

(2) محمد أحمد سلامة مشعل، الحق في محو البيانات الشخصية، دراسة تحليلية في ضوء لائحة حماية البيانات الأوربية GDPR وأحكام المحاكم الأوربية، أستاذ في جامعة الزقازيق، بحث منشور ص37، available (on-line): الحق في محو البيانات الشخصية دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR وأحكام المحاكم الأوروبية سلامة مشعل (ekb.eg).

نصَّ المشرِّع الإماراتي في **(المادة الخامسة)** على أن معالجة البيانات الشخصية تتم ضمن ضوابط معنية، حيث نصت على أن المعالجة يجب أن تكون بطريقة عادلة، وشفافة، ومشروعة، وأن تكون جُمعت لغرض محدد وواضح، وألا يتم معالجتها بوقت لاحق على نحو يتعارض مع ذلك الغرض، إلا أنه يمكن معالجتها بوقت لاحق بشرط أن يكون غرض المعالجة مشابهًا للغرض الذي جُمِعت من أجله، وأيضا اشترط أن تكون البيانات كافية ومقتصرة على ما هو ضروري، وأن تكون صحيحة ودقيقة، ويجب أن تخضع للتحديث إذا لزم الامر، بالإضافة إلى ضمان توفير إجراءات لضمان محو، أو تصحيح البيانات غير الصحيحة، وأن تحفظ بشكل آمن يحميها من أي اختراق، أو انتهاك، أو معالجة غير مشروعة، وأخيرا يجب عدم الاحتفاظ بها بعد استنفاذ الغرض من معالجتها، ويمكن أن تبقى إذا تمَّ إخفاء هوية صاحب البيانات باستخدام خاصية آلية إخفاء الهوية[1].

أما **القانون البحريني** الخاص في حماية البيانات الشخصية في المادة الثالثة منه على النحو الآتي: أن تكون معالجتها منصفة ومشروعة، وأن تكون قد جُمعت لغرض محدد وواضح، وأن تكون كافية، وذات صلة، وصحيحة، ودقيقة، وتخضع لتحديث متى اقتضى الأمر ذلك، وألا تبقى بعد استنفاد الغرض من معالجتها؛ بصورة تسمح بمعرفة صاحب البيانات، ونصَّت أيضا على أن البيانات تُحفظ لمدة أطول؛ لأغراض تاريخية، أو إحصائية، أو للبحث العلمي؛ بشرط ألا تُنسب هذه البيانات إلى صاحبها [2].

كما نص المشرع القطري على ضوابط المعالجة في نص المادة الثالثة حيث نصت على ان لا يجوز معالجتها الا ضمن إطار الشفافية والأمانة واحترام كرامة الإنسان.

---

(1) قانون رقم 45 لسنة (2021)بشأن حماية البيانات الشخصية، دولة الامارات.

(2) قانون حماية البيانات الشخصية لمملكة البحريني رقم(30) لسنة 2018.

نصَّ **المشرِّع الأردني** في مسوِّدة حماية البيانات الشخصية على نوعين من الضوابط، أو ما ذكره في المسوَّدة بالاشتراطات العامة، والخاصة، فنصَّ في المادة السابعة على الاشتراطات العامة كالاتي:

أ. أن يكون الغرض منها مشروعا، ومحدَّدا، وواضحا.

ب. أن تكون متفقة مع الأغراض التي تم جمع البيانات من أجلها.

ج. أن تتم بوسائل قانونية ومشروعة.

د. أن تستند إلى بيانات صحيحة ودقيقة ومحدثة.

هـ. ألا تؤدي إلى تحديد الشخص المعني بعد استنفاد الغرض منها.

و. ألا تؤدي إلى التسبب بضرر للشخص المعني، أو تنال من حقوقه بشكل مباشر، أو غير مباشر.

ز. أن تتم بطريقة تضمن سرية المعلومات، وسلامتها وعدم حدوث أي تغيير عليها [1].

ونص في **المادة الثامنة** على الاشتراطات الخاصة على النحو التالي:

أ. يحظر القيام بمعالجة البيانات الشخصية دون موافقة صاحبها، ما لم تكن المعالجة ضرورية؛ لأي مما يأتي:

1. تنفيذ عقد يكون الشخص المعني بالمعالجة طرفا فيه.
2. اتخاذ خطوات بناء على طلب الشخص المعني بالمعالجة بهدف إبرام عقد.
3. تنفيذ التزام يرتبه القانون، خلافا لالتزام عقدي، أو صدور أمر من محكمة مختصة.
4. حماية المصالح الحيوية للشخص المعني بالمعالجة.

ب. لا يجوز أن تتجاوز معالجة البيانات الشخصية الغرض الذي جُمعت من أجله، والمحدَّد عند أخذ موافقة الشخص المعني بالمعالجة على النحو المبين في هذا القانون.

---

(1) المادة السابعة، من مشروع قانون حماية البيانات الشخصية لسنة 2022.

ج. مع عدم الإخلال بالأحكام الواردة في القوانين التي تُلزم المسؤول عن المعالجة بالاحتفاظ بالبيانات الشخصية التي في عهدته لمدة زمنية محددة، فلا يجوز الاحتفاظ بالبيانات في عهدة المسؤول عن المعالجة لمدة تتجاوز تاريخ انتهاء إجراء أي معالجة عليها.

د. لا يجوز إجراء أي معالجة للبيانات الشخصية لمن لا يتمتع بالأهلية الكاملة دون الحصول على موافقة أحد الوالدين الخطية أو الإلكترونية، وفي حال غياب الوالدين لأي سبب من الأسباب فيتم أخذ موافقة الولي المعيَّن قانوناً لمتابعة شؤونه".

ويتضح مما سبق أن الضوابط التي تحكم معالجة البيانات الشخصية يُمكن تلخيصها كالآتي: بأنه يجب أن تُعالَج البيانات بطريقة مشروعة، وذلك يعني أن يتم أخذ إذن صاحب البيانات وأن تكون البيانات واضحة، بحيث لا تحتمل التأويل، وصريحة، ومحدَّدة، وأن تتم المعالجة وفق الغرض الذي نُظِّمت من أجله، وبالتالي أي معالجة تُخالف الغرض تُعتبر انتهاكًا لخصوصية البيانات الشخصية، كما أنَّ المشرِّع الأردني في مشروع قانون حماية البيانات اشترط موافقة أحد الوالدين، أو الولي القانوني للشخص الذي لا يتمتع بالأهلية، أيضا يجب أن تكون ملائمة فلا يتم جمع بيانات لا حاجة لها في الهدف من المعالجة، والالتزام بمدة حفظ البيانات فعند الانتهاء من الغاية من المعالجة يجب محوها، أو إتلافها.

كما أنه لا بدَّ من الإشارة إلى أنه تختلف مدة الاحتفاظ بالبيانات من حيث الزمنُ بتحقيق الهدف منها في كل مرة؛ وذلك لأنه ليس كل مرة يمكن تحديد وقت الاستنفاذ منها لغاية إتلافها، ومثال على ذلك؛ انحلال الشركة، أو إفلاسها، فلا يمكن إتلاف البيانات الشخصية لمديريها، إذ قد يكونون في حاجة لها لحماية مصالح الشركاء، أو المساهمين، أو أصحاب العقود، فالبيانات قد تكون وسيلة لإثبات عقود، أو التزامات، أو علاقة عمل لا يمكن إتلافها [1].

---

(1) الأشقر، منى جبور، جبور، محمود، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الافراد، مرجع سابق، ص12.

المبحث الثاني
الآثار التي تترتب على معالجة البيانات الشخصية

إن فكرة المعالجة غير المشروعة للبيانات الشخصية تقوم على مسألة الاعتداء على حق الأفراد الذين من حقوقهم أن تُعالَج ضمن ضوابط قانونية[1]، واستجابة لذلك سعت التشريعات الأجنبية والعربية لسنِّ قوانين تُنظّم معالجة تلك البيانات على وجه يحفظ حق الأفراد بعدم انتهاكها؛ فالقانون البحريني والإماراتي، وكذلك اللائحة الأوربية تضمَّنت إجراءات المعالجة، وحقوق المعنيين بالمعالجة، والتزامات المسؤول عن المعالجة، فتلك هي الآثار التي تترتَّب على المعالجة.

وبناءً على ما سبق سيتم تقسيم هذا المبحث إلى مطلبين على النحو الآتي:

المطلب الأول: حقوق الشخص المعني بمعالجة البيانات الشخصية

المطلب الثاني: التزامات الشخص المسؤول عن المعالجة.

المطلب الأول
حقوق الشخص المعني بمعالجة البيانات الشخصية

إن معالجة البيانات يجب أن تتم بصورة دقيقة تحفظ حقوق الشخص المعني في المعالجة، بناءً عليه عزَّزت اللائحة العامة لحماية البيانات **(GDPR)**، فأوجدت حقوقًا للفرد يمارسها في حال خضعت بياناته للمعالجة، فله الحق أن يوافق بشكل صريح وواضح، والحق في نقلها ونسيانها أو محوها.

الفرع الأول: الحق في الموافقة

يحق للمستخدم الموافقة الصريحة والواضحة على السماح للشركة بالتصرف في بياناته الخاصة، عكس ما كان عليه الأمر في السابق، إذ كانت الشركات تكتفي بسكوت المستخدم، وعدم تحرُّكه لتعديل الخصائص الخاصة ببياناته [2].

---

(1) الدهبي خدوجة، مرجع سابق، ص144 وص 150.

(2) نص المادة الرابعة، قانون حماية البيانات الشخصية لدولة قطر، رقم 13، لسنة 2016.

ونصَّ المشرِّع القطري في المادة الرابعة على الحق في موافقة الشخص المعني بالمعالجة، فلا يجوز أن تتمَّ معالجة بياناته دون الحصول على موافقة الفرد مالم تكن المعالجة ضرورية؛ لتحقيق غرض مشروع للمراقب، أو الغير الذي تُرسل إليه البيانات.

وأشار المشرِّع البحريني في قانون حماية البيانات الشخصية في نص المادة الرابعة على الحق في موافقة الشخص المعني في المعالجة، وأورد حالات مستثناة من هذا الحق على النحو التالي:

- أن تكون المعالجة للمصلحة العامة.
- أن تكون المعالجة مرتبطة ببيانات شخصية أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات.
- أن تكون المعالجة ضرورية لإجراءات المطالبة بالحقوق والدعاوى القانونية، أو تتعلَّق بالإجراءات القضائية، أو الأمنية.
- أن تكون المعالجة لحماية الصحة العامة.
- أن تكون المعالجة لأغراض أرشيفية، أو تاريخية، أو إحصائية، أو دراسات علمية.
- أن تكون ضرورية لحماية صاحب البيانات.
- أن تكون ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه [1].

كما أن قانون حماية البيانات الشخصية لمملكة **البحرين** نصَّ على الحق في الموافقة في نص المادة (24)، حيث إنها نصَّت على بعض الشروط للاعتداد بموافقة صاحب البيانات على النحو التالي:

- أن تكون صادرة عن شخص كامل الاهلية.

---

(1) المادة الرابعة من قانون حماية البيانات الشخصية الاماراتي لسنة 2021.

- أن تكون مكتوبة وصريحة وواضحة ومحددة بمعالجة بيانات معينة.
- أن تكون صادرة بناءً على إرادته الحرة بعد إحاطته تماماً بغرض أو أغراض معالجة البيانات، وإحاطته عند الاقتضاء بالعواقب التي تترتَّب على عدم موافقته.
- ونصت في الفقرة الثانية منها على انه إذا كان الشخص ناقص الأهلية أو عديمها، فيعتد بموافقة الولي أو الوصي او القيم في حدود القانون، وذلك وفقاً للشروط في الفقرة الأولى من هذه المادة، ولم يكتفي المشرع بتلك الشروط السابقة أنما أعطى الحق في الفقرة الثالثة لصاحب البيانات في أن يسحب موافقته بموجب أخطار يقدمه لمدير البيانات.

وتجدر الإشارة إلى أن اللائحة الأوربية نصت على أن المعالجة القانونية للبيانات الشخصية للطفل عندما يكون عمر الطفل 16 عاما على الأقل، وبالتالي إذا كانت اقل من ذلك تعتبر المعالجة غير قانونية، الا إذا ادن بها صاحب المسؤولية الأبوية عن الطفل، كما أجازت اللائحة للدول الأعضاء أن تنص بقانون على سن أدنى بشرط إلا يقل سن الطفل عن 13 سنة. [1]

أما في مسوَّدة القانون في **التشريع الأردني** ذكرت حقوق الشخص المعني في المعالجة في الفصل الرابع من المادة (14) حتى المادة (20)، حيث تنصُّ المادة الرابعة عشرة من مسوَّدة قانون البيانات الشخصية على ما يلي:

(1) المادة الثامنة من اللائحة العامة لحماية البيانات الشخصية الأوربية.

ففي **المادة 14** [1] نصَّت على حق الشخص المعني في الموافقة المسبقة، وأن تكون صريحة وواضحة لا تحمل التأويل، سواء كانت خطية أو إلكترونية، وأن تكون محددة من حيث المدة، والغاية؛ لأن في كل مرة تتغير طبيعة ونوع المعالجة، وإن لم يجدِّد موافقته في كل مرة تعتبر ملغاة، كما أن أي موافقة تصدر بسبب ممارسة خادعة، أو غير صحيحة لا تعتبر موافقة ولا يعتدُّ بها.

وكما هو معلوم فإن لكل قاعدة استثناء، حيث ورد في نص المادة الخامسة عشرة بعض الاستثناءات على حق المعني بالمعالجة:

- يجوز مباشرة معالجة البيانات الشخصية دون الحصول على الموافقة الصريحة، والموثَّقة للشخص المعني بالمعالجة، في الحالات التالية:

أ. إذا كانت ضرورية؛ لغرض منع، أو كشف جريمة بناء على قرار قضائي، أو أمر من المدعي العام يهدف إلى منع أو كشف أو متابعة الجرائم المرتكبة خلافًا لأحكام القانون.

ب. إذا كانت مطلوبة، أو مصرحًا بموجب أيٍّ من التشريعات السارية، أو تنفيذا لها، أو كان ذلك بقرار من المحكمة المختصة.

---

(1) تنص المادة الرابع عشر من مسودة قانون البيانات الشخصية على ما يلي:1-الحق في الموافقة المسبقة

أ. لكل شخص الحق في حماية خصوصية بياناته الشخصية ولا يجوز معالجة تلك البيانات إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان ولا يجوز لأي مسؤول عن المعالجة القيام بمعالجة البيانات الشخصية دون الحصول على الموافقة المسبقة الصريحة والموثقة خطيًا أو إلكترونيًا للشخص المعني بالمعالجة، وتعتبر الشروط الواردة في هذه المادة هي المعتمدة لأغراض هذا القانون أينما وردت.

ب. يجب أن يكون طلب الموافقة على أي معالجة للبيانات الشخصية بلغة واضحة وبسيطة وغير مضللة ويمكن الوصول إليه بسهولة.

ج. يجب أن تحدد الموافقة من حيث المدة والغاية وأن يطلب المسؤول عن المعالجة موافقة الشخص المعني بمعالجة بياناته الشخصية في كل مرة تتغير طبيعة ونوع المعالجة التي تجرى على البيانات الشخصية أو أهدافها وفي حال لم يجدد الشخص المعني بمعالجة بياناته الشخصية موافقته صراحة تعتبر الموافقة ملغاة.

لا يعتد بأي موافقة صادرة عن الشخص المعني بمعالجة بياناته الشخصية إذا صدرت عنه استنادًا إلى معلومات غير صحيحة أو ممارسات خادعة أو مضللة وكانت هي السبب في قراره بمنح الموافقة المذكورة.

ج. إذا كانت ضرورية؛ لحماية مصالح الشخص المعني بمعالجة بياناته الشخصية المرتبطة بالحياة، أو الموت، أو مصالحه الحيوية، وبما لا يخالف أحكام هذا القانون.

د. إذا كانت البيانات الشخصية المراد الحصول عليها، أو مباشرة أي معالجة عليها متاحا وصول الجمهور إليها.

الفرع الثاني: الحق في النقل

أقرَّت اللائحة الأوربية العامة حق المستخدمين في نقل بياناتهم من وحدة تحكم إلى وحدة تحكم أخرى، وذلك في نص المادة 20 منها[1]، وكذلك المشرِّع الإماراتي في قانون حماية البيانات ذات الطابع الشخصي، ونص في المادة الرابعة عشرة على الحق في طلب نقل البيانات الشخصية، حيث يحق لصاحب البيانات نقلها لمتحكِّم آخر متى كان ذلك ممكناً من الناحية التقنية.

