جـامـعـة الـشـرقـيـة
A' SHARQIYAH UNIVERSITY

كـــلـيـة الـحـقـوق

قسـم القانـــون العـــام

الحماية الجزائية للبيانات الشخصية في الفضاء الرقمي

"دراسة مقارنة"

إعداد الباحث

المعتصم بن ناصر بن المر الصباري

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام

تخصص القانون الجزائي

إشراف:

الدكتور/ نـزار حـمـدي قـشـطـه

لجنة المناقشة:

إسم عضو اللجنة	الرتبة الاكاديمية	جهة العمل	الصفة
د. نزار حمدي قشطه	أستاذ مشارك	جامعة الشرقية	مشرفاً ورئيساً
د. أحمد بن صالح البرواني	أستاذ مساعد	جامعة الشرقية	مناقشاً داخلياً
د. جمعة بن مسلم العزري	أستاذ مساعد	جامعة السلطان قابوس	مناقشاً خارجياً

سلطنة عُمان

(2025م-1447هـ)

لجنة مناقشة الرسالة

1. رئيس اللجنة ومشرفًا: **د. نزار حمدي إبراهيم قشطة**

الدرجة العلمية: أستاذ مشارك

القسم: القانون العام

الكلية: كلية الحقوق – جامعة الشرقية

التاريخ: 25 من ربيع الأول 1447هـ

التوقيع: 

الموافق: 17 من سبتمبر 2025م

2. عضوًا وممتحنًا داخليًا: **د. أحمد بن صالح البرواني**

الدرجة العلمية: أستاذ مساعد

القسم: القانون العام

الكلية: كلية الحقوق – جامعة الشرقية

التاريخ: 25 من ربيع الأول 1447هـ

التوقيع: 

الموافق: 17 من سبتمبر 2025م

3. عضوا وممتحنًا خارجيًا: د. **جمعة العزري**

الدرجة العلمية: أستاذ مساعد

القسم: القانون الجزائي

الكلية: كلية الحقوق– جامعة السلطان قابوس

التاريخ: 25 من ربيع الأول 1447هـ

التوقيع: 

الموافق: 17 من سبتمبر 2025م

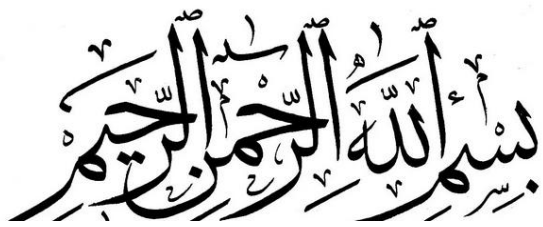
إقـرار الباحــث

أقرّ بأنّ المادة العلمية الواردة في الرسالة قد تمّ تحديد مصدرها العلمي، وأنّ محتوى هذه الرسالة غير مقدم للحصول على أي درجة علمية أخرى، وأنّ مضمون هذه الرسالة يعكس آراء الباحث الخاصة، وهي ليست بالضرورة الآراء التي تتبنّاها الجهة المانحة.

ولا مانع لديّ من قيام الجامعة باستنساخ رسالة الماجستير أو أي جزء منها، وإهداء نسخ منها للجامعات والجهات الأخرى.

الباحث: المعتصم بن ناصر بن المر الصباري الرقم الجامعي: 2214521

التوقيع:



﴿ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡم وَلَا تَجَسَّسُواْ وَلَا يَغۡتَب بَّعۡضُكُم بَعۡضًاۚ أَيُحِبُّ أَحَدُكُمۡ أَن يَأۡكُلَ لَحۡمَ أَخِيهِ مَيۡتا فَكَرِهۡتُمُوهُۚ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ تَوَّاب رَّحِيم ﴾

صدق الله العظيم

سورة الإسراء – الآية (12)

إلى من علّموني معنى الحياة، وقدّموا لي كل الدعم والحب.

إلى من ساندوني في كل خطوة، وكانوا خير معين لي في مسيرتي.

إلى والدي ووالدتي إلى عائلتي التي كانت مصدر إلهامي وقوتي.

أهدي هذا العمل المتواضع ثمرة جهدي وعزمي.

الباحث:

شكر وتقدير

أتقدم بجزيل الشكر والعرفان لأستاذي الفاضل الدكتور/ نزار حمدي قشطه

الذي تشرفت بالإشراف الأكاديمي منه على هذه الرسالة؛ وكان لدعمه العلمي وتوجيهاته القيمة الأثر الأعمق في إثراء هذا البحث، وله مني كل التقدير على ما بذله من صبر وتفانٍ.

كما أتوجه بخالص الامتنان إلى أعضاء لجنة المناقشة الكريمة لجهودهم وملاحظاتهم التي أضافت الكثير إلى جودة هذا العمل.

ولا يمكنني أن أنسى فضل عائلتي، التي كانت مصدر إلهامي وصبري، فلهم مني أعمق الحب والامتنان، والشكر موصول لكل من مد لي يد العون والمساعدة من أساتذة وزملاء وأصدقاء خلال هذه المسيرة العلمية.

الباحث:

الملخص

تتناول هذه الدراسة بشكل شامل الحماية الجزائية للبيانات الشخصية في الفضاء الرقمي؛ مع التركيز على دراسة التشريعات في سلطنة عُمان و المملكة الأردنية الهاشمية، وتبدأ الدراسة بالإشارة إلى أن التطور الهائل في تقنيات الاتصال الحديثة، وعلى الرغم من فوائده العديدة قد أوجد تهديدات جديدة للخصوصية، حيث أصبحت البيانات الشخصية عرضة للسرقة والاختراق والاستخدام غير المشروع، وتؤكد الدراسة أن الأمن المعلوماتي أصبح جزءًا لا يتجزأ من الأمن القومي؛ مما يستدعي إحداث توازن بين الاستفادة من التقنية وحماية حقوق الأفراد في سرية بياناتهم، و تتمحور إشكالية الدراسة حول مدى فعالية الإطار القانوني الحالي في مواجهة الجرائم المتعلقة بالبيانات الشخصية؛ خصوصاً في ظل التنامي المستمر للتهديدات الإلكترونية، ولحل هذه الإشكالية تطرح الدراسة مجموعة من التساؤلات أبرزها: كيفية تحقيق التوازن بين الاستخدام الفعال للتقنيات الحديثة وحماية الخصوصية الشخصية وما هي أبرز التحديات التي تواجه الأجهزة الأمنية في مواجهة الجرائم المعلوماتية وكيف يمكن تحسين وتطوير التشريعات القائمة ولتحقيق هذه الأهداف اعتمدت الدراسة على منهجية بحثية متكاملة؛ تجمع بين المنهج الوصفي والتحليلي لدراسة الوضع القانوني الراهن في سلطنة عُمان والأردن، كما استخدمت الدراسة المنهج المقارن لتحديد نقاط القوة والضعف في التشريعات؛ خاصةً عبر المقارنة مع التشريع الأردني الذي يمتلك إطارًا قانونيًا متكاملًا في هذا المجال، وخلصت الدراسة إلى أن التشريعات العُمانية مثل قانون مكافحة جرائم تقنية المعلومات وقانون حماية البيانات الشخصية قد أحرزت تقدمًا في تجريم الأفعال التي تمس البيانات الشخصية وفرضت عقوبات مالية وسجنية، ومع ذلك تواجه هذه التشريعات تحديات في التطبيق مما يستدعي مراجعتها وتحديثها بما يتناسب مع التطورات التقنية المستمرة؛ لذلك يوصي الباحث بضرورة إنشاء هيئة أو سلطة وطنية مستقلة تتولى الإشراف على تنفيذ قوانين حماية البيانات الشخصية.