كما نصَّت المادة 22 من قانون حماية البيانات الشخصية **الإماراتي** على نقل ومشاركة البيانات الشخصية عبر الحدود؛ لأغراض المعالجة في حال وجود مستوى حماية ملائم، حيث أجازت هذه المادة نقل البيانات الشخصية من المكتب بحالتين،

أولا: أن تكون الدولة أو الإقليم الذي سيتم نقل البيانات إليها لديها تشريعات خاصة بحماية البيانات الشخصية.

ثانيا: انضمام الدولة إلى الاتفاقيات الثنائية، أو متعددة الأطراف المتعلقة بحماية البيانات الشخصية مع الدول التي سيتم نقل البيانات اليها [2].

---

(1) اللائحة العامة الأوربية من حماية البيانات الشخصية GPDR, General Data Protection Regulation – (GDPR) – Official Legal Text (gdpr-info.eu)

(2) المادة 22، قانون حماية البيانات الشخصية الاماراتي لسنة 2021.

لم يكتف المشرِّع الإماراتي بذلك، وإنما نص أيضا على نقل ومشاركة البيانات الشخصية عبر الحدود؛ لأغراض المعالجة في حال عدم وجود مستوى حماية ملائم، وأورد بعض الحالات استثناءً على ما ورد في المادة 22، حيث أجاز نقل البيانات إلى دول لا تتوفر فيها الحماية القانونية بشرط أن تكون بموجب عقد، أو اتفاقية تُلزِم المنشأة في تلك الدول بتطبيق الاشتراطات، والضوابط الموجودة في قانون حماية البيانات الشخصية الإماراتي.

نص قانون حماية البيانات الشخصية البحريني على الحق في النقل في نص المادة 12 على النحو الاتي:" أنْ يكون النقل إلى بلد أو إقليم مدرج في كشف تتولى الهيئة إعداده وتحديثه يتضمن أسماء البلدان والأقاليم التي تقدِّر الهيئة أنَّ لديها تشريعات أو أنظمة معمولاً بها تكفل مستوى كافياً من الحماية للبيانات الشخصية، ويُنشَر هذا الكشف في الجريدة الرسمية.

أنْ يكون النقل بتصريح يصدر من الهيئة في كل حالة على حدة، وذلك إذا قدَّرت أنَّ البيانات سوف يتوافر لها مستوى كافٍ من الحماية، ويكون تقدير الهيئة بمراعاة كافة الظروف المحيطة بعملية نقل البيانات، وبوجه خاص ما يأتي:

- طبيعة البيانات المطلوب نقْلُها، والغرض من معالجتها ومدة المعالجة.
- البلد أو الإقليم مصدر هذه البيانات والوجهة النهائية لها، وما يتوافر في تلك البلدان أو الأقاليم من تدابير لحماية البيانات الشخصية.
- الاتفاقيات الدولية والتشريعات ذات العلاقة المعمول بها لدى البلد أو الإقليم الذي سوف تُنقَل إليه البيانات.

ويجوز أنْ يكون التصريح المشار إليه مشروطاً أو لفترة زمنية محدَّدة"، ثم جاءت المادة 13 من ذات القانون وأوردت بعض الاستثناءات على حق النقل إذا كان نقل البيانات خارج المملكة الى بلد أو إقليم لا يوفر مستوى كافياً من الحماية للبيانات في أي من الحالات التالية:

- إذا وافق صاحب البيانات.
- إذا كان النقل لبيانات مستخرجة من سجل تم إنشاؤه وفقاً للقانون بغرض توفير معلومات للجمهور سواء كان هذا الاطلاع متاح للكافة او مقصور على ذوي المصلحة وفقا لشروط معينة.
- تنفيذ أو ابرام عقد بين صاحب البيانات ومدير البيانات.
- تنفيذ للالتزام يرتبه القانون، خلافا لالتزام عقدي، أو صدور امر من محكمة مختصة او النيابة العامة او قاضي التحقيق او النيابة العسكرية.
- اعداد أو مباشرة مطالبة قانونية أو الدفاع عنها.

كما أشار المشرع القطري على انه يحظر على المراقب اتخاذ أي أجراء او قرار من شأنه الحد من تدفق البيانات الشخصية عبر الحدود واستثنى المعالجة التي تخالف أحكام القانون، وذلك يعني الاعتراف بحق نقل البيانات الشخصية بشرط الا تكون المعالجة مخالفة ومن شأنها الاضرار بالبيانات الشخصية أو بخصوصية الفرد. [1]

ونصت المادة 44 من اللائحة العامة الأوربية على انه:" لا يتم أي نقل للبيانات الشخصية التي تخضع للمعالجة أو المعدة للمعالجة بعد نقلها إلى بلد ثالث أو إلى منظمة دولية إلا إذا تم الامتثال

(1) نص المادة 15، قانون حماية البيانات الشخصية القطري رقم 13 لسنة 2016.

للشروط المنصوص عليها في اللائحة من قبل المراقب المالي والمعالج، بما في ذلك النقل اللاحق للبيانات الشخصية من بلد ثالث أو منظمة دولية إلى بلد ثالث آخر أو الى منظمة دولية ".

كما نصَّ المشرِّع الأردني في مسوَّدة حماية البيانات الشخصية على الحق في النقل في المادة (19) على النحو الآتي:

للشخص المعني بالمعالجة الحق في نقل نسخة من بياناته الشخصية من مسؤول عن المعالجة إلى مسؤول آخر، وليس لأي مسؤول عن المعالجة أن يعارض ذلك النقل وذلك وفقًا للأحكام الواردة في المادة (21) من المسودة.

وعليه، نصت المادة (21) نصت على احكام نقل وتبادل البيانات الشخصية داخل المملكة حيث حظرت نقل البيانات بأي حال من الأحوال بين الشخص المسؤول عن المعالجة.

المادة (21) من مسوَّدة قانون حماية البيانات الشخصية نصَّت على أحكام نقل وتبادل البيانات الشخصية داخل المملكة، حيث حظرت نقل البيانات بأي حال من الأحوال بين الشخص المسؤول عن المعالجة وأي شخص آخر داخل المملكة إلا بموافقة صاحب البيانات، وبشرط أن يحقق النقل مصالح مشروعة للجهة التي تتوفر لديها البيانات ومتلَقِّي البيانات الشخصية، وأن يتوفر لدى الشخص المسؤول عن المعالجة العلم الكافي بالجهة التي ستتلقَّى البيانات الشخصية، والغاية من استخدامها للبيانات، بالإضافة إلى أنه يقع على عاتق الشخص المسؤول عن المعالجة توثيق البيانات التي تم نقلها، أو تبادلها، والغاية من تبادلها وتوثيق موافقات الأشخاص على نقلها، ولا يجوز للمسؤول عن المعالجة تبادل أو نقل أو إتاحة البيانات الشخصية لأي شخص آخر إذا كانت الغاية من ذلك تسويق لمنتجات أو خدمات إلا بموافقة الشخص المعني.

أما فيما يخص أحكام نقل البيانات الشخصية إلى خارج المملكة فقد نصت عليه المادة (22) من مسودة القانون الأردني: أنه لا يجوز نقل أيٍّ من البيانات الشخصية خارج المملكة إلى أي شخص لا يتوافر لديه مستويات كافية من حماية البيانات الشخصية، ولا يعتبر مستوى الحماية كافيًا إذا كان أقلَّ مما يقرِّره هذا القانون من أحكام لحماية البيانات الشخصية.

ويرى الباحث أن أغلبية الدول تضمنت في قوانينها الخاصة بحماية البيانات الشخصية نوعين لنقل البيانات الشخصية، نقل داخلي ضمن الدولة نفسها، ونقل خارجي عابر لحدود الدولة لدولة أخرى، فبعض التشريعات اشترط لنقل البيانات خارج الحدود هو وجود مستوى حماية ملائم للدولة التي سيتم نقل البيانات اليها.

الفرع الثالث: الحق في المحو أو النسيان

لقد تمَّ النص على هذا الحق في فرنسا في أواخر السبعينات من القرن الماضي، فهي أول دولة أوربية تناولت تشريعاتها الحديث عن الحق في النسيان (DROITALOUBLI)، وأن هذا المصطلح لم يكن له ترجمة إنجليزية صحيحة، فمرة يُترجَم على أنه الحق في المحوّ، ومرة أخرى الحق في النسيان، وفي عام 2010 أصدرت فرنسا تشريع خاص بتطبيق الحق في النسيان، أو حق المحو، وقد عمدت اللائحة الأوروبية الأخيرة إلى تقنين مبدأ سبق لإحدى المحاكم الأوروبية أن أقرَّته سنة 2014، وأجبرت من خلاله شركة غوغل على منح المستخدمين الأوروبيين الحق في مسح أية معلومات، أو روابط لا يرغبون في أن ترتبط بأسمائهم في الفضاء الرقمي[1].

(1) محمد سلامة مشعل، مرجع سابق، ص 44 وص 46.

إن القوانين الخاصة بحماية البيانات الشخصية في العديد من الدول استخدمت مصطلح الإتلاف، والمحو، والنسيان، وإخفاء الهوية، وبنظر الباحث إن كلَّ هذه المصطلحات هدفها الرئيس حماية البيانات الشخصية، والرغبة في كونها لم توجد، فالمشرِّع الإماراتي استخدم مصطلح الحق بالإتلاف، في المقابل المشرِّع الأردني استخدم مصطلح النسيان في مسوَّدة حماية البيانات أخذت بهذا الحق في نص المادة (20) منه، فأورد عدة أسباب للحق في النسيان وإخفاء الهوية:

1- إذا تمَّت معالجة البيانات الشخصية بشكل، أو لغرض غير الذي جمعت من أجله.

2- إذا سحب الشخص المعني بالمعالجة الموافقة التي كانت تستند إليها المعالجة.

3- إذا خضعت البيانات الشخصية لمعالجة غير مشروعة.

4- إذا كان من الضروري محو البيانات الشخصية لتنفيذ التزام قانوني، أو تعاقدي محمول على المسؤول عن المعالجة، أو لانقضائه.

ب- مع عدم الإخلال بالأحكام الواردة في هذه المادة، يلتزم المسؤول عن المعالجة عندما يتلقى طلب محو البيانات الشخصية أن يتخذ التدابير اللازمة، بما في ذلك التدابير الفنية لمحو البيانات الشخصية التي يعالجها، أو إخفاء هوية أصحابها[1].

عرَّف المشرِّع في مسوَّدة قانون حماية البيانات الشخصية الأردني في المادة الثانية الحق في النسيان، فحق النسيان: هو تمكين الشخص المعني بالمعالجة من محو بياناته الشخصية أو إخفائها.

لقد كان لحكم محكمة العدل الأوربية في قضية (Google Spiainc) (12/313) في 13 مايو 2014 دورٌ هامٌ في الاعتراف بالحق في المحو على مستوى الاتحاد الأوربي، حيث يعتبر أول

(1) (المادة 20)، مسودة قانون حماية البيانات الشخصية الأردني لعام 2022.

حكم قضائياً بالحق في المحو، وبسبب هذا الحكم شهدت الساحة الأوربية والأمريكية الكثير من النقاشات حول الاستجابة لطلب المستخدم بحذف معلومات تتعلَّق به بحيث لا يمكن الوصول إليها مرة أخرى، وكان الجدل حول طبيعة الحق بالمحو، وهل الاعتراف فيه انتهاك لحرية التعبير، وانتهاك للحق بالوصول إلى المعلومة أم أنه مظهر من مظاهر الخصوصية، وسيطرة الشخص على بياناته، حيث تمَّ انتقاد الحكم من قبل الولايات المتحدة الامريكية، وذلك لأنها تمنح أهمية كبيرة لحرية التعبير، والحق في الوصول إلى المعلومات، وأنها لا تهتم بشأن الخصوصية بقدر الاتحاد الأوربي، وهذا يعني أن الحق في المحو ليس مطلقاً، وله ضوابط معينة؛ لأنه يتعارض مع حقوق أخرى؛ مثل الحق في حرية التعبير، والوصول الى المعلومة.

إن الدول الأوربية تناولت هذا الحق أو ما يسمى بحق (النسيان)، ففي فرنسا جاء النص على هذا الحق في نص المادة (40) من قانون المعلوماتية والحرية الصادر عام1978،فمرة يُترجم على أنه الحق في النسيان، وتارة يُترجم الحق في المحو، وفي عام 2010 تم تقديم تشريع تمَّت تسميته (ميثاق الحق بالنسيان) ،أما في بريطانيا فكان أول قرار لها بالحق في المحو عام 2004، حيث يسعى الاتحاد الأوربي في لائحة حماية البيانات إلى وضع تنظيم قانوني، يشمل حق المحو، والاستثناءات التي ترد عليه، والحالات التي تنطبق عليه من خلال نص المادة (17) ، بحيث أصبح بإمكان مستخدمي الإنترنت داخل الاتحاد الأوروبي طلب مسح بياناتهم الشخصية [1]، وذلك ما جاء في نص المادة الخامسة عشرة في قانون حماية البيانات الإماراتي التي أعطت الشخص المعني الحق في محو أو تصحيح بياناته، بالإضافة إلى تقييد أو إيقاف المعالجة، أما المشرِّع السعودي لم يستخدم

(1) محمد أحمد سلامة مشعل، الحق في محو البيانات الشخصية، مرجع سابق، ص1، ص4، ص 38، ص44، ص51.

مصطلح المحو إنما استخدم مصطلح إتلاف البيانات في المادة الثامنة عشرة في الفقرة الأولى منها على النحو الاتي:

1. على جهة التحكم إتلاف البيانات الشخصية فور انتهاء الغرض من جمعها، ومع ذلك، يجوز لها الاحتفاظ بتلك البيانات بعد انتهاء الغرض من جمعها إذا تمت إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد، وفق الضوابط التي تحدِّدها اللوائح.
2. على جهة التحكم الاحتفاظ بالبيانات الشخصية حتى بعد انتهاء الغرض من جمعها في الحالتين الآتيتين:

- إذا توافر مسوغ نظامي يوجب الاحتفاظ بها مدة محددة، وفي هذه الحالة يجرى اتلافها بعد انتهاء هذه المدة، أو انتهاء الغرض من جمعها، أيهما أطول.
- إذا كانت البيانات الشخصية متصلة اتصالا وثيقا بقضية منظورة أمام جهة قضائية، وكان الاحتفاظ بها مطلوبا لهذا الغرض، وفي هذه الحالة يجرى إتلافها بعد استكمال الإجراءات القضائية الخاصة بالقضية.

نصَّ قانون حماية البيانات الشخصية البحريني في المادة (23)على الحق في المطالبة بالتصحيح والحجب والمسح، حيث إنه أجاز لكل صاحب بيانات أن يتقدَّم لمدير البيانات بطلب مشفوع بما يثبت هُويته؛ لتصحيح أو حجب أو مسح البيانات، وذلك حسب الحال، فإذا كانت معالجتها تتم خلافا لأحكام القانون، أو كانت البيانات غير صحيحة، أو ناقصة، أو محدثة، أو كانت المعالجة غير مشروعة، وعلى مدير البيانات الاستجابة للطلب دون مقابل، وذلك خلال عشرة أيام عمل من تاريخ تسلُّم الطلب، ثم جاء في الفقرة الثانية واستثنى أيَّ سجل متاح للجمهور الاطلاع عليه، وفي الفقرة الثالثة نص على أنه لا يجوز معالجة البيانات التي يتم حجبها؛ استنادا لأحكام الفقرة الأولى إلا

بموافقة صاحب البيانات، أو لغرض الإثبات، أو لحماية حقوق طرف ثالث، وكما أنها نصت المادة في الفقرة الخامسة على أنه على مدير البيانات خلال خمسة عشر يومًا من تاريخ استجابته كليا، أو جزئيا للطلب إخطار أي طرف ثالث أفصح له عن تلك البيانات عن التصحيح، أو المسح، أو الحجب الذي تم نتيجة طلب صاحب البيانات، ما لم يكن ذلك متعذرا، أو لا يمكن تحقيقه.

ونصت المادة 3/5 من قانون حماية البيانات الشخصية القطري على الحق في حذف البيانات أو محوها في حال قام صاحب البيانات بسحب موافقته السابقة على المعالجة أو في حال الاعتراض على المعالجة أن كانت غير ضرورية أو كانت زائدة عن متطلباتها أو مخالفة قانونا أو عند انتهاء الغرض الذي تمت من أجله المعالجة.

ومثال على الحق في المحو، بتاريخ 2019/09/11 قام السيد (ق) مارست A.A.A الحق في المحو (أن تنسى بياناته الشخصية)، فيما يتعلق بعنوان URL ضد .GOOGLE SPAIN, S.L واعتبر صاحب الشكوى الذي تظهر بياناته الشخصية في مقال إخباري من عام 2012، أن المعلومات الواردة في نتائج البحث قديمة، وعفا عليها الزمن وغير دقيقة، وأنه ليس لها أي تأثير على الحاضر، ولا صلة يمكن أن تسهم في النقاش العام.

وفي 2020/01/20، وافق مدير AEPD على قبول المطالبة المقدمة من المدَّعي ضد GOOGLE SPAIN، S.L، ووافق على نقل المطالبة إلى الأخيرة، مع إعطاء مهلة خمسة عشر يوم عمل لتقديم الادعاءات. وذكرت غوغل في ادِّعاءاتها أن صاحبة الشكوى مارست حقها في المحو، ولكن ادَّعاءاتها رُفضت لأسباب قانونية.

ثم أعيد النظر في الطلب، وتبين أن البيانات الشخصية لصاحب الشكوى لم تعد منشورة على الموقع المتنازع عليه، قام مشرف الموقع الإلكتروني المتنازع عليه بإخفاء هوية البيانات الشخصية

لصاحبة الشكوى عن طريق استبدال اسمها بالأحرف الأولى؛ ونتيجة لذلك لم يظهر عنوان URL المتنازع عليه بين نتائج بحث Google بعد الآن عند البحث عن اسمها [1].

المطلب الثاني
التزامات الشخص المسؤول عن المعالجة

لقد عرَّف المشرِّع الإماراتي في قانون حماية البيانات الشخصية المعالج، وذلك في نص المادة الأولى منه بأنه: "المنشأة أو الشخص الطبيعي الذي يعالج البيانات الشخصية نيابة عن المتحكِّم، بحيث يقوم بمعالجتها تحت توجيهه وفقاً لتعليماته".

أما المشرِّع البحريني فعرَّفه في نص المادة الأولى على النحو الآتي:" معالِج البيانات: الشخص الذي يتولى معالجة البيانات لحساب مدير البيانات ونيابة عنه، ولا يشمل ذلك كل مَن يعمل لدى مدير البيانات أو معالِج البيانات".

أما المادة (28) من **اللائحة الأوربية** نصَّت على: عندما تتم المعالجة نيابة عن وحدة التحكم، يجب على وحدة التحكم استخدام المعالجات فقط التي توفر ضمانات كافية لتنفيذ التدابير الفنية، والتنظيمية المناسبة؛ بطريقة تلبِّي المعالجة فيها متطلبات هذه اللائحة، وتضمن حماية حقوق موضوع البيانات. [2]

كما أنه لا يجوز للمعالج إشراك معالج آخر دون إذن كتابي محدَّد، أو عام مسبق من وحدة التحكم، ففي حالة التفويض الكتابي العام يجب على المعالج إبلاغ وحدة التحكم بأي تغييرات مقصودة

---

(1) https://gdprhub.eu/index.php?title=AEPD_-_N%C2%BA:_TD/00005/202: (on-line) available. 2022/8/23 تمت زيارة الموقع الساعة 3 مساءً تاريخ

(2) General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu) . تمت زيارة الموقع الساعة 3 مساءً تاريخ 2022/8/22.

تتعلق بإضافة أو استبدال معالجات أخرى، مما يمنح وحدة التحكم الفرصة للاعتراض على هذه التغييرات.

تخضع المعالجة من قبل المعالج لعقد، أو أيِّ إجراء قانوني آخر بموجب قانون الاتحاد، أو الدولة يكون العضو ملزِما للمعالج فيما يتعلق بوحدة التحكم، ويحدِّد موضوع المعالجة، ومدتها، وطبيعة المعالجة والغرض منها، ونوع البيانات الشخصية، وفئات أصحاب البيانات، والتزامات وحقوق وحدة التحكم. وينص ذلك العقد أو أي إجراء قانوني آخر– بوجه خاص– على أن المعالج:

1. يعالج البيانات الشخصية فقط بناءً على تعليمات موثَّقة من وحدة التحكم، بما في ذلك ما يتعلَّق بنقل البيانات الشخصية إلى بلد ثالث، أو منظمة دولية، ما لم يكن ذلك مطلوبا بموجب قانون الاتحاد أو الدولة العضو الذي يخضع له المعالج؛ في مثل هذه الحالة يجب على المعالج إبلاغ وحدة التحكم بهذا الشرط القانوني قبل المعالجة، ما لم يحظر هذا القانون هذه المعلومات؛ لأسباب مهمة تتعلق بالمصلحة العامة، يضمن أن الأشخاص المصرَّح لهم بمعالجة البيانات الشخصية قد ألزموا أنفسهم بالسرية، أو يخضعون لالتزام قانوني مناسب للسرية، مع مراعاة طبيعة المعالجة
2. يساعد وحدة التحكم من خلال التدابير التقنية والتنظيمية المناسبة، قدر الإمكان للوفاء بالتزام وحدة التحكم، بالاستجابة لطلبات ممارسة حقوق موضوع البيانات، بناء على اختيار وحدة التحكم.
3. حذف أو إرجاع جميع البيانات الشخصية إلى وحدة التحكم بعد انتهاء تقديم الخدمات المتعلقة بالمعالجة، وحذف النسخ الموجودة ما لم يتطلب قانون الاتحاد، أو الدولة العضو تخزين البيانات الشخصية.

4. يتيح للمراقب جميع المعلومات اللازمة لإثبات الامتثال للالتزامات المنصوص عليها في هذه المادة، والسماح بعمليات التدقيق، والمساهمة فيها، بما في ذلك عمليات التفتيش، التي يجريها المراقب المالي، أو مدقق حسابات آخر مفوَّض من قبل المراقب المالي.
5. يجب على المعالج إبلاغ وحدة التحكم على الفور إذا رأى أن التعليمات تنتهك هذه اللائحة، أو غيرها من أحكام حماية بيانات الاتحاد، أو الدولة العضو.

عندما يُشارك المعالج معالجا آخر؛ لتنفيذ أنشطة معالجة محدَّدة نيابة عن وحدة التحكم، تفرض نفس التزامات حماية البيانات المنصوص عليها في العقد، أو أي إجراء قانوني آخر بين وحدة التحكم والمعالج على ذلك المعالج الآخر، عن طريق عقد، أو أي إجراء قانوني آخر بموجب قانون الاتحاد، أو الدولة العضو على وجه الخصوص توفير ضمانات كافية؛ لتنفيذ التدابير الفنية والتنظيمية المناسبة؛ بطريقة تلبي المعالجة متطلبات هذه اللائحة. وفي حالة فشل هذا المعالج الآخر في الوفاء بالتزاماته المتعلقة بحماية البيانات، يظل المعالج الأولي مسؤولا مسؤولية كاملة تجاه وحدة التحكم عن أداء التزامات ذلك المعالج الآخر. [1]

نصَّ قانون حماية البيانات الشخصية البحريني على التزامات مدير البيانات، ففي المادة الثامنة نص على التزامه بأمان المعالجة بحيث يتخذ التدابير الفنية، والتنظيمية الكفيلة بحماية البيانات من الإتلاف غير المقصود، أو الفقد العرضي، وفي المادة التاسعة على سرية المعالجة، وعدم الإفصاح عن أية بيانات شخصية، ويلتزم بمعالجتها ضمن الحدود المشروعة.

نصت المادة 8 إلى المادة 15 من قانون حماية البيانات الشخصية القطري على التزامات المراقب والمعالج، حيث كان مضمون هذه المواد الالتزام بمعالجة البيانات الشخصية بأمانه وشفافية

(1) General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu).

ومشروعية وان تكون المعالجة ضمن الغرض المحدد والا تخرج عن الغاية من معالجتها، وان يقوم المعالج بإخطار صاحب البيانات بالمعالجة، واتخاذ كافة التدابير والاحتياطات عند معالجة البيانات الشخصية.

في نص المادة الثامنة من **القانون الإماراتي** نص على الالتزامات التي تقع على عاتق المعالج ومضمونها على النحو الآتي:

- يجب أن يلتزم بإجراءات المعالجة وفقا لتعليمات المتحكم، وفي نطاق موضوعها والغرض منها.
- يجب أن يقوم بتطبيق كافة الإجراءات الإدارية، والتدابير التقنية الملائمة لحماية البيانات.
- حماية البيانات سواء أثناء تحديد وسيلة المعالجة، أو أثناء المعالجة.
- يجب أن تكون إجراءات المعالجة وفق الغرض والمدة المحددات، وإن تجاوز المدة وجب عليه إخطار جهة التحكم، وأخذ الإذن بالتمديد.
- يلتزم بمحو البيانات بعد انقضاء الهدف من المعالجة.
- عدم القيام بأعمال من شأنها الإفصاح عن البيانات.
- الالتزام بتأمين عملية المعالجة وتأمين الأجهزة للوسائط الإلكترونية المستخدمة في عملية المعالجة.
- في حال اشترك أكثر من معالج في عملية المعالجة، وجب أن يكون هناك عقد مكتوب يحدِّد أدوارًا ومسؤولية كلٍّ منهم حول عملية المعالجة، وألَّا يعتبروا مسؤولين بالتضامن عن أي مسؤوليات، أو التزامات في القانون.

أما المشرع البحريني فقد نص على التزامات المعالج من خلال التزامه بإخطار صاحب البيانات بمعالجة بيانات شخصية خاصة به [1]، وإخطاره بأن له الحق في الاعتراض على استخدام بياناته لأغراض التسويق المباشر [2]، والتزامه بعدم معالجة البيانات الشخصية يعد الاعتراض على معالجتها، التي تلحق معالجتها ضرراً مادياً أو معنوياً [3].

وفيما يخص **التشريع الأردني** ذكر التزامات المعالج في مسوَّدة قانون حماية البيانات الشخصية في نص المادة الحادي عشر كما يلي:

"أن يكون المسؤول عن المعالجة ملزما بحماية البيانات الشخصية التي في عهدته، وعن تلك التي سُلِّمت إليه من قبل أي شخص آخر، وفقًا لأحكام هذا القانون.

ب- يلتزم المسؤول عن المعالجة بوضع سياسات، وإجراءات خاصة تتعلق بمعالجة البيانات الشخصية، وآلية تلقِّي الشكاوى بخصوصها، والرد عليها، وفقًا لأحكام هذا القانون، على أن يقوم بنشرها في وسائل الإعلام المتاحة، بما في ذلك الموقع الإلكتروني الخاص به.

ج- يلتزم المسؤول عن المعالجة بتوفير وسائل المساعدة البصرية والسمعية والحسية، وأي وسيلة أخرى مناسبة، تضمن تلبية احتياجات الشخص المعني بمعالجة بياناته الشخصية من ذوي الإعاقة في ممارسة حقوقهم.

د- يلتزم المسؤول عن المعالجة بتسمية مراقب حماية البيانات الشخصية [4]".

---

(1) المادة 18 قانون حماية البيانات الشخصية لمملكة البحرين.

(2) المادة 19 قانون حماية البيانات الشخصية لمملكة البحرين.

(3) المادة 21 قانون حماية البيانات الشخصية لمملكة البحرين.

(4) المادة 11 من مسودة قانون حماية البيانات الشخصية الأردني.

وبناءً على ما سبق فإن التزامات الشخص المسؤول عن المعالجة تكون بتأمين حماية للبيانات الشخصية باتخاذ كافة التدابير، والإجراءات في حدود نطاق الغرض من المعالجة، وفي المدة المحددة، وأن أغلب الدول حظرت أي فعل يقوم به المسؤول عن المعالجة، يخالف ما جاء من ضوابط شرعية للمعالجة، ويخالف ما جاء في الأُطر القانونية الخاصة في حماية البيانات الشخصية، فأي مخالفة تُعرِّضه للمسائلة القانونية، وفي هذا السياق كان المشرِّع الأردني على جانب من التميز بتضمينه في مسوَّدة القانون رعاية الأشخاص ذوي الإعاقة الذي يتيح لهم ممارسة حقهم في حفظ وحماية بياناتهم، وذلك في الفقرة الثالثة من المادة الحادي عشر، أما بالنسبة للمشرِّع الإماراتي فقد توسَّع أكثر في ذكره الاشتراك في المعالجة، ووضع قيدًا؛ بأنه يجب أن يكون الاشتراك بعقد مكتوب كتابةً، وإلا اعتُبر المشتركون مسؤولين بالتضامن عن أي إجراءٍ مخالفٍ، حيث إنه كان متوافقًا مع ما جاء في اللائحة الأوربية لحماية البيانات، كما نص على أنه يجب تأمين عملية المعالجة، والأجهزة التي تتم من خلالها المعالجة.

الفصل الرابع
الحماية الجزائية للبيانات الشخصية

إن الحياة الاجتماعية في الوقت الحالي محاطة بعدد من المخاطر نظراً للانتشار الواسع للمعطيات ذات الطابع الشخصي في مجال الرقمية [1]، فمجرد الاطلاع على تلك البيانات يتحقق انتهاكها لان من احد سماتها أن تبقى سرية وبعيدة عن أنظار الاخرين [2]، حيث أصبح بمجرد أن يقوم الشخص بتصفح الإنترنت تخزن معلوماته بشكل تلقائي وذلك من خلال تقنية تسمى بتقنية السحابية (**Cloud Storage**)، علاوة على أن الجهات المختصة بإنفاذ القانون أصبحت على اطلاع كامل على بيانات الأشخاص، وذلك بحكم صلاحياتها الوظيفية، فأصبحت تقوم باستخدام أجهزة تعقب عبر الهاتف، والمواقع الجغرافية للأشخاص المراد التجسُّس، والتنصت عليهم، ومثال على ذلك الشبكة المعروفة باسم (**Carnivore**)، والتي استخدمت للتنصت على مزوِّدي خدمة الإنترنت من قبل الحكومة الإلكترونية للتجسُّس على مزوِّدي خدمة الإنترنت؛ لمراقبة رسائل البريد الإلكترونية، ومراقبة الرسائل بين مشتركي الإنترنت، حيث كان المسؤول عن هذه الشبكة مكتب التحقيقات الفيدرالية في الولايات المتحدة الأمريكية[3]، ولم يقتصر الأمر على التجسس على مشتركي

---

(1) البحر، ممدوح خليل، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، ص11.

(2) الهيتي، محمد حماد مرهج، (2006)، جرائم الحاسوب، دراسة تحليلية، دار المناهج للنشر والتوزيع، ط1، الأردن ص106.

(3) الشوابكة، أمين، مرجع سابق، ص 66.

الأنترنت فحسب وطال التجسس المكالمات الهاتفية والمحادثات الشخصية، كما أن الأمر وصل إلى تعقُّب الأشخاص أثناء القيادة عبر تقنية **GPS/ ALPR** بدون صلاحية، أو الحصول على إذن[1].

فالانتهاكات التي تقع على البيانات الشخصية قد تكون من الفضوليين والمتطفلين، وتكون من السلطة المختصة بإنفاذ القوانين في الدولة، وقد يكون من الأشخاص الذين يدعون بالهاكرز، أو المجرم المعلوماتي، أو المسؤول عن المعالجة.

إن موافقة الأشخاص على جمع بياناتهم وتخزينها ومعالجتها لا يعني تركها دون حماية، ولا يعني حرية تداولها، ونقلها إلى الآخرين لتصبح علانية. [2]

وبناءً عليه، سيتم تقسيم هذا الفصل إلى مبحثين على النحو الآتي:

المبحث الأول: صور الجرائم الواقعة على البيانات الشخصية.

المبحث الثاني: الأساس القانوني لانعقاد المسؤولية الجزائية.

المبحث الأول
صور الجرائم الواقعة على البيانات الشخصية

إن الجرائم التي تقع على البيانات الشخصية هي أحد أنواع الجرائم المعلوماتية، حيث تعدَّدت الاتجاهات في تقسيم الجرائم المعلوماتية [3]، فاستخدام الحاسوب في جمع ومعالجة البيانات الشخصية المتصلة في حياتهم الخاصة إيجابيات متعددة لا يمكن لأحد إنكارها، سواء في الشؤون الاقتصادية

---

(1) أرجدال علي (2019)، حماية المعطيات الشخصية بالمغرب، دراسة تحليلية مقارنة، جامعة محمد الخامس، كلية العلوم القانونية، الرباط، رسالة لنيل دبلوم الماستر في القانون العام، available (on-line): حماية المعطيات الشخصية بالمغرب – دراسة تحليلية ومقارنة (droitarabic.com) PDF.