الكلمات المفتاحية: البيانات الشخصية، الفضاء الرقمي، الجرائم المعلوماتية، الأمن الرقمي، الخصوصية.

Abstract

This study comprehensively addresses the criminal protection of personal data in the digital space, focusing on the study of legislation in the Sultanate of Oman and the Hashemite Kingdom of Jordan. The study begins by pointing out that the tremendous development in modern communication technologies, despite its many benefits, has created new threats to privacy, as personal data has become vulnerable to theft, hacking, and illegal use. The study confirms that information security has become an integral part of national security, which requires striking a balance between benefiting from technology and protecting the rights of individuals to the confidentiality of their data. The problem of the study revolves around the effectiveness of the current legal framework in confronting crimes related to personal data, especially in light of the continuous growth of electronic threats. To solve this problem, the study raises a set of questions, most notably: How to achieve a balance between the effective use of modern technologies and the protection of personal privacy? What are the most prominent challenges facing security agencies in confronting cybercrimes? How can existing legislation be improved and developed? To achieve these goals, the study relied on an integrated research methodology that combines the descriptive and analytical approach to study the current legal situation in the Sultanate of Oman and Jordan. The study also used the comparative approach to identify the strengths and weaknesses of legislation, especially through comparison with Jordanian legislation, which has a comprehensive legal framework in this field. The study concluded that Omani legislation, such as the Anti-Cybercrime Law and the Personal Data Law, has made progress in criminalizing acts that affect personal data and has imposed financial and prison penalties. However, these laws face implementation challenges, which necessitate review and updating them to keep pace with ongoing technological developments.

Keywords: personal data, digital space, cybercrime, digital security, privacy.

المقدمة:

تقنية الاتصال الحديثة ووسائل الاتصال لها دور كبير في تطور المجتمعات وتحويلها من مجتمع الصناعة إلى مجتمع المعلومات والمعرفة حيث تساهم هذه التقنيات في تحديث الخدمات وتوفيرها بشكل أفضل؛ مما يجعل استخدامها من السمات الأساسية للعالم الحديث حتى أصبح كل مرفق يعتمد على هذه التقنيات خاصة القطاعات الخدمية الخاصة والعامة والتي تسعى إلى تقديم خدمات أفضل للأفراد من خلال توفير الجهد والوقت وحتى المسافات ومع الهدف المشترك لتحقيق هذه الغاية تقوم هذه القطاعات بإنشاء بنوك مختلفة للمعلومات حيث أحيانًا يتم استخدام البيانات المخزنة في هذه البنوك لأغراض غير مشروعة أو بيعها للمهتمين بذلك.

كما أن الخدمات والمعاملات الإلكترونية التي أصبحت لها دوراً حيوياً في الاقتصاد الوطني للعديد من الدول تعتمد بشكل أساسي على المعلومات، وهذا يعزز من أهمية المعلومات والحاجة إلى حمايتها بشكل جيد، ومع ذلك تعاملت العديد من الدول في البيئة الرقمية مع ضعف مستوى الحماية المقررة للبيانات والمعلومات الشخصية من خلال– استخدام العديد من المواقع على الإنترنت، بما في ذلك مواقع التواصل الاجتماعي والخدمات الأخرى وهذا يمكن أن يشكل خطورة على خصوصية المستخدمين خاصة مع ضعف مستوى الأمن والحماية في تلك المواقع.

إن تزايد اعتماد المستخدمين على التقنيات الحديثة مع ضعف مستوى الأمن والحماية يجعلهم عرضة دائمة لهجمات إلكترونية تهدف إلى الوصول غير المشروع إلى معلوماتهم وبياناتهم الشخصية وتتعاظم المخاطر أيضًا بسبب متطلبات الجهود الوطنية والدولية لمكافحة الإرهاب والجريمة المنظمة التي تفرض الكشف عن

البيانات وتبادلها بين الدول، مما يعرضها لأعمال القرصنة والاطلاع غير المشروع و هذه الزيادة الهائلة في حجم البيانات والمخاطر المترتبة عليها والتي قد تؤدي إلى خسائر جسيمة على الصعيدين الأمني والاقتصادي للدولة تجعل من الأمن المعلوماتي جزءاً لا يتجزأ من منظومة الأمن القومي للسلطنة (أو أي دولة) وتستدعي الدفاع عن مواطنيها وأجهزتها المختلفة وعلى الرغم من التأثيرات المختلفة للتقنية فإن توظيفها السيئ يشكّل تهديداً كبيراً ومستمراً على خصوصية البيانات والمعلومات الشخصية للمستخدمين ويتصاعد هذا التهديد مع زيادة الاعتماد على هذه الوسائل.

ولا شك في أن التقنيات الحديثة في مجال الاتصال والمعلوماتية لها تأثير كبير ومتزايد على حقوق الأفراد وحرياتهم. على سبيل المثال، ارتفعت شكاوى الأفراد المتعلقة بالخصوصية بشكل قياسي، حيث سجلت اللجنة الوطنية للمعلوماتية والحريات في فرنسا (CNIL) وحدها ما مجموعه 16,433 شكوى في عام 2023، مسجلة زيادة بنسبة 35% مقارنة بالعام السابق، مما يؤكد تنامي الوعي بضرورة حماية البيانات الشخصية.

وقد سَجَلَتِ الأعوام الأخيرة تزايدًا غير مسبوق في عدد الهجمات الإلكترونية على النظم المعلوماتية بالدول العربية وتشير التقارير إلى أن قطاعات مثل الحكومة والقطاع العام هي الأكثر استهدافًا في منطقة الشرق الأوسط، ويليهما قطاعات الخدمات المالية والطاقة وقد وصل متوسط التكلفة الإجمالية لاختراق البيانات في منطقة الشرق الأوسط وشمال إفريقيا إلى 8.75 مليون دولار أمريكي في عام 2024؛ مما يضع المنطقة بين أعلى المعدلات العالمية ومؤكداً حجم الخسائر الجسيمة التي تترتب على الصعيدين الأمني والاقتصادي.

ولا شك في أن الأمر يحتاج إلى إحداث توازن بشكل يضمن الاستفادة من التقنية ووسائل الاتصال الحديثة مع ضمان حماية حق الفرد في سرية البيانات والمعلومات الشخصية وعدم التعرض لهذا الحق ومن

أجل ذلك فقد عَنتِ الكثير من الدول ومنها سلطنة عُمان والأردن؛ بوضع تشريعات تكفل تنظيم استخدام تقنية المعلومات بحيث تكون في خدمة الفرد لا وبالًا عليه تنتهك من خلالها الحقوق والحريات الفردية أو العامة وفي المنطقة العربية يمكن ملاحظة زيادة اعتماد مؤسسات ومرافق الدولة على البيانات الشخصية واستخدامها لأغراض مختلفة و هذا يجعلنا نتساءل عن مدى الحماية الجنائية التي تتمتع بها البيانات الشخصية الإلكترونية في تلك الدول خصوصاً في ظل تنامي استخدام تقنية المعلومات في مختلف المجالات؛ لذلك تهدف هذه الدراسة إلى تقديم فهم شامل للحماية الجزائية للبيانات الشخصية في الفضاء الرقمي والتحديات التي تواجه هذا المجال والجهود المبذولة لضمان حماية البيانات الشخصية في ظل التطورات التكنولوجية المستمرة.

أولًا: مشكلة الدراسة:

تُشكل حماية البيانات الشخصية في الفضاء الرقمي واحدة من أبرز التحديات القانونية والأمنية التي تواجه المجتمعات الحديثة فعلى الرغم من التطور الهائل في التكنولوجيا ووسائل الاتصال الحديثة وما نتج عنه من اعتماد كلي عليها في القطاعات الحيوية إلا أن هذا التطور جلب معه تهديدات متزايدة تستهدف الخصوصية وتتجلى هذه التهديدات في أشكال متعددة مثل السرقة التقنية والاختراق غير القانوني والإتلاف المتعمد للبيانات والجرائم التي تستهدف الأنظمة المعلوماتية بأكملها.

كما تنبع مشكلة الدراسة من الحاجة الماسة إلى تقييم ودراسة الإطار القانوني للحماية الجزائية (الجنائية) للبيانات الشخصية في ظل هذا التهديد المتصاعد وتحديد مدى كفاية وفعالية التشريعات الوطنية في مواجهة الجرائم المتعلقة بهذه البيانات خاصة مع غياب نصوص قانونية موحدة وشاملة؛ وبالتالي تتلخص المشكلة في

التساؤل الرئيسي ما مدى فاعلية التنظيم القانوني العُماني للحماية الجزائية للبيانات الشخصية في الفضاء الرقمي مقارنة بكل من التشريعات الإماراتية والأردنية في مواجهة التحديات المتجددة للجرائم المعلوماتية؟

ثانيًا: تساؤلات الدراسة.

1- كيف يمكن تحقيق التوازن بين الاستخدام الفعّال للتقنيات الحديثة ووسائل الاتصال وبين حماية الخصوصية الشخصية للأفراد؟

2- ما هي أبرز التحديات التي تواجه الأجهزة الأمنية والتنظيمية في مواجهة الجرائم المعلوماتية المتعلقة بالبيانات الشخصية؟

3- كيف يمكن تحسين وتطوير التشريعات القائمة لتتماشى مع التطورات التكنولوجية المستمرة؟

4- ما هو دور التعاون الدولي في حماية البيانات الشخصية وكيف يمكن تعزيز هذا التعاون؟

5- كيف تؤثر الثقافة الرقمية والعادات الاجتماعية للمستخدمين في فعالية حماية البيانات الشخصية؟

ثالثًا: أهداف الدراسة.

1- تهدف الدراسة إلى فحص الإطار القانوني العُماني والدولي المتعلق بحماية البيانات الشخصية في الفضاء الرقمي وتقييم مدى فعالية النصوص القائمة في مواجهة التحديات الراهنة للجرائم المعلوماتية.

2- تسعى الدراسة إلى تحديد الثغرات القانونية التي يستغلها القراصنة لخرق خصوصية البيانات الشخصية وتقديم توصيات وأطر قانونية لتحقيق التوازن بين استخدام التقنيات الحديثة وحماية البيانات.

3- تهدف الدراسة إلى تسليط الضوء على التحديات التي تواجه الأجهزة الأمنية والتنظيمية في مواجهة الجرائم المعلوماتية وتقديم حلول لتعزيز الأمان الرقمي.

4- تهدف الدراسة إلى تقديم مقترحات لتحسين وتطوير التشريعات القائمة لتتماشى مع التطورات التكنولوجية المستمرة.

رابعًا: أهمية الدراسة:

1- الأهمية العلمية، تُعد هذه الدراسة إضافة نوعية للمكتبة القانونية والأكاديمية حيث تسعى إلى تحقيق ما يلي: تقديم فهم عميق ومنهجي للإطار القانوني الجزائي (الجنائي) الذي يكفل حماية البيانات الشخصية في الفضاء الرقمي والتحليل الدقيق للمفاهيم القانونية المتعلقة بالجرائم المعلوماتية، إثراء الدراسات القانونية المقارنة من خلال تحليل نقدي ومقارن للتشريعات العُمانية مع التشريعات المختارة (الإماراتية والأردنية) في مجال الحماية الجزائية للبيانات؛ مما يفتح آفاقًا جديدة للبحث في التشريعات العربية، و الكشف عن الثغرات ونقاط الضعف القانونية التي قد تعترض تطبيق النصوص الجزائية الحالية وتحديد مدى مواكبتها للتطورات التقنية السريعة خاصة في سياق جرائم الهوية الرقمية والقرصنة.