(2) الشوابكة امين، مرجع سابق، ص62.

(3) الحسيني عمار عباس، جرائم الحاسوب والأنترنت الجرائم المعلوماتية، مرجع سابق ص 98 وص99.

والاجتماعية والعلمية، وهذا أدَّى إلى وجود ما يسمَّى ببنوك البيانات، وعُرِّفت بأنها: " تكوين قاعدة بيانات تفيد موضوعاً معيناً، وتهدف لخدمة غرض معين ومعالجتها، بواسطة أجهزة الحاسبات الإلكترونية؛ لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض معينة [1] ".

إن وجود نظام في الدولة يستطيع الوصول إلى المعلومات المتصلة بالفرد في جهاز حاسوب مركزي، يمكنه من خلاله جمع عدد كبير من المعلومات؛ كالمعلومات الاجتماعية والصحية والمالية، فهي تجمع جميع بياناته الشخصية، وبالتالي يصبح الأفراد شبه عراة لا يتمتعون باي ستار يحمي حياتهم الخاصة، وذلك يعود لسرعة جمع ومعالجة وتبادل هذه البيانات، ويزداد الأمر خطورة عندما تفتقد الدولة لجهة تشرف على جمع ومعالجة هذه البيانات، فيقع على هذه البيانات العديد من الانتهاكات، وبالمقابل يقع على عاتق الدولة واجب حمايتها ومراقبتها. [2]

وبناءً عليه، سيتم تقسيم هذا المبحث إلى خمسة مطالب على النحو الآتي:

المطلب الأول: جريمة معالجة البيانات الشخصية دون ترخيص.

المطلب الثاني: جريمة الجمع والتخزين غير المشروع للبيانات الشخصية.

المطلب الثالث: جريمة الانحراف عن الغاية من المعالجة الإلكترونية للبيانات.

المطلب الرابع: جريمة الاحتفاظ بالبيانات الشخصية أكثر من المدة القانونية اللازمة.

المطلب الخامس: جريمة إفشاء البيانات الشخصية.

---

(1) أيوب، بولين انطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق، ص96.

(2) أيوب، بولين انطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق، ص 106.

المطلب الأول
جريمة معالجة البيانات الشخصية دون ترخيص

لقد تم الإشارة في هذه الدراسة على عدة حقوق تترتب للشخص في مواجهة المعالج الذي مهمته جمع البيانات لغاية معالجتها لغرض وغاية محددة ومن واجبه أن لا يقوم بجمع البيانات الشخصية ومعالجتها دون اخذ اذن أو موافقة صاحبها، فان قيامه بالمعالجة دون ترخيص يستوجب العقاب كونه خالف قواعد قانونية تقضي بعدم المعالجة دون إذن او ترخيص من صاحب الشأن.

تم تقسيم هذا المطلب إلى ثلاثة فروع على النحو الاتي:

الفرع الأول: الركن المادي.

الفرع الثاني: الركن المعنوي.

الفرع الثالث: الركن الشرعي.

الفرع الأول: الركن المادي

تقوم هذه الجريمة عند قيام الشخص المسؤول عن معالجة البيانات الشخصية بمعالجة البيانات دون ترخيص وفي غير الأحوال المنصوص عليها قانوناً، وتتم أيضاً بمعالجة البيانات بعد إلغاء الترخيص، أو بعد انتهاء مدته [1]، وبالتالي فإن الركن المادي يعتمد على سلوك المعالجة دون إذن، أو ترخيص من اللجنة المختصة، ويتحقق فعل المعالجة، سواء في إدخال البيانات، أو توزيعها، أو دمجها مع بيانات أخرى، أو تحليلها؛ لتعطي معلومة معينة ذات دلالة خاصة، وكل هذه الأنشطة تكون دون ترخيص من الجهة المختصة [2].

---

(1) احمد، حسن خالد، مرجع سابق ص 50.

(2) الحسيني عمار عباس، جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، مرجع سابق، ص239.

الفرع الثاني: الركن المعنوي

يجب أن يتوافر في هذه الجريمة القصد الجنائي العام الذي يقوم على عنصري العلم والإرادة، فبالنسبة لعنصر العلم يجب أن يكون لدى الجاني علم بأن البيانات التي سيتم معالجتها هي بيانات ذات طابع شخصي، وأن هذه الجريمة تتم دون إذن من الجهة المختصة، أما عنصر الإرادة هو أن تتجه إرادة الجاني لفعل المعالجة، بأي صورة من الصور دون مراعاة الضوابط القانونية [1]

الفرع الثالث: الركن الشرعي

من المعلوم ان لا جريمة ولا عقوبة الا بنص، حيث أوردت العديد من الدول في قوانينها الخاصة بحماية البيانات الشخصية نصوصًا قانونية تُجرِّم عملية المعالجة دون ترخيص، فالقانون الإماراتي لحماية البيانات الشخصية في المادة الرابعة منه نصت على حظر معالجة البيانات الشخصية دون موافقة صاحبها، لكن في ذات المادة أوردت بعض الاستثناءات منها، ان تكون المعالجة ضرورية لحماية المصلحة العامة أو تكون المعلومات المراد معالجتها أصبحت متاحة، ومعلومة لدى الكافة بفعل صاحب البيانات، أن تكون ضرورية لحماية المصلحة العامة، أو أن تكون لأغراض أرشيفية، أو علمية، أو تاريخية [2].

وكذلك القانون القطري جرم عملية المعالجة دون ترخيص في نص المادة الرابعة حيث نصت على ما يلي:" لا يجوز للمراقب معالجة البيانات الشخصية، إلا بعد الحصول على موافقة الفرد، ما لم تكن المعالجة ضرورية لتحقيق غرض مشروع للمراقب أو الغير الذي تُرسل إليه البيانات.

---

(1) أيوب، بولين انطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق، ص 417، وانظر ايضاً، الحسيني عمار عباس، جرائم الحاسوب والانترنت (الجرائم المعلوماتية)، مرجع سابق، ص240.

(2) نص المادة الرابعة من قانون حماية البيانات الشخصية الإماراتي، لسنة 2021.

أما المشرع الأردني فجرم هذا الفعل في نص المادة الثامنة من مسودة القانون الخاصة بحماية البيانات الشخصية، حيث جاء النص كالاتي: يحظر القيام بمعالجة البيانات الشخصية دون موافقة صاحبها، واستثنى من ذلك الحالات الآتية:

- تنفيذ عقد يكون الشخص المعني بالمعالجة طرفا فيه.
- اتخاذ خطوات بناء على طلب الشخص المعني بالمعالجة بهدف إبرام عقد.
- تنفيذ التزام يرتبه القانون خلافا لالتزام عقدي أو صدور أمر من محكمة مختصة.
- حماية المصالح الحيوية للشخص المعني بالمعالجة. [1]

المطلب الثاني
جريمة الجمع والتخزين غير المشروع للبيانات الشخصية

يقصد بهذه الجريمة جميع الأفعال من جمع أو تسجيل أو حفظ أو تخزين، التي تتم في نطاق الأنشطة المعروفة بالمعالجة الآلية للبيانات الشخصية في نظم المعلومات، أو بنوك المعلومات. [2]

ومن أبرز انتهاك الخصوصية فيما يخص جريمة جمع البيانات ما يعرف بفضيحة **Face book Cambridge Analytical)** شركة كامبريدج، ففي عام **(2018)** كانت قد قامت بجمع بيانات شخصية حول ملايين من الأشخاص على موقع فيسبوك دون أخذ موافقتهم قبل استخدامها؛ لأغراض الدعاية السياسية، مما أدَّى ذلك الفعل إلى هبوط سعر أسهم شركات فيسبوك العالمية [3].

سيتم تقسيم هذا المطلب الى:

الفرع الأول: الركن المادي.

الفرع الثاني: الركن المعنوي.

الفرع الثالث: الركن الشرعي.

---

(1) نص المادة 8 من مسودة قانون حماية البيانات الشخصية الأردني.

(2) أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق، ص 393.

(3) سلامة، مشعل، الحق في الخصوصية، مرجع سابق، ص31.

الفرع الأول: الركن المادي

إن جريمة جمع وتخزين البيانات الشخصية غير المشروع تتم دون رضا صاحبها، أو ليتم استخدامها لأهداف مغايرة عن التي جُمعت من أجلها [1]، كما يمكن أن ترد عملية الجمع على بيانات شخص واحد؛ كاسمه، وعنوانه، وقد تكون بيانات لعدة أشخاص، كجمع عناوين البريد الإلكتروني لهم، والجريمة تتم سواء كان الجمع يدويا؛ كجمع ملفات ورقية، أو من جمعها من خلال وسيلة تقنية [2]، فتفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني، أو بتوصيل أسلاك بطريقة خفية إلى الكمبيوتر الذي تخزَّن داخله البيانات، والحصول عليها من ملفات مُخزَّنة [3]، وفي هذا السياق اعتُبرت محكمة النقض الفرنسية تجميع عناوين البريد الإلكتروني للأشخاص دون علمهم يُعتبر تجميعاً غير مشروع للبيانات الشخصية، وفعل يستحق العقوبة [4].

إن القيام بفعل الجمع والتخزين غير المشروع يحقق الركن المادي لهذا الجُرم، فإن المشرِّع الفرنسي جَرَّم أولا الطريقة التي جُمعت فيها البيانات بالغش والتدليس، أما في الفقرة التالية فجرَّم السلوك الجرمي الواقع على طبيعة تلك البيانات، فالقانون منع المعالجة الإلكترونية المتمثِّلة بالجمع والتخزين بدون موافقة صريحة، متى كانت هذه البيانات تكشف بشكل مباشر، أو غير مباشر الأصول العرقية، أو الآراء الدينية، أو الانتماءات النقابية [5].

---

(1) احمد، حسن خالد، مرجع سابق، ص50.

(2) طباش، عز الدين، 2018، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، العدد 2، مقال منشور، ص 30، https://www.asjp.cerist.dz/en/PresentationRevue/72. تمت زيارة الموقع الساعة 4 مساءً، تاريخ 2022/8/28.

(3) أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق، ص395.

(4) التهامي، سامح عبد الواحد، ضوابط معالجة البيانات الشخصية، مرجع سابق، ص 406.

(5) أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق ص 401، وانظر ايضاً الحسيني، مرجع سابق، ص241.

الفرع الثاني: الركن المعنوي

إن هذه الجريمة تتحقق بالقصد الجنائي العام القائم على عنصري العلم والإرادة، وذلك يعني أنه يجب أن يعلم الجاني أن البيانات التي يقوم بمعالجتها تتعلق بشخص طبيعي، وأن يعلم بأن سلوك معالجتها محظور قانونا، بالإضافة إلى اتجاه إرادته لمعالجتها برغم أن فعله مخالف للقانون، وهي تتحقق بالقصد العام دون الخاص، ولا عبرة بالأسباب التي دعته لارتكاب هذه الجريمة [1].

الفرع الثالث: الركن الشرعي

نص المشرع الإماراتي في المادة 7 /1 على انه:" يجب على المتحكم الالتزام باتخاذ الإجراءات والتدابير التقنية والتنظيمية الملائمة لتطبيق المعايير القياسية اللازمة لحماية وتأمين البيانات الشخصية حفاظا على سريتها وخصوصيتها، وضمان عدم اختراقها أو أتلافها او تغييرها أو العبث بها... إلخ"، نلاحظ من النص السابق انه لم يتم النص على هذه الجريمة بشكل مباشر، الا انه يمكن أن نستخلصها من هذا النص واجب على المتحكم اتخاذ التدابير اللازمة التي من شأنها أن تحمي البيانات من اختراقها والعبث بها.

أما المشرع البحريني فلم ينص على هذه الجريمة وكذلك المشرع الأردني فلم ينص على جريمة الجمع والتخزين غير المشروع في مسودة مشروع القانون الخاصة بحماية البيانات الشخصية ولا أي قانون آخر.

---

(1) الحسيني، عمار عباس، مرجع سابق، ص242.

المطلب الثالث

جريمة الانحراف عن الغاية من المعالجة الإلكترونية للبيانات

ان معالجة البيانات يجب أن تتم ضمن مدة محددة وضمن حدود الغاية من المعالجة فلا يجوز أن تنحرف الجهة المختصة بالمعالجة عن الهدف من المعالجة.

وبناءً عليه قسم هذا المطلب الى:

الفرع الأول: الركن المادي

الفرع الثاني: الركن المعنوي

الفرع الثالث: الركن الشرعي

الفرع الأول: الركن المادي

حيث يتمثَّل السلوك الجُرمي لهذه الجريمة بالانحراف عن الغاية من معالجة البيانات الشخصية، بحيث يعلم الجاني أن سلوكه يشكِّل انحرافا عن الغرض من المعالجة، فمن البديهي أن الذي يقوم بهذا الفعل هو الشخص المسؤول عن المعالجة، وهذا يعني أن عمليتي الجمع والتخزين تمَّتا بطريقة مشروعة، لكن سلوك الانحراف عن الغاية جاء في مرحلة لاحقة لهما، بالإضافة الى اتجاه إرادة الجاني الى ذلك السلوك، كما أن مضمون طلب المعالجة هو المعيار لتحديد سلوك الانحراف، فالغرض من المعالجة موجود في مضمون الطلب المقدَّم إلى جهة المعالجة [1].

الفرع الثاني: الركن المعنوي

إن هذه الجريمة تتطلب قيام القصد العام، بحيث إن الجاني يعلم أن فعل الانحراف عن الغاية المنشودة مخالف قانوناً، ويجب أن تتجه إرادته للانحراف عن الغاية، وهي من الجرائم العمدية،

---

(1) الحسيني، عمار عباس، مرجع سابق، ص 243.

بالإضافة إلى أنه لا عبرة بمقاصد الجاني، أو دوافعه من هذا السلوك [1]، وعلى سبيل المثال: لو استغل الجاني البيانات الشخصية الخاصة بشخص آخر، الخاصة بمقدار ثروته لمعرفة مركزه المالي. [2]

فالجريمة تقوم عندما يعلم الجاني بانه يقوم بالانحراف عن الغاية المنشودة من المعالجة، وهذا يعني ان هذه الجريمة لا تقوم بالإهمال او قلة الاحتراز او الخطأ.

الفرع الثالث: الركن الشرعي

إن المشرِّع الإماراتي حظر هذا السلوك في قانون حماية البيانات الشخصية حيث نص على أن تجميع البيانات الشخصية لغرض محدد وواضح، وألا يتم معالجتها في وقت لاحق بشكل يتنافى مع الغاية التي جُمعت من أجلها إلا في حالة كان الغرض من المعالجة يتشابه ويتماثل مع الهدف الذي جُمعت من أجله في البداية. [3]

اما المشرع البحريني فحظر الانحراف عن الغاية من المعالجة في نص المادة الثالثة الفقرة الثانية من قانون خصوصية البيانات الشخصية على ان لا يتم إجراء معالجة غير متوافقة مع الغرض الذي جمعت من أجله البيانات المعالجة اللاحقة لها التي تتم حصرا لأغراض تاريخية أو إحصائية أو للبحث العلمي وبشرط ألا تتم لدعم اتخاذ أي قرار أو أجراء بشأن فرد محدد.

والمشرع الأردني حظر هذا الفعل في نص المادة 14 من مسودة مشروع قانون لحماية البيانات الشخصية نصَّت على حق الشخص المعني في الموافقة المسبقة، وأن تكون صريحة وواضحة لا

---

(1) الحسيني، عمار عباس، مرجع سابق ص244.

(2) أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق ص421.

(3) نص المادة الخامسة من قانون حماية البيانات الشخصية الاماراتي لسنة 2021.

تحمل التأويل، سواء كانت خطية أو إلكترونية، وأن تكون محددة من حيث المدة، والغاية؛ لأن في كل مرة تتغير طبيعة ونوع المعالجة، وإن لم يجدِّد موافقته في كل مرة تعتبر ملغاة، كما أن أي موافقة تصدر بسبب ممارسة خادعة، أو غير صحيحة لا تعتبر موافقة ولا يعتدُّ بها.