2- الأهمية العملية والتطبيقية: توفر هذه الدراسة نتائج وتوصيات ذات قيمة مباشرة لصناع القرار والمؤسسات وتشمل ما يلي: مساعدة المشرّع العُماني والأجهزة التنظيمية في تطوير وتحديث القوانين الجزائية ذات الصلة من خلال تقديم توصيات وأطر قانونية واضحة تهدف إلى تعزيز الحماية ضد الجرائم المعلوماتية، و المساهمة في تحصين منظومة الأمن المعلوماتي على المستوى الوطني عن طريق تسليط الضوء على جهود الأجهزة الأمنية والتنظيمية في مواجهة الجرائم العابرة للحدود، مما يدعم الدفاع عن مصالح الدولة وأجهزتها، و المساعدة في إرساء التوازن الضروري بين الاستفادة الكبيرة من التقنيات الحديثة وضرورة حماية خصوصية وحريات الأفراد من الاستخدام غير المصرح به أو الإتلاف المتعمد لبياناتهم التي تُعد "أصولًا رقمية" عالية القيمة.

سادسًا: منهج الدراسة.

تعتمد هذه الدراسة على منهجية تبدأ بالمنهج الوصفي والتحليلي لفحص النصوص القانونية المتعلقة بحماية البيانات الشخصية في الفضاء الرقمي في كل من التشريع العُماني والتشريع الأردني؛ حيث تتشابه سلطنة عُمان والمملكة الأردنية الهاشمية في كونهما دولتين عربيتين ذات نظام قانوني مستمد من الشريعة الإسلامية وهذا التشابه يتيح إجراء مقارنة أكثر دقة وواقعية، وأيضًا دولة الأردن لها السبق في اصدار قوانين لحماية البينات الشخصية؛ ثم بعد ذلك سيتم استخدام المنهج المقارن لإجراء مقارنة دقيقة بين التشريعين لتحديد نقاط القوة والضعف في كل منهما مع التركيز على استخلاص الدروس المستفادة، وأخيرًا سيتم تقييم فعالية تطبيق هذه التشريعات على أرض الواقع وتحديد التحديات التي تواجهها؛ مما يمهد الطريق لتقديم توصيات ومقترحات عملية تهدف إلى تحسين وتطوير التشريع العُماني.

سابعًا: الدراسات السابقة:

الدراسة الأولى: فهد بن عابد الشرقاوي، الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية: دراسة تحليلية، كلية الشريعة والقانون، جامعة الأزهر، دمنهور، مصر، 2023.

تتناول هذا الدراسة موضوع "الإطار القانوني لحماية البيانات الشخصية في تشريعات المملكة العربية السعودية"، تم تقسيم الدراسة إلى مقدمة وثلاثة مباحث وخاتمة وتوصيات المبحث الأول تناول تعريف البيانات الشخصية وأنواعها من خلال مطلبين: المطلب الأول عن تعريف البيانات الشخصية لغة واصطلاحا، والمطلب الثاني عن أنواع البيانات التي حماها النظام السعودي.

المبحث الثاني ركز على حقوق الفرد المتعلقة بالبيانات الشخصية عبر أربعة مطالب: الحق في العلم بالبيانات، الحق في الوصول إلى البيانات، الحق في تصحيح البيانات، والحق في إتلاف البيانات، أما المبحث الثالث فتناول الحماية القانونية للبيانات الشخصية من خلال مطلبين: الأول عن الحماية القانونية للمعلومات الشخصية العادية، وذكر سبعة أوجه للحماية القانونية في النظام السعودي، والثاني عن الحماية القانونية للمعلومات الشخصية الرقمية وذكر بعض الأوجه للحماية القانونية في النظام السعودي، كما تناول ضرورة وضع تعريف شامل للبيانات الشخصية في التشريعات السعودية، تعزيز الحماية القانونية للبيانات الشخصية من خلال تشريعات واضحة وصارمة، الحاجة إلى تحديث القوانين لمواكبة التطورات التكنولوجية وتأمين الحماية الرقمية، و أهمية تفعيل الرقابة والإجراءات القانونية لحماية البيانات الشخصية وضمان فعالية تطبيقها، ولقد

أوصى البحث بوضع ضمانات قانونية وإجرائية فعالة لتعزيز الحماية القانونية للبيانات الشخصية، بما يسهم في توفير حماية شاملة وفعالة لهذه البيانات في ظل التحديات الرقمية المعاصرة.

- أوجه الاتفاق: تتفق الدراستان في تناولهما الموضوع الجوهري المتعلق بـ الحماية القانونية للبيانات الشخصية في سياق التحول الرقمي والاعتماد على التكنولوجيا وتقرّان بأهمية تحديث التشريعات لمواكبة التطورات التكنولوجية وتأمين حماية رقمية فعالة كما تشتركان في التسليم بـ ضرورة وضع ضمانات قانونية وإجرائية قوية وفعالة لتعزيز هذه الحماية والتصدي للتحديات المعاصرة فضلاً عن تناولهما حقوق الأفراد المتعلقة ببياناتهم الأساسية كالحق في الوصول إلى البيانات وتصحيحها أو إتلافها وهي حقوق عالمية تشكل ركيزة الإطار القانوني لكلا البلدين.
- أوجه الاختلاف : يكمن الاختلاف الرئيسي بين الدراستين في النطاق الجغرافي وتركيز المعالجة القانونية؛ فـ الدراسة الحالية تتخصص في مجال الحماية الجزائية (العقابية) للبيانات الشخصية وتجري مقارنة قانونية (وإن كان التركيز الأساسي على سلطنة عُمان كما هو ظاهر من بيانات الرسالة)؛ مما يجعل تركيزها ينصب بشكل أساسي على التجريم والعقوبات و في المقابل تهتم هذه الدراسة بـ الإطار القانوني العام والتحليلي لحماية البيانات في تشريعات المملكة العربية السعودية حيث تتناول الحقوق والتعاريف والحماية القانونية بشكل أوسع يشمل الحماية العادية والرقمية دون اقتصار على الجانب الجزائي مما يمنحها نطاقاً أعم وأشمل للتشريعات المنظمة.

الدراسة الثانية: سامح سامي عرابي المسؤولية الجنائية عن انتهاك الخصوصية المعلوماتية عبر مواقع التواصل الاجتماعي: دراسة مقارنة في القانونين المصري والفرنسي، كلية القانون الجامعة البريطانية، مصر، 2022.

أتاحت شبكة الإنترنت إنشاء مواقع التواصل الاجتماعي بهدف تبسيط التواصل بين المستخدمين دون تكلفة مادية، ومساعدتهم على تبادل المعارف والانفتاح على الثقافات العالمية ومع ذلك ظهرت انتهاكات لخصوصية مستخدمي هذه المواقع، مما استدعى تدخل المشرع الجنائي في مصر وفرنسا لتقرير المسؤولية عن هذه الانتهاكات.