المطلب الرابع
جريمة الاحتفاظ بالبيانات الشخصية أكثر من المدة القانونية اللازمة

ان الاحتفاظ بالبيانات الشخصية أكثر من المدة المحددة في طلب المعالجة يعد مخالفة تقع على عاتق المسؤول عن المعالجة، فلا يجوز ان تتجاوز المدة المحددة.

وعليه سيتم تقسيم المطلب الى ثلاثة فروع:

الفرع الأول: الركن المادي.

الفرع الثاني: الركن المعنوي.

الفرع الثالث: الركن الشرعي.

الفرع الأول: الركن المادي

يتحقق الركن المادي في هذه الجريمة بفعل الاحتفاظ بالبيانات الشخصية أكثر من المدة القانونية اللازم، حتى وان تم الجمع والحفظ بطريقة مشروعة [1]، وذلك لان التجريم ينصب على فعل الحفظ خارج المدة المحددة قانونا، فمن حق صاحب البيانات تحديد مدة المعالجة وعند الانتهاء من الغرض من المعالجة حقه ان يطالب بالمحو او النسيان، فسلوك الاحتفاظ بالبيانات الشخصية أكثر من المدة المحددة يعتبر انتهاك لحق الشخص بنسيان أو محو بياناته.

---

(1) الحسيني، عمار عباس، مرجع سابق، ص245.

الفرع الثاني: الركن المعنوي

ويتخذ الركن المعنوي في هذه الجريمة صورة القصد العام القائم على عنصري العلم والإرادة، بحيث يكون الجاني على علم بأنه يقوم بالاحتفاظ ببيانات شخصية أكثر من المدة المحددة قانونا، وأن تتجه إرادته إلى سلوك الاحتفاظ غير المشروع بحكم القانون، وأن هذه الجريمة لا تتطلب القصد الخاص فلا عبرة من دوافعه. [1]

فهي تعد من الجرائم المقصودة فإرادة الجاني تتجه الى حفظ البيانات خارج المدة وهو على علم بأن ذلك الاحتفاظ خارج المدة المحددة ويعلم ان هذا السلوك بغير رضا صاحب البيانات وبدون اذن او تصريح منه، وبناء عليه فان تم هذا السلوك نتيجة الخطأ او الإهمال فلا تقوم الجريمة.

الفرع الثالث: الركن الشرعي

حظر المشرِّع البحريني الاحتفاظ بالبيانات الشخصية أطول من المدة المحددة في طلب الإخطار المسبق، فجاء في نص القانون في المادة العاشرة [2]، فلا يمكن الاحتفاظ بالبيانات لمدة غير محددة، فعلى معالج البيانات أن يحدد المدة والهدف من المعالجة، بحيث يتم إتلافها، ومحوها بمجرد تحقق الهدف. [3]

---

(1) الحسيني، عمار عباس، مرجع سابق، ص 245.

(2) https://www.almeezan.qa/LawArticles.aspx?LawTreeSectionID=17484&lawId=7121&language=ar المادة العاشرة من قانون ال رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية على المراقب التحقق من أن البيانات الشخصية التي يجمعها، أو التي يتم جمعها لصالحه، ذات صلة بالأغراض المشروعة وكافية لتحقيقها، وعليه التحقق من أن تلك البيانات دقيقة ومكتملة ومحدثة بما يفي بالأغراض المشروعة، وألا يحتفظ بها لمدة تزيد على المدة الضرورية لتحقيق تلك الأغراض.

(3) الأشقر، منى جبور، الجبور، محمود، مرجع سابق، ص125.

وحظر المشرع القطري الاحتفاظ بالبيانات الشخصية أكثر من المدة الضرورية لتحقيق الغرض من معالجتها. [1]

نصت المادة 8 من قانون حماية البيانات الشخصية الإماراتي على انه يجب أن يلتزم المعالج بحدود المدة المتفق عليها للمعالجة وان لا يتجاوزها في الفقرة 3/8 على النحو الاتي:" يجب أن يلتزم المعالج بأجراء المعالجة وفق الغرض والمدة المحددة لها، وفي حال تجاوزت المعالجة المدة المحددة يجب عليه أن يخطر المتحكم بذلك ليأذن له بتمديد هذه المدة أو يصدر اليه توجيهاته المناسبة.

وحظر المشرع الأردني في مسودة القانون الخاص في حماية البيانات الشخصية في المادة 9 كما يلي:" يتعين على المسؤول وقبل البدء بالمعالجة إعلام الشخص المعني خطيا أو إلكترونيا بما يلي:

أ. البيانات التي ستتم معالجتها وتاريخ البدء بذلك.

ب. الغرض الذي تجري من أجله معالجة ببياناته

ج. المدة الزمنية التي ستتم خلالها معالجة البيانات، على ألا يتم تمديد هذه المدة إلا بموافقة الشخص المعني ووفقا لأحكام القانون.

د. المعالج الذي سيشارك المسؤول في تنفيذ المعالجة ها ضوابط أمن وسلامة حماية البيانات ومعلومات عن التشخيص.

---

(1) نص المادة العاشرة من قانون حماية البيانات الشخصية القطري لسنة 2016.

المطلب الخامس
جريمة إفشاء البيانات الشخصية

إن المقصود بجريمة الإفشاء في هذه الجريمة هو نقل البيانات الشخصية من قبل المسيطِر عليها بحكم أنه مسؤول عن معالجتها إلى شخص أو جهة غير مختصة بتلقي هذه البيانات، وليس المقصود بها التمكن من اختراق النظام المعلوماتي، والحصول على تلك البيانات من خارج دائرة المختصين بمعالجتها والأخيرة هي من صور جرائم الكمبيوتر، وليست جريمة الإفشاء غير المشروع، فالإفشاء هنا يقع من المسؤول عن المعالجة والجمع والحفظ. [1]

فهي تعني نقل البيانات من المسؤول عن معالجتها إلى شخص آخر أو جهة غير مختصة بالاطلاع عليها وليس لها الحق بالاطلاع عليها.

وبناءً عليه، سيتم تقسيم المطلب إلى ثلاثة فروع كما يلي:

الفرع الأول: الركن المادي.

الفرع الثاني: الركن المعنوي.

الفرع الثالث: الركن الشرعي.

الفرع الأول: الركن المادي

تقوم الجريمة بقيام الشخص المسموح له بمعالجة أو جمع أو تخزين البيانات الشخصية بإفشائها إلى جهة أخرى ليس لها الصلاحية بالاطلاع عليها، ولا يقصد في هذه الجريمة جريمة الاختراق من قبل غير المختصين بحكم القانون بمعالجتها، ويتحقق الإفشاء عند الدخول للنظام، واستخراج البيانات

(1) أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق ص 402.

وهدفه إيصالها للغير أياً كان، سواء هيئة حكومية، أو غير حكومية، أو شخص طبيعي،[1] فهو حقق معنى الاطلاع على البيانات الشخصية، وعند دخوله للنظام كان قاصدا الإفشاء، كما أن المشرِّع النمساوي سار على نفس النهج، حيث إنه عقاب كل من أفشى عمدا، أو استخدم معلومات آلية، أو مصرَّح له وحده، بسبب طبيعة عمله في مجال المعالجة الإلكترونية للمعلومات؛ للاطلاع عليها [2]، كما أنه يشترط لاكتمال هذه الجريمة أن ينقلها كما هي بدون أي تغيير أو تعديل.

فالسلوك هنا مجرد نقل بهدف إفشائها للغير فإذا تعدَّى ذلك ندخل بصورة أخرى من صور الجرائم الواقعة على البيانات، ويقصد بالغير هنا الجميع ما عدا الفاعل وصاحب البيانات، ولم يحدِّد القانون طريقة نقلها، أو نطاقها سواء لعدد معين من الأشخاص، أو عدد غير محدد [3].

ولا بدَّ من الإشارة إلى الفرق بين جريمة إفشاء الأسرار وجريمة إفشاء البيانات الشخصية، فجريمة إفشاء الأسرار موضوعها إفشاء معلومات سرية؛ إما رسمية، أو متعلِّقة ببعض المهن؛ كالطب والمحاماة، والفرق الآخر أن جريمة إفشاء المعلومات الشخصية يُتصوَّر ارتكابها؛ بسبب الإهمال، أو عدم الاحتياط، في حين جريمة إفشاء الأسرار لا يُتصوَّر وقوعها إلا بصورة القصد. [4]

يتحقق الركن المادي بتوافر عنصر الحيازة للبيانات الشخصية، سواء بقصد نقلها، وتصنيفها، أو معالجتها، والعنصر الثاني عنصر الإفشاء لمن ليس لهم الصلاحية بالاطلاع عليها، ويجب أن يقترن بعنصر الإفشاء عدم رضا المجني عليه، وهذا يعني إذا كان برضا المجني لا يتحقق النشاط المادي

---

(1) احمد، خالد حسن، مرجع سابق، ص 50 وص 76.

(2) الشوابكة محمد امين، جرائم الحاسوب والانترنت، مرجع سابق، ص 355.

(3) الزعبي، جلال محمد، المناعسة، أسامة احمد، مرجع سابق ص232.

(4) أيوب، بولين أنطونيوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، مرجع سابق، ص 403.

لهذه الجريمة، فمن الواضح أنها من جرائم الضرر، فإن كان فعل الإفشاء لا يحقق ضررًا لا تقوم الجريمة. [1]

الفرع الثاني: الركن المعنوي

إن الركن المعنوي في هذه الجريمة يتخذ صورتين العمد والخطأ، فالعمد يتوفر بعنصري العلم والإرادة، بأن يعلم الجاني بأنه يقوم بإفشاء غير مشروع للبيانات الشخصية لجهة غير مسموح لها قانوناً بالاطلاع عليها.

يتمثل الركن المعنوي أن تتجه إرادة الجاني بأن يحقق ضررًا أو اعتداءً على شرف، أو اعتبار صاحب البيانات الشخصية، أما فيما يخص صورة الخطأ فهنا تتحقق النتيجة بسبب إهمال البيانات الشخصية بنا يحقق إفشاؤها للغير، كما أن رضا المجني عليه يكون سبباً في إباحة الفعل وبالتالي انتفاء الجريمة [2].

الفرع الثالث: الركن الشرعي

جرم المشرع البحريني في نص المادة 58 من قانون حماية البيانات الشخصية في الفقرة الأولى /(ط) مع عدم الأخلال بأية عقوبة أشد ينص عليها أي قانون آخر: يعاقَب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تقل عن ألف دينار ولا تتجاوز عشرين ألف دينار، أو بإحدى هاتين العقوبتين، كلُّ مَن: أفصح عن أية بيانات أو معلومات من المتاح له النفاذ إليها بحكم عمله أو استخدمها لمنفعته أو لمنفعة الغير، وذلك دون وجه حق وبالمخالفة لأحكام هذا القانون، كما حظر المشرع القطري إفشاء البيانات او الوصول اليها في نص المادة 13 من قانون حماية البيانات الشخصية.

---

(1) الحسيني، عمار عباس، مرجع سابق، ص 247

(2) الحسيني، عمار عباس، مرجع سابق، ص248.

أما المشرع الإماراتي فقط نص في المادة 2/20 على ما يلي: يراعى عند تقديم مستوى أمن المعلومات التي نصت عليها الفقرة الأولى من ذات المادة، ما يأتي:

- المخاطر المصاحبة للمعالجة بما فيها تلف البيانات الشخصية أو ضياعها أو التعديل العرضي عليها أو غير القانوني لها أو الإفشاء او الوصول غير المصرح به لها سواء تم نقلها أو تخزينها او معالجتها.

أما المشرع الأردني فجرم الإفشاء في نص المادة 27 من مسودة القانون الخاصة بحماية البيانات الشخصية على النحو الاتي:

يعاقب بغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (10000) عشرة آلاف دينار كل من ارتكب أيا من الأفعال التالية:

د –إفشاء البيانات الشخصية الموجودة لديه دون موافقة الشخص المعني بالمعالجة.

أما فيما يخص التشريع الأردني لا يوجد نصوص كهذه سوى نص المادة (355) من قانون العقوبات الأردني الخاص بإفشاء الأسرار في الفقرة الأولى والثالثة وجاء النص كالآتي:" يُعاقَب بالحبس مدة لا تزيد على ثلاث سنوات كلُّ مَن:

- حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية، وأباح هذه الأسرار لمن ليس له صلاحية الاطلاع عليها، أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع وفقا للمصلحة العامة.
- كان بحكم مهنته على علم بسر، وأفشاه دون سبب مشروع [1].

وبالتالي فإن الباحث يرى بأن النصوص العقابية الخاصة بجريمة إفشاء الأسرار لا تصلح لحماية البيانات الشخصية التي تكون محلا للمعالجة الآلية.

---

(1) قانون العقوبات الأردني المعدل حتى سنة 2022.

المبحث الثاني
الأساس القانوني لانعقاد المسؤولية الجزائية

إن ملاحقة الأفراد وانتهاك بياناتهم الشخصية والتعدِّي عليها من خلال الوصول إلى البيانات المخزَّنة في ازدياد، وذلك بسبب وسائل تقنية المعلومات التي ساهمت بشكل كبير في الوصول إلى سجلات البيانات المخزَّنة، ومن ثم إساءة استخدامها، كما أن الإقرار بحماية البيانات الشخصية إقرارٌ بحق المواطن في الحفاظ على خصوصيته من جهة أولى، كما إنه إقرار بحق الدولة في الاطلاع على هذه البيانات ومعالجتها، ضمن أُطُرٍ قانونية وتنظيمية محددة وواضحة، وذلك يسمح بالسلطات المختصة، بمنع وقوع أعمال مخلَّة بالأمن والنظام، أو بملاحقة ومعاقبة مرتكبيها من جهة ثانية[1].

وبالتالي إن وضع إطار قانوني لحماية البيانات الشخصية لا يكفي، فلا بدَّ من وجود جهة تنفذ القانون، وتكفل الرقابة السليمة على معالجة البيانات الشخصية، وأيضا تكفل إيقاع العقوبات المناسبة جرَّاء أيَّ مخالفة.

في البداية لا بدَّ من الحديث عن تشكيل اللجنة أو السلطة التي تُعتبر جهازًا إداريًّا مستقلًّا حيث يجب أن تصدر توصياتها وقرارتها بشكل مستقل عن أي سلطة أخرى، وهذا يجعل لقراراتها الطبيعة الإدارية، بحيث يطعن بقرارتها أمام محاكم القضاء الإداري، واستقلاليتها تكون بعدم إخضاعها للهرمية الوظيفية كما هو الحال في الوزارات، بحيث لا يتلقون أوامرَ، أو آراءٍ، أو تعليماتٍ من أي وزارة، أما بالنسبة لاستقلالية موظفيها فيجب أن يتمتعوا بحصانة؛ لعدم عزلهم و عدم ممارستهم أية وظيفة، أو نشاط يمكن يتعارض مع عضويتهم في اللجنة، أو السلطة، ولا يجوز أن يكون رئيسًا الهيئة، أو أعضائها من الموظفين، أو أصحاب الشركات التي تعمل في معالجة البيانات، بالإضافة إلى عدم

---

(1) احمد، حسن خالد، مرجع سابق، ص 56.

وجود أية مصالح لهم في مؤسسات هذه الأنشطة، وذلك ما جاء في التوصيات الأوربية لعام 1995 التي نصت على ضرورة استقلالية الهيئات أو السلطات التي تُعنى بحماية البيانات الشخصية، وذلك ما جاء في نص المادة (28) من الاتفاقية [1]، كما أن تعيين أعضاء الهيئة غالباً ما يكون من قبل السلطة التنفيذية، أما الأفضل أن يتم تعيينهم من قبل السلطة التشريعية، وذلك لتكون الهيئة أكثر استقلالية من أن يُعيَّنوا من قبل السلطة التنفيذية، فمثلا في إنجلترا يتم تعيين الأعضاء من أصحاب الخبرة، وأشخاص مستقلين عن السلطة السياسية التي تتولَّى الحكم، لكن في معظم الدول يتم تعيين أعضاء من الشخصيات السياسية؛ كوزراء أو برلمانيين [2].

وبناءً عليه، سيتم تقسيم هذا المبحث إلى مطلبين كالآتي:

المطلب الأول: الرقابة على حماية البيانات الشخصية.

المطلب الثاني: العقوبات الجزائية المترتبة على انتهاك البيانات الشخصية.