وتنوعت هذه الانتهاكات بحسب الدور الذي يشغله الكيان المعتدي، سواء كان متحكمًا في البيانات الشخصية أو معالجًا لها أو حائزًا عليها، وقد تمثلت إشكالية الدراسة في اتساع نطاق المسؤولية الجنائية عن انتهاك الخصوصية المعلوماتية لمستخدمي مواقع التواصل الاجتماعي، وهدفت إلى تحديد نطاق مسؤولية مشغلي هذه الوسائل عن هذه الانتهاكات.

تتبعت الدراسة قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020، وقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، واعتمدت على المنهج القانوني المقارن لدراسة النظام القانوني الفرنسي وبيان أوجه الاختلاف مع النظام القانوني المصري، لتحقيق أهدافها، تناولت الدراسة في المطلب الأول ماهية الخصوصية المعلوماتية عبر مواقع التواصل الاجتماعي، وفي المطلب الثاني نطاق المسؤولية الجنائية الناشئة عن انتهاك الخصوصية المعلوماتية، مسبوقًا بمطلب تمهيدي عن ماهية النظام المعلوماتي، كما توصلت الدراسة إلى ضرورة تحديد نطاق المسؤولية الجنائية لمشغلي وسائل التواصل الاجتماعي وتوفير الحماية القانونية

اللازمة للبيانات الشخصية لمستخدمي هذه الوسائل، من خلال تشريعات قانونية واضحة وفعالة تحمي خصوصيتهم في ظل التطورات التكنولوجية المستمرة والتحديات الرقمية المعاصرة.

- أوجه الاتفاق: تتفق الدراستان بشكل أساسي على التركيز الجنائي في معالجة انتهاكات البيانات فكلاهما يتناول "المسؤولية الجنائية" أو "الحماية الجزائية" عن انتهاك خصوصية الأفراد في الفضاء الرقمي كما تتشاركان في اعتماد المنهج القانوني المقارن لتحقيق أهدافهما حيث تسعى كلتاهما إلى تحديد نطاق هذه المسؤولية في مواجهة التطورات التكنولوجية المستمرة وتوصي كلتا الدراستين بضرورة توفير حماية قانونية واضحة وفعالة للبيانات الشخصية لمستخدمي الوسائل التقنية مع التأكيد على الحاجة إلى تشريعات فعالة وواضحة لمواجهة التحديات الرقمية المعاصرة.
- أوجه الاختلاف: يكمن الاختلاف الرئيسي في النطاق الجغرافي ونوع الانتهاك المحدد؛ فـ الدراسة الحالية تتناول الحماية الجزائية للبيانات بشكل عام في قانون سلطنة عُمان (مع مقارنة غير محددة هنا) وتتناول البيانات في الفضاء الرقمي بصورة واسعة أما هذه الدراسة فتركز بشكل أدق على انتهاكات الخصوصية المعلوماتية التي تتم عبر "مواقع التواصل الاجتماعي" تحديدًا وتُجري مقارنتها بين القانونين المصري والفرنسي مع التركيز على تحديد نطاق مسؤولية مشغلي هذه الوسائل (المتحكم والمعالج والكيانات الحائزة للبيانات)؛ مما يجعل نطاقها أكثر تخصصاً في بيئة تكنولوجية محددة.

الدراسة الثالثة: ضرغام عبدالله فاضل أبو خمرة، حماية بيانات الأفراد الشخصية عبر شبكة الإنترنت: دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2021

تناولت هذه الدراسة موضوع الحماية المدنية لبيانات الأفراد الشخصية عبر شبكة الإنترنت في إطار مقارن بين القانون الأردني والعراقي، مع الإشارة إلى بعض القوانين العربية من أجل توفير الحماية اللازمة لبيانات الأفراد الشخصية.

وقد تطرقت هذه الدراسة إلى البحث في ماهية البيانات الشخصية محل الحماية، وتبين من خلال البحث أن البيانات الشخصية تشمل جميع المعلومات المتعلقة بالشخص الطبيعي دون الشخص المعنوي وتنقسم إلى نوعين: بيانات عادية وبيانات حساسة يحظر معالجتها إلا بموافقة صاحبها يلاحظ أن جميع هذه البيانات تندرج تحت مظلة حرمة الحياة الخاصة والتي تعتبر من الحقوق الدستورية الأساسية، كما تناولت الدراسة أيضًا الأنماط والوسائل المستخدمة في التعدي على هذه البيانات ومن أبرز صورها مواقع التواصل الاجتماعي، في حين كانت القرصنة الإلكترونية أبرز الوسائل المستخدمة في التعدي على البيانات، هدفت الدراسة إلى محاولة التعرف على التنظيم القانوني الأمثل لحماية البيانات الشخصية للأفراد عبر شبكة الإنترنت في ظل هذه القوانين، وتوصلت الدراسة إلى مجموعة من النتائج، من أبرزها:

تُعَدُّ البيانات الشخصية للأفراد من الحقوق الشخصية، حيث يرتكز أساس حمايتها القانونية على حق الإنسان في حرمة حياته الخاصة مما يوفر لها حماية أمام الجميع أوصت الدراسة المشرعين الأردني والعراقي بوضع ضمانات قانونية وإجرائية فعالة لضمان حماية البيانات الشخصية خلال التطبيق العملي وبناءً على هذه النتائج وتؤكد الدراسة على ضرورة تعزيز الإطار القانوني لحماية البيانات الشخصية عبر الإنترنت لمواجهة التحديات الرقمية المعاصرة وتوفير حماية فعالة وشاملة.

- أوجه الاتفاق: تتفق الدراستان في تناولهما المحور الأساسي المتمثل في حماية البيانات الشخصية للأفراد في البيئة الرقمية وتُسلم كلتاهما بأن الأساس القانوني لحماية هذه البيانات يرتكز على الحق الدستوري في حرمة الحياة الخاصة كما تتقاطع الدراستان في الإشارة إلى أن شبكة الإنترنت ومواقع التواصل الاجتماعي تمثل أبرز الوسائل التي تشهد انتهاكات لهذه البيانات وتتفقان في التوصية بـ ضرورة تعزيز الإطار القانوني ووضع ضمانات قانونية وإجرائية فعالة لمواجهة التحديات الرقمية وتوفير حماية شاملة وفعالة للبيانات في ظل التطور التكنولوجي المستمر.
- أوجه الاختلاف: يكمن الاختلاف المحوري بين الدراسة الحالية وهذه الدراسة في الجانب القانوني محل البحث؛ فـ الدراسة الحالية (الحماية الجزائية للبيانات) تتركز حول المسؤولية الجنائية وتحديد التجريم والعقوبات في هذا المجال و في المقابل تركز هذه الدراسة على الحماية المدنية لبيانات الأفراد عبر الإنترنت مما يجعل مناط بحثها هو التعويض المدني عن الضرر الناجم عن التعدي على هذه البيانات كما تختلفان في النطاق الجغرافي المقارن؛ حيث تهتم الدراسة الحالية بشكل أساسي بالقانون العُماني بينما تجري الدراسة الثالثة مقارنة بين القانونين الأردني والعراقي.

ثامنًا– خطة الدراسة: سنقوم الدراسة إلى فصلين وفقًا لما يلي:

الفصل الأول: الإطار القانوني لحماية البيانات الشخصية.

المبحث الأول: شروط جمع البيانات الشخصية.

المبحث الثاني: حماية البيانات الشخصية بين حقوق الأفراد والضمانات القانونية.

الفصل الثاني: جرائم انتهاك البيانات الشخصية في العصر الرقمي.

المبحث الأول: الجرائم الناتجه عن إساءة استخدام وسائل الفضاء الرقمي

المبحث الثاني: المسؤولية الجزائية عن انتهاك البيانات الشخصية.

الفصل الأول
الإطار القانوني لحماية البيانات الشخصية

في عصرنا الحالي يشهد الإنسان اعتماداً متزايداً على الإنترنت في شتى مناحي حياته، ومع ذلك لا يمكننا إغفال المخاطر الجمة التي تحدق بالمستخدمين في هذا العالم الرقمي وعلى رأسها تلك المتعلقة بانتهاك حرمة الحياة الخاصة عبر الاعتداء على البيانات الشخصية؛ فولوج عالم الإنترنت وشبكات التواصل الاجتماعي يستلزم من المستخدمين الإفصاح عن طائفة من البيانات التي تمكن القائمين على هذه الشبكات من التعرف على هويتهم، وهو ما يضطرهم معه إلى البوح ببيانات لصيقة بشخصيتهم[1]، ونظراً لأن الواقع العملي يشير إلى تفشي صور إساءة استخدام الإنترنت، فقد أسفر ذلك عن ظهور ضرب جديد من التعدي يستهدف النيل من البيانات الشخصية للأفراد، ويشكل هذا الأمر خطراً داهماً على الأفراد، حيث يتم الولوج غير المشروع إلى بياناتهم الشخصية المخزنة عبر شبكة الإنترنت مما يعرضهم للإساءة في حقهم في خصوصية بياناتهم الشخصية، والتي تشمل صوراً شخصية وعائلية وبيانات خاصة بالحالة الصحية والمالية والوظيفية والمهنية والعائلية على وجه العموم[2].

مع ظهور العالم الرقمي أصبحت البيانات الشخصية أكثر عرضة للخطر، حيث يمكن تخزينها ونسخها ومشاركتها بسهولة عبر الإنترنت على الرغم من أن الرقمنة لها فوائدها إلا أنها أدت إلى تقليل خصوصية

---

[1] ضرغام عبد الله فاضل، حماية بيانات الأفراد الشخصية عبر الإنترنت "دراسة مقارنة"، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، 2021، ص 2

[2] باسل فايز حمد القطاطشة، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية: دراسة مقارنة، رسالة دكتوراه جامعة العلوم الإسلامية العالمية، عمان، 2022، ص 9.

البيانات، مما أثار مخاوف بشأن الحماية الجزائية تُعتبر البيانات الشخصية حقوقًا أساسية للفرد وترتبط بكل جوانب حياته، مما يجعلها تستحق الحماية القانونية القصوى.[1].

وتتعاظم أهمية موضوع الحماية الجزائية للبيانات بالنظر إلى أن البيانات ذات قيمة أدبية غير مالية بمعنى أن الإساءة إليها لا تمس الذمة المالية للفرد وإنما تمس الجانب الأدبي؛ لذلك يتعين حماية من تتعلق بهم البيانات من المساس بشرفهم أو اعتبارهم أو كرامتهم أو سمعتهم أو مركزهم الاجتماعي أو حرمة حياتهم الخاصة أو استخدام هذه البيانات على نحو غير مشروع من شأنه أن يهدد مصالح الأفراد وقد سنت العديد من الدول قوانين خاصة لحماية البيانات الشخصية للأفراد منها سلطنة عُمان التي أصدرت مرسوم سلطاني رقم ٦ / ٢٠٢٢ بإصدار قانون حماية البيانات الشخصية وأيضًا اللائحة رقم 24 لسنة 2023 و تعميم رقم ٦ / ٢٠٢٤ بشأن سياسة حماية البيانات الشخصية لوحدات الجهاز الإداري للدولة؛ لذلك سنتناول في هذا الفصل مبحثين:

المبحث الأول: حماية البيانات الشخصية بين حقوق الأفراد والضمانات القانونية.

المبحث الثاني: شروط جمع ومعالجة البيانات الشخصية والضمانات القانونية لحمايتها.

[1] محمد عرفان الخطيب، ضمانات الحق في العصر الرقمي من تبدل المفهوم لتبدل الحماية، قراءة في الموقف التشريعي الأوروبي والفرنسي وإسقاط على الموقف التشريعي الكويتي، بحث منشور على مجلة كلية القانون العالمية، أبحاث المؤتمر السنوي الدولي الخامس من 9 – 10 مايو 2018، الكويت، ملحق خاص العدد 3، الجزء الأول، 2018، ص 258.

المبحث الأول: حماية البيانات الشخصية بين حقوق الأفراد والضمانات القانونية

في عصر تتزايد فيه أهمية البيانات الشخصية كأصول رقمية وتتوسع فيه نطاق استخداماتها في مختلف جوانب الحياة؛ أصبح التنظيم القانوني لهذه البيانات ضرورة ملحة لحماية حقوق الأفراد وضمان خصوصيتهم.