المطلب الأول
الرقابة على حماية البيانات الشخصية

إن العديد من الدول استجابت لحماية البيانات الشخصية، فأصدرت قوانين لحمايتها، فكان الإطار القانوني لأغلب الدول يضم جهة، أو هيئة، أو مجلسًا لحماية البيانات الشخصية، **فالقانون الإماراتي** في نص المادة الأولى عرَّف المكتب على النحو الآتي: " مكتب الإمارات للبيانات المنشأ بموجب المرسوم بقانون اتحادي **رقم (44)** لسنة:" يختص المكتب الذي يتبع مجلس الوزراء بمجموعة من المهام التي تشمل:

- اقتراح وإعداد السياسات والاستراتيجيات والتشريعات المتعلقة بشؤون حماية البيانات.

---

(1) الأشقر، منى جبور، الجبور محمود، مرجع سابق، ص154.

(2) الأشقر، منى جبور، الجبور محمود، مرجع سابق، ص 155 وما بعدها.

- اقتراح واعتماد الأسس والمعايير الخاصة بالرقابة على تطبيق التشريعات الاتحادية المنظمة؛ لحماية البيانات.
- إعداد واعتماد الأنظمة الخاصة بالشكاوى والتظلُّمات المتعلقة بحماية البيانات.
- إصدار الأدلة والتعليمات اللازمة لتطبيق تشريعات حماية البيانات [1].
- يقوم المكتب بتنفيذ عمليات الرقابة على تطبيق التشريعات الاتحادية المنظمة لحماية البيانات، وإجراء التحقيقات اللازمة للتأكد من مدى الامتثال لها، ونشر الوعي حول أحكام ومتطلبات القانون من خلال تنظيم المؤتمرات والندوات وورش العمل وغيرها.

نصت المادة (39/1) من قانون حماية البيانات **الشخصية البحريني** على تشكيل المجلس من سبعة أعضاء، وجاء النص كالآتي:

- عضو يرشِّحه مجلس الوزراء.
- عضو ترشِّحه جامعة البحرين من بين أعضاء هيئة التدريس بدرجة لا تقل عن أستاذ مشارك في تخصُّص مناسب لمجال عمل الهيئة.
- عضو ترشِّحه هيئة تنظيم الاتصالات من بين شاغلي الوظائف العليا بها.
- عضو يرشِّحه مصرف البحرين المركزي من بين شاغلي الوظائف العليا به.
- عضو ترشِّحه غرفة تجارة وصناعة البحرين.
- عضو ترشِّحه الجهة التي يقدِّر الوزير بعد التشاور مع محافظ مصرف البحرين المركزي بأنها الأوسع تمثيلاً لأصحاب الأعمال في قطاع المؤسسات المالية.
- عضو ترشِّحه الجهة التي يقدِّر الوزير أنها الأوسع تمثيلاً للمختصين في مجال تقنية المعلومات.

---

(1) نص المادة الثالثة من قانون رقم 44 لسنة 2021.

كما نصت المادة (40) على المهام والصلاحيات المنوطة بالمجلس على النحو الآتي:

"يقوم المجلس بإصدار اللوائح والقرارات واتخاذ التدابير اللازمة لتنفيذ القانون، ويصدر لوائح داخلية لتنظيم شؤون موظفين الهيئة تشمل قواعد تعيينهم ونقلهم وترقيتهم ومرتَّباتهم ومكافآتهم وأحكام تأديبهم، وذلك دون التقيد بأحكام قانون الخدمة المدنية، والقواعد السلوكية التي يجب عليهم مراعاتها بالإضافة إلى اعتماد مشروع الميزانية السنوية، وحسابها الختامي المدقَّق، وقبول الموارد المالية ودراسة التقارير الدورية التي يقدِّمها الرئيس التنفيذي [1].

أما مسوَّدة قانون حماية البيانات الشخصية **الأردني** نصت على تشكيلة مجلس حماية البيانات الشخصية في **المادة الرابعة** حيث يشكَل بقرار من مجلس الوزراء على النحو التالي:

- الوزير رئيسًا.
- مفوض الحماية نائباً للرئيس.
- رئيس اللجنة القانونية في مجلس النواب عضوًا.
- رئيس مجلس الأمناء للمركز الوطني لحقوق الإنسان عضوًا.
- المفوض العام لحقوق الإنسان عضوًا.
- مفوض المعلومات المعين بموجب قانون ضمان حق الحصول على المعلومات عضوًا.
- الأجهزة الأمنية عضوين.
- ذوو الخبرة والاختصاص في مجال البيانات الشخصية ثلاثة أعضاء.

ذهبت هذه المادة إلى أنه يترأس المجلس الوزير، وهذا من شأنه أن يخلَّ باستقلالية عمل المجلس، وكيف ستستقيم مسألة الحماية مع وجود عضوين من الأجهزة الأمنية، فهل يعقل أن يكون الخصم

---

(1) من قانون حماية البيانات الشخصية البحريني لسنة 2018.

والحكم واحدًا، وهل سيحقق مجلس الحماية إن كانت الانتهاكات من قبل السلطة التنفيذية، بالإضافة إلى أن الجهتين المتمثِّلتين بالسلطة التنفيذية، والأجهزة الأمنية هما أكبر حاضن ومعالج للمعلومات الشخصية المتعلقة بالأفراد، وبالتالي خطر إفشائها وارد من قبل هذه الجهات التي من المفترض أنهم أمناء عليها.

ونصَّت **المادة الخامسة** على صلاحيات المجلس حيث يمارس المجلس جميع الصلاحيات اللازمة لقيامه بمهامه وفقًا لأحكام هذا القانون بما في ذلك:

إقرار السياسات والاستراتيجيات المتعلقة بحماية البيانات، وإقرار الخطط والبرامج اللازمة للحماية، وتحديد أفضل الوسائل الواجب اتباعها؛ لضمان حسن أداء المسؤول عن المعالجة، ووضع آلية الشكاوى والطلبات المقدمة من الشخص المعني بحق المسؤول عن المعالجة، أو بحق أي مسؤول آخر، بالإضافة إلى إصدار التوصيات بشأن المعاهدات، والاتفاقيات، والتشريعات، والأنظمة، والتعليمات المتعلقة بحماية البيانات الشخصية، وإقرار التعليمات الداخلية المتعلقة بمهام مراقب حماية البيانات الشخصية، – إصدار التعليمات التي تبين شروط وإجراءات الحصول على الموافقة، وسحب الموافقة والنماذج الخاصة بالموافقة، وسحب الموافقة وتصاريح نقل، أو تبادل البيانات الشخصية داخل وخارج المملكة، و إصدار المجلس قائمة مُحدَّثة بشكل دوري للدول، أو الهيئات، أو المنظمات الدولية، أو الإقليمية المعتمدة لدى المملكة، والتي يتوافر لديها مستوى الحماية الكافي، وإقرار التقرير السنوي الخاص بحماية البيانات الشخصية الصادر عن مفوِّض الحماية ورفعه إلى مجلس الوزراء. وأي مهام أخرى تُناط بالمجلس بمُقتضى التشريعات النافذ [1].

(1) المادة الخامسة، مسودة قانون حماية البيانات الشخصية الأردني.

أما المشرِّع البحريني في المادة 39 في الفقرة الثالثة منها نصت على أنه لا يجوز الجمْع بين منصب الوزير وعضوية مجلس الإدارة، وكان موفَّقاً في ذلك أكثر من التشريع السعودي والإماراتي والأردني، حيث كان أقرب إلى الحياد، والاستقلالية منهما.

ومثال على استقلالية وحياد اللجنة الخاصة بحماية البيانات الشخصية في اللوكسمبرج، حيث تُعدُّ مؤسسة عمومية مستقلة ذات شخصية قانونية، و تتمتع بالاستقلال الإداري والمالي، وكذلك الحال بالنسبة للَّجنة الوطنية للحريات والمعلومات في فرنسا CNIL هي أيضا سلطة إدارية مستقلة [1].

وبناءً على ما سبق، وبعد عرض النصوص القانونية الجزائية المتعلقة بحماية البيانات الشخصية في القانون الإماراتي والبحريني ، ومسوَّدة قانون حماية البيانات الشخصية الأردني، اتضح أن تشكيلة مجلس حماية البيانات في جميع هذه الدول لم يكن مستقلاً، فلا يمكن أن تستقيم الرقابة والحماية، وذلك يرجع إلى أن السلطة التي تقوم بالمعالجة للبيانات المتمثلة بالسلطة التنفيذية هي نفسها السلطة التي تعمل على المراقبة والحماية، حيث وقعت هذه التشريعات في إشكالية عدم الحياد، والاستقلالية في الحماية، وكان الأجدر بها أن تعين رئيس المجلس عن طريق الانتخاب.

المطلب الثاني

المسؤولية الجزائية المترتِّبة على انتهاك البيانات الشخصية

من الملاحظ في العصر الحاضر أن أغلبية الدول سعت إلى تنظيم إطار قانوني خاص لحماية البيانات الشخصية التي قد تكون محلا للاعتداءات بشتى الطرق، والمُتأمِّل في تواريخ اهتمام الدول في هذا الشأن، يرى أن الدول الأوربية سبأَّقة في هذا الشأن، على خلاف الدول العربية التي تنبَّهت لمعالجة موضوع حماية البيانات الشخصية للأفراد منذ سنوات قليلة.

وبناءً على ما سبق، سيتم تقسيم هذا المطلب إلى فرعين على النحو الآتي:

---

(1) ارجدال، علي، حماية المعطيات الشخصية، مرجع سابق، ص83.

الفرع الأول: المسؤولية الجزائية في التشريعات المقارنة.

الفرع الثاني: المسؤولية الجزائية في التشريع الأردني.

الفرع الأول: المسؤولية الجزائية في التشريعات المقارنة

نصَّ **المشرِّع البحريني** في قانون حماية البيانات الشخصية رقم 2018 في المادة (58) على العقوبات الجزائية المترتِّبة على انتهاك البيانات الشخصية، فنصَّ على أن كلَّ من عالج بياناتٍ حساسةً بخلاف أحكام المادة الخامسة [1]، وهي التي تتضمَّن الاشتراطات الخاصة بمعالجة البيانات

(1) تُحظَر معالَجة البيانات الشخصية الحساسة دون موافقة صاحبها، ويُستثنَى من هذا الحظْر ما يأتي:
1) المعالَجة التي يقتضيها قيام مدير البيانات بالتزاماته ومباشرة حقوقه المقرَّرة قانوناً في مجال علاقة العمل التي تربطه بالعاملين لديه.
2) المعالجة الضرورية لحماية أيِّ إنسان إذا كان صاحب البيانات –أو الوصي أو الولي أو القَيِّم عليه – غير قادر قانوناً على إعطاء موافقته على ذلك، وبشرط الحصول على تصريح مسبق من الهيئة طبقاً للمادة (15) من هذا القانون.
3) معالجة البيانات التي أتاحها صاحبها للجمهور.
4) المعالجة الضرورية لمباشرة أيٍّ من إجراءات المطالبة بالحقوق القانونية أو الدفاع عنها، بما في ذلك ما يقتضيه التجهيز لهذا الأمر والاستعداد له.
5) المعالجة الضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو تقديم الرعاية الصحية أو العلاج أو إدارة خدمات الرعاية الصحية من قِبَل مرخَّص له بمزاولة أيٍّ من المهن الطبية، أو أيِّ شخص ملزَم بحكم القانون بالمحافظة على السرِّية.
6) المعالجة التي تتم في سياق أنشطة الجمعيات بأنواعها والنقابات وغيرها من الجهات التي لا تهدف إلى تحقيق ربح، وذلك بشرط الالتزام بما يأتي:
أ) انْ تتم المعالجة في حدود ما هو ضروري للغرض الذي أنشئت الجمعية أو النقابة أو الجهة من أجله.
ب) أنْ ترد المعالجة على بيانات تخص أعضاء تلك الجمعية أو النقابة أو الجهة أو لأفراد لهم اتصال منتظم معها بحكم طبيعة نشاطها.
ج) ألا يتم الإفصاح عن البيانات لأيِّ شخص آخر ما لم يوافق صاحب البيانات على ذلك.
7) المعالَجة التي تتم من قِبَل جهة عامة مختصة بالقدر الذي يقتضيه تنفيذ المهام المنوطة بها قانوناً.
8) معالجة بيانات تتعلق بالأصل العِرْقي أو الإثْنِي أو الديني إذا كانت ضرورية للوقوف على مدى توافر المساواة في الفرص أو المعاملة لأفراد المجتمع الذين ينحدرون من أصول عِرْقية أو إثْنِية أو دينية مختلفة، وبشرط مراعاة الضمانات المناسبة لحقوق وحريات أصحاب البيانات المقرَّرة قانوناً.
وعلى مجلس الإدارة أنْ يُصدِر قراراً بتحديد القواعد والإجراءات التي يتعيَّن على مدراء البيانات الالتزام بها بشأن المعالجة المشار إليها.

الشخصية الحساسة من هذا القانون، أو نقل بيانات شخصية خارج المملكة إلى بلد، أو إقليم خلافا لحكم أيٍّ من المادتين (12) و(13) [1] من هذا القانون، أو إذا عالج بيانات شخصية دون إخطار

---

(1) – مادة (12):

نقْل البيانات الشخصية إلى بلدان وأقاليم توفِّر مستوى كافِياً من الحماية

يُحظَر على مدير البيانات نقْل البيانات الشخصية إلى خارج المملكة في غير الحالات التالية:

1) أنْ يكون النقل إلى بلد أو إقليم مدرج في كشف تتولى الهيئة إعداده، وتحديثه يتضمن أسماء البلدان، والأقاليم التي تقدِّر الهيئة أنَّ لديها تشريعات أو أنظمة معمولاً بها، تكفل مستوى كافياً من الحماية للبيانات الشخصية، ويُنشَر هذا الكشف في الجريدة الرسمية.

2) أنْ يكون النقل بتصريح يصدر من الهيئة في كل حالة على حدة، وذلك إذا قدَّرت أنَّ البيانات سوف يتوافر لها مستوى كافٍ من الحماية، ويكون تقدير الهيئة بمراعاة كافة الظروف المحيطة بعملية نقل البيانات، وبوجه خاص ما يأتي:

أ) طبيعة البيانات المطلوب نقْلُها، والغرض من معالجتها ومدة المعالجة.

ب) البلد أو الإقليم مصدر هذه البيانات والوجهة النهائية لها، وما يتوافر في تلك البلدان أو الأقاليم من تدابير لحماية البيانات الشخصية.

ج) الاتفاقيات الدولية والتشريعات ذات العلاقة المعمول بها لدى البلد أو الإقليم الذي سوف تُنقَل إليه البيانات.

ويجوز أنْ يكون التصريح المشار إليه مشروطاً أو لفترة زمنية محدَّدة.

مادة (13):

1) استثناءً من أحكام المادة (12) من هذا القانون، يجوز لمدير البيانات نقْل بيانات شخصية خارج المملكة إلى بلد، أو إقليم لا يوفر مستوى كافياً من الحماية للبيانات في أيٍّ من الحالات التالية:

أ) إذا وافق صاحب البيانات على هذا النقل.

ب) إذا كان هذا النقل لبيانات مستخرجة من سجل تم إنشاؤه وفقاً للقانون، بغرض توفير معلومات للجمهور، سواءً كان الاطلاع على هذا السجل متاحاً للكافة، أو مقصوراً على ذوي المصلحة وِفْقاً لشروط معينة. وفي هذه الحالة يتعيَّن للاطلاع على هذه المعلومات استيفاء الشروط المقرَّرة للاطلاع على السجل.

ج) إذا كان هذا النقل ضرورياً لأي مما يأتي:

(1) تنفيذ عقد بين صاحب البيانات ومدير البيانات، أو لاتخاذ خطوات سابقة بناءً على طلب صاحب البيانات بهدف إبرام عقد.

(2) تنفيذ أو إبرام عقد بين مدير البيانات وطرف ثالث لمصلحة صاحب البيانات.

(3) حماية مصالح حيوية لصاحب البيانات.

(4) تنفيذ التزام يرتِّبه القانون، خلافاً لالتزام عقدي، أو صدور أمر من محكمة مختصة أو النيابة العامة، أو قاضي التحقيق، أو النيابة العسكرية.

(5) إعداد أو مباشرة مطالَبة قانونية أو الدفاع عنها.