لقد أصبحت البيانات الشخصية التي تتضمن معلومات حساسة مثل الأسماء والعناوين وأرقام الهواتف والسجلات الصحية والمالية، عرضة للانتهاكات والاستغلال غير المشروع، مما يستدعي وضع إطار قانوني شامل ينظم جمع هذه البيانات ومعالجتها وتداولها؛ لذلك يهدف هذا المبحث إلى استكشاف التنظيم القانوني للبيانات الشخصية من خلال تحليل الحقوق التي يتمتع بها الأفراد في حماية بياناتهم الشخصية، واستعراض الوسائل القانونية المتاحة لضمان هذه الحماية، سيُخصص هذا المبحث لدراسة ودراسة الإطار القانوني الذي ينظّم عمليتي جمع ومعالجة البيانات الشخصية، بما في ذلك المبادئ الأساسية مثل الشفافية والموافقة والتقييد بالغرض والسرية والأمان، لذلك سنتناول في هذا المبحث مطلبين:

نتناول الأول حقوق الأفراد في حماية البيانات الشخصية، ونتناول الثاني وسائل الحماية القانونية للبيانات الشخصية.

المطلب الأول: حقوق الأفراد في حماية بياناتهم الشخصية

يجب على المسؤول عن المواقع الإلكترونية توفير آليات تمكن الأشخاص من متابعة بياناتهم الشخصية ومراقبتها، وإجراء التعديلات أو الاعتراضات اللازمة، وسحبها عند الحاجة، مع ضمان شفافية كاملة حول الغايات التي يتم جمع البيانات من أجلها؛ لذلك سنتاول في هذا المطلب فرعين الأول يوضح موقف المشرع

العماني من حقوق الإفراد في حماية بياناتهم الشخصية والثاني نوضح موقف المشرع الأردني ثم نوضح أوجه الاتفاق والاختلاف بين التشريعين [1].

الفرع الأول- موقف المشرع العُماني من حقوق الأفراد في حماية بياناتهم الشخصية:

وررد في النظام الأساسي لسلطنة عُمان مادة 36 " للحياة الخاصة حرمة، وهي مصونة لا تمس وللمراسلات الإلكترونية بكافة أنواعها، والمراسلات الهاتفية، والبرقية، والبريدية، وغيرها من وسائل الاتصال، حرمة وسريتها مكفولة، فلا يجوز مراقبتها، أو تفتيشها، أو الاطلاع عليها، أو إفشاء سريتها، أو تأخيرها، أو مصادرتها إلا في الأحوال التي يبينها القانون، ووفقا للإجراءات المحددة فيه"[2].

ومن هذا المنطلق عرف المشرع العُماني البيانات الشخصية بأنها " هي أي معلومات تحدد هوية فرد طبيعي بشكل مباشر أو غير مباشر وذلك باستخدام معرّف واحد أو أكثر، مثل الاسم، الرقم المدني، المعرفات الإلكترونية، البيانات المكانية، أو معلومات تتعلق بالهوية الجينية، الجسدية، العقلية، النفسية، الاجتماعية، الثقافية، أو الاقتصادية"، وعرف صاحب البيانات الشخصية بأنه" الشخص الطبيعي الذي يمكن التعرف عليه من خلال بياناته الشخصية"[3].

---

[1] محمود حسن إسماعيل، مبادئ علم الاتصال ونظريات التأثير، الطبعة الرابعة، الدار العالمية للنشر والتوزيع، القاهرة، مصر،2004، ص 112.

(2) المادة رقم 36 من النظام الأساسي لسلطنة عُمان الصادر بالمرسوم السلطاني رقم 6 / 2021.

[3] المادة الأولى من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

ونجد أن المشرع العُماني أقر حقوقا لصاحب البيانات في قانون حماية البيانات الشخصية "المواد من العاشرة إلى الثانية عشر" والتي تتمثل في [1]:

أولًا- موافقة صاحب البيانات على معالجة بياناته الشخصية:

تؤسس المادة (10) من قانون حماية البيانات الشخصية مبدأ "الموافقة الصريحة" و"الشفافية" كشرطين أساسيين لأي معالجة قانونية للبيانات حيث لا يجوز معالجة البيانات الشخصية إلا في إطار يضمن الشفافية والأمانة، مع الحفاظ على احترام كرامة الإنسان ويُعد الحصول على الموافقة الصريحة لصاحب البيانات شرطاً لازماً لشرعية المعالجة ولضمان عدم التلاعب أو الغموض و تشدد المادة على أن يكون طلب هذه الموافقة مكتوباً وواضحاً وصريحاً ومفهوماً كما تُلزم المتحكم (الجهة التي تعالج البيانات) بعبء إثبات حصوله على هذه الموافقة الكتابية مما يجعلها ركيزة أساسية لحماية الحقوق الفردية ومحاسبة المتحكمين[2]، ووفقا لما ورد في نص المادة (11) الفقرة (أ) من قانون حماية البيانات الشخصية العُماني يكون لصاحب البيانات الشخصية الحق في "إلغاء موافقته على معالجة بياناته الشخصية وذلك مع عدم الإخلال بالمعالجات التي تمت قبل الإلغاء"[3].

يتمتع صاحب البيانات بحق كامل وغير قابل للاختصار في الاعتراض على جمع ومعالجة بياناته الشخصية، وهو حق مكفول بموجب المادة الرابعة من التوجيه الأوروبي الصادر في عام 1995، ويشمل هذا الحق جوهرًا حقين أساسيين: أولهما إمكانية الاعتراض على أي تدخل أو تتبع أو استقصاء يهدف إلى الكشف

---

[1] المواد من 10 إلى 12 من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (10) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[3] المادة 11 الفقرة (أ) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

عن جوانب حياته الخاصة، وثانيهما، سلطة منع وصول أي معلومات تتعلق بخصوصيته إلى أي طرف ثالث غير مصرح له بذلك [1].

يستطيع صاحب البيانات أن يمارس حقه في الاعتراض على جمع معلوماته الشخصية في مرحلتين:

- **المرحلة الأولى:** عند بدء عملية الجمع مباشرة وذلك بالامتناع عن تقديم المعلومات المطلوبة سواءً بمغادرة الموقع الإلكتروني أو بعدم تعبئة الحقول المخصصة أو عدم تحديد الخيارات المطلوبة.
- **المرحلة الثانية:** بعد بدء عملية الجمع حيث يحق لصاحب البيانات رفض تقديم المعلومات أو نشرها للغير وذلك بتفعيل خاصية "OPT-IN" التي يوفرها الموقع الإلكتروني كما يحق لصاحب البيانات طلب إيقاف معالجة بياناته الشخصية من خلال ممارسة حقه في سحب هذه البيانات [2].

كما يتمتع صاحب البيانات بحق أصيل في طلب وقف معالجة بياناته الشخصية وذلك من خلال آلية تُعرف باسم "OPT-OUT"، حيث يقوم صاحب البيانات بإرسال رسالة إلكترونية إلى الموقع الإلكتروني المعني يعبر فيها صراحة عن رغبته في إيقاف معالجة بياناته الشخصية.