2) مع عدم الإخلال بأحكام البند (1) من هذه المادة، يجوز للهيئة التصريح بنقْل بيانات شخصية، أو مجموعة منها، إلى بلد أو إقليم لا يكفل مستوى كافياً من الحماية وِفْقاً لمتطلبات المادة (12) من هذا القانون، إذا قدم مدير البيانات ضمانات كافية بشأن حماية الخصوصية والحقوق والحريات الأساسية للأفراد. ويجوز، بوجه خاص، أنْ تكون هذه الضمانات وِفْقاً لعقدٍ أحدُ أطرافه مدير البيانات. وعلى الهيئة أنْ تقْرُن منْح التصريح في هذه الحالة باستيفاء شروط معينة.

الهيئة، تخلَّف عن إخطار الهيئة بأيِّ تغيير يطرأ على البيانات التي قام بإخطار الهيئة بها، أو عالج بيانات شخصية دون تصريح مسبق من الهيئة، أو قدَّم إلى الهيئة، أو إلى صاحب البيانات بيانات كاذبة، أو مضلِّلة، أو على خلاف الثابت في السجلات، أو البيانات، أو المستندات التي تكون تحت تصَرُّفه، أو حجَب عن الهيئة أية بيانات، أو معلومات، أو سجلات، أو مستندات من تلك التي يتعيَّن عليه تزويد الهيئة بها، أو تمكينها من الاطلاع عليها؛ للقيام بمهامِّها المقرَّرة، أو تسبَّب في إعاقة، أو تعطيل عمل مفتِّشي الهيئة، أو أيِّ تحقيق تكون الهيئة بصدد إجرائه، أو أفصح عن أية بيانات، أو معلومات من المتاح له النفاذ إليها بحكم عمله، أو استخدمها لمنفعته، أو لمنفعة الغير، وذلك دون وجه حق، وبالمخالفة لأحكام هذا القانون، يعاقَب بالحبس مدة لا تزيد على سنة، وبالغرامة التي لا تقل عن ألف دينار، ولا تتجاوز عشرين ألف دينار، أو بإحدى هاتين العقوبتين [1].

كما نصت الفقرة الثانية من المادة (85) على أن يُعاقَب بالغرامة التي لا تقل عن ثلاثة آلاف دينار، ولا تتجاوز عشرين ألف دينار، مَن خالف حكم أيٍّ من البندين (1) أو (2) من المادة (32) من هذا القانون، وفي حالة الحكم بالإدانة للمحكمة أنْ تقضي بمُصادرة المبالغ المتحصَّلة من الجريمة.

وتنص المادة (32) على ما يلي:

1) على عضو مجلس الإدارة لدى نظر المجلس لأيِّ موضوع يكون لهذا العضو فيه مصلحة شخصية مباشرة، أو غير مباشرة تتعارض مع مقتضيات منصبه، أنْ يُفْصِح عن ذلك كتابةً حالَ علمه بعزْم المجلس نظرَ هذا الموضوع، ولا يجوز لهذا العضو حضور مناقشات المجلس بشأن ذلك الموضوع، أو التصويت عليه.

---

(1) – نص (المادة 85) من قانون حماية البيانات الشخصية البحريني لسنة 2018.

2) يُحظَر أنْ يكون للرئيس التنفيذي أو لأيٍّ من موظَّفي الهيئة مصلحة مباشرة، أو غير مباشرة في مجال عمل الهيئة تتعارض مع مقتضيات الوظيفة، وعلى كلٍّ منهم الإبلاغ كتابةً فوراً عن أية مصلحة تنشأ له في هذا الشأن، خلال فترة شغْل الوظيفة لدى الهيئة. ويكون إبلاغ الرئيس التنفيذي لمجلس الإدارة، وما عداه من موظَّفي الهيئة فيبلغ الرئيس التنفيذي.

كما عاقب في الفقرة الثالثة من ذات المادة بالحبس مدة لا تزيد على شهر، وبالغرامة التي لا تقل عن مائة دينار، ولا تتجاوز خمسمائة دينار، أو بإحدى هاتين العقوبتين، كلَّ مَن استعمل –دون وجه حق– شعار الهيئة، أو رمزاً، أو شارة مماثلة، أو مشابهة له.

فلم يكتفِ **المشرِّع البحريني** بذلك وحسب، بل قرَّر مسؤولية جزائية للشخص الاعتباري، أو المعنوي، وذلك في نص المادة (59) وجاء النص كالآتي:

"مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي، يعاقَب الشخص الاعتباري بما لا يجاوز مِثْلَي الغرامة المقرَّرة للجريمة إذا ارتُكِبت باسمه، أو لحسابه، أو لمنفعته أية جريمة من الجرائم المنصوص عليها في المادة (58) من هذا القانون، وكان ذلك نتيجة تصرُّف، أو امتناع أو موافقة، أو تستُّر، أو إهمال جسيم من أيٍّ من أعضاء مجلس إدارة الشخص الاعتباري، أو أيِّ مسؤول مفوَّض آخر في ذلك الشخص الاعتباري، أو ممَّن يتصرَّف بهذه الصفة.

أما فيما يخصُّ **المشرِّع القطري** فنصَّ على العقوبات التي تترتَّب على انتهاك البيانات الشخصية من نص المادة (23) الى المادة (25)، حيث نص في المادة (23) على عقوبة الغرامة التي لا تزيد على مليون ريال كلَّ من يخالف أحكام المواد (4)، (8)، (9)، (10)، (11)، (12)، (14)، (15)،

(22) من قانون حماية البيانات الشخصية وهذه المواد هي ما تخص حقوق الشخص المعني بالمعالجة، والتزامات المسؤول عن المعالجة.

ونصت **المادة (24)** على ما يلي: مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر، يعاقب بالغرامة التي لا تزيد على خمسة ملايين ﷼، كلَّ من خالف أيًا من أحكام المواد: (13)، (16)، (فقرة ثالثة)، (17) من هذا القانون.

حيث نصت **المادة (23)** نصت على أنه يقع على عاتق المراقب، أو المعالج اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية من الضياع، أو التلف، أو التعديل، أو الإفشاء، أو الوصول إليها بشكل غير مشروع، وعلى المعالج أن يخطر المراقب عند وجود أي خطر يهدد البيانات الشخصية للأفراد بأي وجه.

أما الفقرة الثالثة من المادة (16) فنصت على أنه لا يجوز معالجة البيانات الشخصية ذات الطبيعة الخاصة إلا بعد التصريح بذلك من قبل الإدارة المختصة.

والمادة (17) نصت على أنه يجب على أي مالك، أو مشغِّل أي موقع إلكتروني موجَّه للأطفال مراعاة وضع إخطار على الموقع؛ حول ماهية بيانات الأطفال، وكيفية استخدامها، والسياسات التي يتبعها في الإفصاح عنها، والحصول على موافقة صريحة من ولي أمر الطفل الذي تتم معالجة البيانات الشخصية عنه، وذلك عن طريق اتصال إلكتروني، أو أي وسيلة أخرى مناسبة، و وتزويد ولي أمر الطفل بناءً على طلبه، وبعد التحقق من هويته، وصفٍّ نوع البيانات الشخصية التي تتم معالجتها مع بيان الغرض من المعالجة، ونسخة من البيانات التي تمَّت معالجتها، أو جمعها عن الطفل، وحذف او محو أو وقف معالجة أي بيانات شخصية تم جمعها من الطفل أوعنه إذا طلب ولي الامر ذلك، وألا تكون مشاركة الطفل في لعبة أو عرض جائزة أو أي نشاط آخر مشروطًا بتقديم

الطفل بيانات شخصية تزيد على ما هو ضروري للمشاركة في هذا النشاط [1]، لا بد من الإشارة الى ان المشرع القطري جانب الصواب عندما أولى حماية لفئة الأطفال في مواجهة التقنية الرقمية.

والمادة (25) نصت على عقوبة الشخص المعنوي المخالف بالغرامة التي لا تزيد على مليون ريال إذا ارتكبت باسمه ولحسابه إحدى الجرائم التي نص عليها القانون، ومع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

نصت المادة (24) من قانون حماية البيانات **الشخصية الإماراتي** على أنه لصاحب البيانات تقديم شكوى إلى مكتب حماية البيانات في حال وجد مخالفة لأحكام قانون حماية البيانات الشخصية، أو أن المتحكم أو المعالج قام بمعالجة البيانات بما يخالف أحكام القانون، حيث يتولَّى المكتب استلام الشكاوى والتحقق منها بالتنسيق مع المتحكم أو المعالج، وفي حال ثبوت المخالفة من قبل المتحكم أو المعالج للمكتب صلاحية توقيع الجزاءات الإدارية، وحيث أعطى الحق لكل ذي مصلحة التظلم بشكل خطي لمدير عام المكتب من أي قرار، أو جزاء إداري اتُّخِذ في حقه من قبل المكتب، وذلك خلال 30 يوما من تاريخ إخطاره بذلك الجزاء أو القرار، ويتم البتُّ فيه خلال 30 يوما من تقديمه، وذلك جاء في نصِّ المادة 25 من ذات القانون.

لم يذكر **القانون الإماراتي** الخاصة في حماية البيانات الشخصية الجزاءات والمخالفات الإدارية، بل نص في المادة (26) من قانون حماية البيانات الشخصية، يصدر مجلس الوزراء بناءً على اقتراح مدير عام المكتب قراراً بتحديد الأفعال التي تشكل مخالفة لأحكام قانون حماية البيانات الشخصية، والجزاءات الإدارية التي يتم توقيعها.

---

(1) المادة 17/ قانون حماية البيانات الشخصية القطري لسنة 2016.

الفرع الثاني: المسؤولية الجزائية في التشريع الأردني

لقد نصَّ المشرِّع الأردني في قانون الجرائم الإلكترونية في المادة الثالثة الفقرة الأولى منها على أنه يُعاقَبُ كلَّ من دخل قصداً إلى الشبكة المعلوماتية، أو نظام معلومات بأي وسيلة دون تصريح، أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع، ولا تزيد على ثلاثة أشهر، أو بغرامة لا تقل عن مئة دينار، ولا تزيد على مائتي دينار، أو بكلتا العقوبتين.

وفي الفقرة الثانية نصَّت على أنه أن كان الهدف من الدخول إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشركة المعلوماتية أو نظام معلومات الشبكة المعلوماتية يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنة، وبغرامة لا تقل عن 200 دينار، ولا تزيد عن ألف دينار.

أما الفقرة الثالثة فنصَّت على أنه يعاقب كل من دخل قصدا إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنة وبغرامة لا تقل عن 200، ولا تزيد على (1000) ألف دينار.

يلاحظ من النص السابق أنه في الفقرة الأولى عالج المشرِّع الأردني مسألة الدخول إلى الشبكة المعلوماتية أو نظام معلومات بدون تصريح، والفقرة الثانية عالجت مسألة الدخول بهدف القيام بأفعال غير مشروعة؛ كالتغيير والتعديل أو نسخ بيانات أو معلومات أو الحجب ....الخ ، فالمشرِّع الأردني لم يحدِّد طبيعة المعلومات، أو البيانات التي قد يتم نسخها، أما الفقرة الثالثة فجرَّمت الأفعال غير المشروعة التي قد تقع على الموقع الإلكتروني كإتلافه، أو انتحال صفته أو انتحال شخصية مالكه، ورتَّبت عقوبة الحبس والغرامة معاً، نصَّت المادة الرابعة من قانون الجرائم الإلكترونية على ما يلي:

"يعاقب كل من أدخل أو نشر أو استخدم قصداً برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليه أو تغيير موقع الكتروني أو الغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنة، وبغرامة لا تقل عن (200) مائتي دينار، ولا تزيد على (1000) ألف دينار".

إن المشرِّع **الأردني** لم يحدِّد طبيعة المعلومات أو البيانات التي يتم الاطلاع عليها في المادة السابقة، ونصَّ في المادة الخامسة منه على أنه يعاقب كل من قام قصدا بالتقاط أو باعتراض أو بالتنصت أو أعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن 200 مائتي دينار، ولا تزيد على ألف دينار.

إن المشرِّع في المادة السادسة من ذات القانون نصَّت على أنه يعاقب كل من حصل قصداً دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق بطاقات الائتمان أو بالبيانات او بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة، ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (500) خمسمائة دينار، ولا تزيد على (2000) ألفي دينار.

ونصَّت المادة السابعة على أنه يعاقب كل من قام بأحد الأفعال المنصوص عليها في المواد السابقة (3، 4، 5،6)، إذا وقعت على نظام معلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق

بتحويل الأموال أو بتقديم طلبات الدفع أو التقاص أو التسويات أو بأي من الخدمات المصرفية المقدَّمة من البنوك والشركات المالية بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن (5000) خمسة آلاف دينار، ولا تزيد عن (15000) خمسة عشر ألف دينار.

ونصت المادة التاسعة في الفقرة الأولى نصت على أنه: " " يعاقب كل من أرسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالا إباحية وتتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة آلاف دينار".

والفقرة الثانية من هذه المادة عاقبت كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إنشاء أو أعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر من العمر، أو من هو معوَّق نفسياً أو عقلياً، أو توجيهه أو تحريضه على ارتكاب جريمة، بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ألف دينار، ولا تزيد على خمسة آلاف دينار.

كما عاقب المشرِّع الأردني في قانون الاتصالات الأردني رقم 13 لسنة 1995 على ما يلي:" تعتبر المكالمات الهاتفية والاتصالات الخاصة من الأمور السرية التي لا يجوز انتهاك حرمتها وذلك تحت طائلة المسؤولية القانونية [1]".

---

(1) نص المادة (56)، من قانون الاتصالات الأردني.

ونصت المادة 71: " كل من نشر أو أشاع مضمون أي اتصال بواسطة شبكة اتصالات عامة أو خاصة أو رسالة هاتفية اطلع عليها بحكم وظيفته أو قام بتسجيلها دون سند قانوني يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة، أو بغرامة لا تقل عن (100) دينار، ولا تزيد على (300) دينار أو بكلتا العقوبتين".

ونصَّ على أنه:" كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات، أو شجَّع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر، ولا تزيد على ستة أشهر، أو بغرامة لا تزيد على (200) دينار أو بكلتا العقوبتين[1]".

يلاحظ من النصوص القانونية السابق بأن المشرِّع الأردني عاقب كل من يقوم بنشر مضمون اتصال أو رسائل هاتفية بحكم وظيفته، بالإضافة إلى أنه رتَّب عقوبة جزائية لكل من يعترض أو يعيق، أو يشطب محتويات رسالة بواسطة شبكات الاتصال، فلم يتطرق إلى موضوع نقل، أو تداول البيانات الشخصية الخاصة بالأفراد، فالقانون هنا جرَّم تناقل أو نشر أو حور أو شطب محتويات رسالة.

إن المشرِّع الأردني لم يرتِّب حماية للبيانات الشخصية ضمن تشريعاته، حيث إنه جاء خالياً من أي تشريع ينظم مسالة حماية البيانات الشخصية بشكل خاص، باستثناء مسوَّدة القانون لسنة 2016 التي لم تصدر إلى غاية كتابة هذه الدراسة، حيث سنتطرق للحماية الجزائية التي رتَّبتها هذه المسوَّدة، فالمشرِّع الأردني قد حظر فيها القيام بنقل أو تبادل البيانات الشخصية داخل أو خارج المملكة دون التقيد بالأحكام المقرَّرة في مسوَّدة قانون حماية البيانات الشخصية، وحظر أيضاً الحصول على معلومات شخصية بطريقة مضلِّلة، أو عن طريقة الخديعة إدراج أو إدخال بيانات غير صحيحة إلى

---

(1) – نص (المادة 76)، قانون الاتصالات الأردني.

قاعدة البيانات بصورة متعمدة، أو إفشاء البيانات الشخصية دون موافقة الشخص المعني بالمعالجة، أو الوصول غير المشروع أو مراقبتها أو الاطلاع عليها أو الحصول عليها أو توقيفها أو مُصادرتها بشكل مخالف للقانون، أو انتهاك أي من وسائل أمن المعلومات، أو التدابير التقنية الموضوعة لحماية البيانات الشخصية بموجب هذا القانون، أو أن يقوم المسؤول برفض سحب الموافقة على المعالجة، والاستمرار بالمعالجة رغم ذلك، أو القيام بإتلاف البيانات الشخصية، وبناء عليه يترتَّب على تلك الأفعال عقوبة جزائية تتمثل بفرض غرامة لا تقل عن ألف دينار، ولا تزيد على عشرة آلاف دينار[1].

أما فيما يخصُّ الحماية الجزائية للبيانات الشخصية على وجه الخصوص، فقد وردت في مسوَّدة قانون حماية البيانات الشخصية فعاقب المشرِّع الأردني بغرامة لا تقل عن ألف دينار، ولا تزيد على عشرة آلاف دينار، إذا لم يلتزم المعالج بالضوابط القانونية التي نصت عليها المادة (12) بأن لا يتجاوز الغرض المحدَّد للمعالجة ومدتها، وإن لم يلتزم بمحو البيانات بانقضاء مدة المعالجة، وإن لم يلتزم المعالج بسرية البيانات، حيث يقع على عاتقه حمايتها استنادًا الى نصِّ المادة (13) من المسوَّدة، بالإضافة إلى واجب عليه أن لا ينقل البيانات إلا بموافقة صاحبها حيث يقع على عاتقه ضمان سلامة البيانات، وتهيئة الوسائل المناسبة التي تساعد في كشف حالات الاعتداء عليها، وذلك حسب نص المادة (14)

كما يجوز للمحكمة المختصة بناءً على طلب النيابة العامة، أو المتضرِّر، أو من تلقاء نفسها، أن تقضي بإتلاف البيانات الشخصية موضوع الدعوى التي صدر بها قرار قطعي بالإدانة [2]،

(1) نص (المادة 27)، مسودة قانون حماية البيانات الشخصية الأردني.

(2) نص (المادة 29)، مسودة قانون حماية البيانات الشخصية الأردني.

وتتضاعف العقوبة إذا ارتكب أيًّا من الأفعال السابقة من قبل موظف عام، أو إذا تكرَّر الفعل من قبل الشخص نفسه [1].

يرى الباحث أن على المشرِّع الأردني الإسراع في إصدار المسوَّدة الخاصة في حماية البيانات الشخصية، كما يتمنى على المشرِّع إعادة النظر في تشكيلة المجلس؛ لتكون على قدر من الاستقلالية والحياد، وحبذا لو أنه إضافة حماية أكثر للبيانات الحيوية، وبالإضافة إلى أنه كان على المشرِّع الأردني والأجدر به أن يقوم بتغليظ العقوبات الخاصة بانتهاك البيانات الشخصية، أُسوةً بالمشرِّع السعودي والبحريني اللَّذين قرَّرا عقوبة الحبس والغرامة معا، ويُؤخذ على مسوَّدة القانون الأردني الخاصة في حماية البيانات الشخصية أنها جاءت خالية من الإقرار بمسؤولية الشخص الاعتباري أو المعنوي، وتتمنى الدراسة على المشرِّع أن يسير على نهج المشرِّع البحريني الذي قرَّر عقوبة للشخص الاعتباري كما جاء في نص المادة (59).

(1) نص (المادة 30)، مسودة قانون حماية البيانات الشخصية الأردني.

الفصل الخامس
الخاتمة، النتائج، التوصيات

أَوَّلًا: الخاتمة

وبعد البحث والتحليل في موضوع الدراسة المتعلِّق بالحماية الجزائية للبيانات الشخصية، وذلك بعد استعراض ماهية البيانات الشخصية من خلال تعريفها، وبيان طبيعتها، وتوضيح الفرق بينها وبين المعلومات، وبيان نطاق حمايتها ضمن الحق في الخصوصية، بالإضافة إلى التطرق لماهية معالجة البيانات الشخصية، والآثار المترتِّبة عليها، ومن ثم ذكر الجرائم التي تقع عليها، ومن ثم الحديث عن حمايتها، والعقوبات الجزائية المترتِّبة على انتهاكها، وذلك من خلال دراسة مقارنة بين التشريع الأردني وبعض التشريعات العربية، حيث توصلت الدراسة إلى مجموعة من النتائج، وفيما يليها بعض التوصيات.

ثانيًا: النتائج

1- إن البيانات تأتي على عدة صور، فالبيانات الشخصية هي إحدى هذه الصور، فالبيانات قد تكون شخصية؛ كالاسم واللقب، وقد تكون غير شخصية؛ كالبيانات العسكرية او الاقتصادية.

2- ليست جميع البيانات تعتبر بيانات شخصية، فالبيانات المتاحة والبيانات المجهولة التي لا تعرف بهوية أي شخص لا تُعدُّ بيانات شخصية.

3- إن الحق في الخصوصية، والحق في حماية البيانات الشخصية، رغم انهما مترابطان إلا أنهما حقان منفصلان.

4- إن معالجة البيانات الشخصية يجب أن تتم ضمن ضوابط قانونية محددة، فأي معالجة دون التقيد بتلك الضوابط تكون غير مشروعة.

5- إن معالجة البيانات الشخصية تُرتب مجموعة من الآثار حيث تتمثل بالتزامات المسؤول عن المعالجة بالإضافة إلى حقوق الشخص المعني بالمعالجة.

6- إن الانتهاكات التي تقع على البيانات الشخصية تتمثل بعدة جرائم: جريمة إفشاء البيانات الشخصية، جريمة الانحراف عن الغاية من المعالجة، جريمة الجمع والتخزين غير المشروع للبيانات الشخصية، جريمة معالجة البيانات الشخصية دون ترخيص، جريمة الاحتفاظ بالبيانات الشخصية أكثر من المدة القانونية اللازمة.

7- تتمثل حماية البيانات الشخصية في أغلبية القوانين الدولية الخاصة في حماية تلك البيانات، ومنها:

أولا: بالرقابة من خلال هيئة أو مجلس يختص في الإجراءات والتدابير اللازمة لحماية ورقابة البيانات.

ثانيا: ترتيب عقوبات جزائية تتمثل بالحبس والغرامة.

8- المشرِّع الأردني لم يصدر لغاية كتابة الدراسة قانون حماية البيانات الشخصية، فما زال في طور المسوِّدة.

ثالثًا: التوصيات

1- اوصي المشرِّع الأردني بضرورة الإسراع بإصدار قانون حماية البيانات الشخصية؛ وذلك للحفاظ على بيانات الأفراد الشخصية في ظل التطورات التقنية التي أصبحت مصدرا يهدد أمنهم وسريرتهم، أُسوةً بباقي الدول العربية والأجنبية.

2- اوصي المشرِّع الأردني بضرورة تعديل نص المادة الرابعة من مسوَّدة مشروع قانون حماية البيانات الشخصية، وذلك من خلال إعادة النظر بتشكيلة مجلس حماية البيانات الشخصية،

بأن يتم اختيار رئيس المجلس بطريق الانتخاب، وأن لا يتكون المجلس من السلطة التنفيذية، فمن المعلوم أن السلطة التنفيذية هي المسؤولة عن معالجة البيانات الشخصية، فلا يعقل أن تكون الجهة المعالجة هي ذات الجهة التي تراقب وتحمي البيانات، وبالتالي فإن المشرِّع وقع بإشكالية عدم الاستقلالية والحياد التي يجب أن يتمتع بها المجلس المسؤول عن مراقبة وحماية البيانات الشخصية.

3- اوصي المشرِّع الأردني بضرورة إقرار المسؤولية الجزائية للشخص المعنوي أُسوةً بالمشرِّع البحريني.

4- كما لا بدَّ من توفير حماية أكبر لمعالجة البيانات الشخصية الخاصة بالأطفال في ظل استخدام الأجهزة الإلكترونية من خلال موافقة ولي الطفل على المعالجة، وذلك بما أخذ به المشرِّع القطري في قانون حماية البيانات الشخصية في نص المادة 17 منه.

5- اوصي المشرِّع الأردني بضرورة تأمين حماية أكبر للبيانات الحيوية (البيرومترية) في ظل رقمنة الهوية.

6- بالإضافة إلى أن الباحث يوصي المشرِّع الأردني بتغليظ العقوبات المترتبة على انتهاك البيانات الشخصية، أُسوةً بالمشرِّع البحريني.

قائمة المراجع

أَوَّلًا: الكتب

- إبراهيم، خالد ممدوح (2008)، **أمن المعلومات الالكترونية**، الدار الجامعية.
- البحر، ممدوح خليل، **حماية الحياة الخاصة في القانون الجنائي**، دراسة مقارنة، دار النهضة العربية، القاهرة.
- الحسيني عمار عباس (2017)، **جرائم الحاسوب والانترنت والجرائم المعلوماتية**، منشورات زين الحقوقية، بيروت، لبنان.
- الحسيني، عمار عباس (2017)، **التصوير المرئي والتسجيل الصوتي وحجيتهما في الاثبات الجنائي**، دراسة مقارنة المركز العربي للنشر والتوزيع، ط 1.
- الحسيني، محمد يحيى، **الحماية القانونية للبيانات الشخصية**، دراسة مقارنة بين القانون البريطاني والاماراتي، دار القضاء.
- الخلايلة، عايد رجا، (2011)، **المسؤولية التقصيرية الإلكترونية**، دراسة مقارنة، دار الثقافة للنشر والتوزيع الطبعة الثانية.
- الزعبي، جلال محمد، المناعسة، أسامة احمد، (2010)، **جرائم تقنية نظم المعلومات الإلكترونية**، دراسة مقارنة، دار الثقافة للنشر والتوزيع.
- الزعبي، علي أحمد عبد، (2006)، **حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب**، طرابلس، لبنان.
- شمس الدين، أشرف توفيق، (2007)، **الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية**، دار النهضة العربية.
- الشوابكة، محمد أمين، (2011)، **جرائم الحاسوب والانترنت**، دار الثقافة للنشر والتوزيع.
- العادلي، محمود صالح (2006)، **الحماية الجنائية لأسرار المحامي للمحافظة على أسرار موكليه**، دراسة مقارنة، الإسكندرية دار الفكر الجامعي.

- عبد الله، عبد الكريم عبد الله، **جرائم المعلوماتية والانترنت**، منشورات الحلبي الحقوقية.

- عمر، رشاد خالد، (2013)، **المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية**، دراسة تحليله مقارنة، المكتب الجامعي الحديث.

- قورة، نائلة عادل محمد فريد، **جرائم الحاسب الآلي الاقتصادية**، دراسة نظرية وتطبيقية، مصر.

- محمد، محمود عبد الرحمن، نطاق **الحق في الحياة الخاصة دراسة مقارنة**، دار النهضة العربية، القاهرة.

- المضحكي، حنان ريحان، (2014) **الجرائم المعلوماتية** "دراسة مقارنة"، ط1، منشورات الحلبي الحقوقية، بيروت.

- الهيتي، محمد حماد مرهج، (2006)، **جرائم الحاسوب، دراسة تحليلية**، دار المناهج للنشر والتوزيع، ط1، الأردن.

ثانيًا: الرسائل والأُطروحات العلمية

- السكر، سلطان فياض محمد، (2022)، **جريمة انتهاك سرية المعلومات عبر الوسائل الالكترونية في التشريع الأردني**، رسالة ماجستير، جامعة الشرق الأوسط كلية الحقوق.

- صبرينة، بن سعيد، (2015)، **حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا "الإعلام والاتصال"**، رسالة دكتوراه، منشورة، جامعة لحاج خضر، باتنه، الجزائر.

- العابدين، مروة زين، (2016)، **الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت، بين القانون الدولي الاتفاقي والقانون الوطني**، رسالة دكتوراه، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر.

- لامي، بارق منتظر عبد الوهاب، (2017)، **جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني**، رسالة ماجستير، جامعة الشرق الأوسط.

- مرنيز، فاطمة، **حرمة الحق في الخصوصية للعامل في ظل الوسائل التكنولوجية الحديثة**، رسالة دكتوراه منشوره.

ثالثا: البحوث والدوريات

- أحمد، خالد حسن، (2020)، **الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية**، دراسة مقارنة.

- العيداني، محمد (2018). **حماية المعطيات الشخصية في الجزائر على ضوء قانون رقم (07/18)**، مجلة معالم للدراسات القانونية والسياسية، عدد 5.

- أرجدال علي (2019)، **حماية المعطيات الشخصية بالمغرب، دراسة تحليلية مقارنة**، جامعة محمد الخامس، كلية العلوم القانونية، الرباط، رسالة لنيل دبلوم الماستر في القانون العام، (droitarabic.com).

- الأشقر، منى، الأشقر محمود، **البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد** ، المركز العربي للبحوث القانونية والقضائية، ط1، لبنان (archive.org) .

- بوعمرة، آسيا، **الحماية المزدوجة لقواعد البيانات، المجلة الجزائرية للعلوم القانونية،** (https://www.asjp.cerist.dz/en/article/) .

- جابر، أشرف (2015)، **استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق في الخصوصية**، مجلة العلوم الإنسانية جامعة الاخوة منتوري، الجزائر.

- الدهبي، خديجة (2017)، **حق الخصوصية في مواجهة الاعتداءات الالكترونية** ، دراسة مقارنة، مجلة الأستاذ الباحث القانوني للدراسات القانونية، عدد 8،(https://www.asjp.cerist.dz/en/article/)

- الرابحي عزيزة (2018)، **الاسرار المعلوماتية وحمايتها الجزائية**، رسالة دكتوراه منشورة، جامعة أبو بكر بلقايد، تلسمان، كلية الحقوق،

- الزهرة جرقيف، (2021)، **الحماية الجزائية للمعطيات ذات الطابع الشخصي في التشريع الجزائري**، مجلة العلوم القانونية والاجتماعية، المجلد السادس، العدد الرابع.

- الشافعي، آمال، ام السعد شافعي، ال**تأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوربي**، بحث منشور، مجلة الباحث القانوني، مجلد 1 عدد2، جامعة الحاج لخضر، باتنه.

- الصالحين محمد، **التنظيم القانوني لاستخدام البيانات الشخصية في الاعلام الجديد**، كلية الحقوق، جامعة بن غازي، مجلة الحقوق، مجلد13

- طباش، عز الدين، (2018)، **الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري**، المجلة الأكاديمية للبحث القانوني، العدد2 .

- عثمان، طارق، (2007)، **الحماية الجنائية للحياة الخاصة عبر الانترنت**، دراسة مقارنة، كلية الحقوق، جامعة محمد خيضر.

- محمد أحمد سلامة مشعل، **الحق في محو البيانات الشخصية**، دراسة تحليلية في ضوء لائحة حماية البيانات الأوربية (GDPR)، وأحكام المحاكم الأوربية، أستاذ في جامعة الزقازيق.

- المعداوي، محمد احمد، **حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي**، (https://search.mandumah.com/).

- المعمري، مسعود بن حميد، **نطاق الحماية الجزائية للحق في الخصوصية**، دراسة مقارنة، مجلة كلية القانون الكويتية العالمية

- يحي، تومي، (2020)، **الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء قانون رقم 18-07**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية مجلد 4 عدد2.

- عرب، يونس، **دور حماية الخصوصية في تشجيع الاندماج الرقمي**، المركز الوطني للتوثيق، (http://thiqaruni.org).

رابعًا: القوانين والأنظمة

- دستور المملكة الأردني لسنة 1946.

- دستور دولة الإمارات العربية المتحدة (1971).

- قانون العقوبات الاتحادي لدولة الامارات العربية (1987).

- قانون العقوبات الاردني لسنة 1960.

- قانون حماية البيانات الشخصية البحريني لسنة 2018.

- قانون حماية البيانات الشخصية القطري رقم 13 لسنة 2016.
- قانون رقم 45 لسنة (2021)بشأن حماية البيانات الشخصية، دولة الامارات.
- مسودة قانون حماية البيانات الشخصية الأردني لعام 2022.
- نصوص اللائحة الأوربية العامة.

خامسًا: الاتفاقيات

- الاتفاقية الامريكية لحقوق الانسان لعام 1969.
- العهد الدولي للحقوق المدنية والسياسية الصادر عام 1966.
- نصوص ومواد الاتفاقية الأوروبية لحقوق الإنسان.
- اتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا في 4 نوفمبر 1950.

سادسًا: المواقع الإلكترونية

- (mandumah.com)
- (https://ontology.birzeit.edu/term//)
- (https://mawdoo3.com/)
- (The Origins and History of the Right to Privacy (thoughtco.com)
- (General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu)
- (https://gdprhub.eu/index.php?title=AEPD_-_N%C2%BA:_TD/00005/202-)
- (https://www.asjp.cerist.dz/en/article/17021-)
- (mohamah.net)
- (https://www.asjp.cerist.dz/en/PresentationRevue/72)
- (https://search.ebscohost.com/login.aspx?authtype=uid)