وهذا ما نص عليه المشرع العُماني في المادة (18) الفقرة الثانية من اللائحة التنفيذية لقانون حماية البيانات الشخصية التي نصت على"لصاحب البيانات الشخصية الحق في طلب محو بياناته الشخصية لدى

---

[1] نعيم مغبغب، مخاطر المعلوماتية والإنترنت المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن، بيروت، لبنان، 2000، ص 201.

[2] أحمد بدر، علم المكتبات والمعلومات دراسات في النظرية والارتباطات الموضوعية، الطبعة الأولى، دار الغريب، القاهرة، مصر، 1996، ص 111.

المتحكم إذا ألغى موافقته على معالجة بياناته وذلك دون الإخلال بحكم المادة (17) من هذه اللائحة" والتي تنص على أنه يجوز للمتحكم في البيانات الامتناع عن تنفيذ طلب صاحب البيانات الشخصية بشكل كلي أو جزئي، شريطة أن يكون هذا الامتناع مبررًا بأحد سببين: إما أن يكون الطلب متكررًا بشكل لا يستند إلى مسوغات منطقية أو أن يتطلب تنفيذه جهدًا غير عادي يفوق القدرة التشغيلية المعتادة وفي كل الأحوال يقع على المتحكم التزام بإصدار قرار الرفض وإخطار صاحب البيانات به مُسبباً سبب الرفض بوضوح[1].

ثانيًا– حق تصحيح وتعديل البيانات:

نص المشرع العُماني في المادة (11) الفقرة (ب) من قانون حماية البيانات الشخصية يكون لصاحب البيانات الشخصية الحق في طلب تعديل بياناته الشخصية أو تحديثها أو حجبها[2]، كما يُمنح صاحب البيانات الحق في تعديل أو تغيير أو مسح بياناته الشخصية المحفوظة لدى صاحب الموقع الإلكتروني، وهو حق مكفول بموجب المادة الثانية عشرة من التوجيه الأوروبي لعام 1995 ومدعوم بأغلب التشريعات التي تعترف بهذا الحق مثل القانون الفرنسي لعام 1978 في المادة السادسة والثلاثين و يُعتبر هذا الحق من الضمانات الأساسية لحماية خصوصية الأفراد؛ حيث يتيح لهم التحكم في المعلومات المخزنة عنهم لدى التجار الإلكترونيين

---

[1] المادة 18 /2 من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

[2] المادة 11 الفقرة (ب) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

أو حتى لدى الجهات الرسمية وغير الرسمية، وذلك عن طريق الاطلاع على هذه البيانات وتصحيحها أو استكمال أي نقص فيها[1].

ثالثًا- الحصول على نسخة من البيانات:

صاغ المشرع العُماني في المادة (11) الفقرة (ج) من قانون حماية البيانات الشخصية حقاً صريحاً لصاحب البيانات الشخصية في الحصول على نسخة من بياناته الشخصية التي تتم معالجتها مؤكداً بذلك على مبدأ الشفافية وتمكين الفرد من الوصول إلى معلوماته الخاصة والتحكم فيها"[2]، وهذا ما أكدته أيضًا المادة (19) من اللائحة التنفيذية لقانون حماية البيانات الشخصية والتي تنص على " يحق لصاحب البيانات الشخصية أن يطلب من المتحكم نسخة من بياناته الشخصية المعالجة بصيغة مقروءة وواضحة إلكترونية أو ورقية شريطة التأكد من خلو النسخة التي قدمها من أي بيانات شخصية تحدد هوية شخص آخر"[3].

من وجهة نظر الباحث يُعد النص على حق صاحب البيانات في الحصول على نسخة من بياناته الشخصية في المادة (3/11) من القانون العُماني والمادة (19) من اللائحة التنفيذية خطوة تشريعية مهمة تعكس التزام السلطنة بمعايير حماية البيانات العالمية.

---

[1] محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي، مطبوعات جامعة الكويت، إبريل 1992، ص 114.

[2] المادة 11 الفقرة (ج) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[3] المادة 19 من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

كما تشير إمكانية نقل البيانات إلى حق أصحاب البيانات في نقل بياناتهم الشخصية بين مزودي الخدمات المختلفة مما يضمن لهم حرية اختيار الخدمات، وتجنب الحبس في منصة واحدة ويعزز المنافسة والابتكار، وقد كانت اللائحة العامة لحماية البيانات (GDPR)[1] الصادرة عن الاتحاد الأوروبي رائدة في الاعتراف بهذا الحق[2]؛ حيث تمنح المادة 20 الأفراد الحق في الحصول على بياناتهم بتنسيق منظم وقابل للقراءة آليًا، مما يسهل عمليات نقل البيانات بين المتحكمين والمعالجين، وتفتح إمكانية نقل البيانات فرصًا ريادية للشركات الناشئة؛ حيث يمكنها إنشاء خدمات مبتكرة تتكامل مع المنصات الحالية، وتعزز قابلية التشغيل البيني بين الخدمات المختلفة، وتحفز الشركات على تحسين عروضها، وعلى سبيل المثال تتيح إمكانية نقل البيانات للمستخدمين تنزيل سجلاتهم من منصات التواصل الاجتماعي والخدمات المصرفية؛ مما يمكنهم من استكشاف منصات بديلة، أو تحليل بياناتهم المالية ومع ذلك تثير إمكانية نقل البيانات تحديات تتعلق بالخصوصية والأمان والمعايير الفنية حيث يجب تحقيق التوازن بين سهولة النقل وحماية المعلومات الحساسة، وإنشاء تنسيقات موحدة لنقل البيانات؛ لذا يجب على رواد الأعمال تبني هذا الحق وبناء خدمات تحترم الاستقلال الفردي وتعزز المنافسة، للمساهمة في خلق مشهد رقمي يزدهر بالاختيار والشفافية والتقدم[(3)].

[1] تشير (GDPR) إلى اللائحة العامة لحماية البيانات (General Data Protection Regulation)، وهي القانون الأوربي الذي يمثل الإطار التشريعي الأقوى عالمياً لتوحيد قواعد حماية البيانات الشخصية لجميع الأفراد داخل الاتحاد الأوروبي، ويفرض التزامات صارمة وعقوبات مالية ضخمة على أي جهة تعالج بياناتهم، بهدف تمكين الأفراد من التحكم ببياناتهم بشكل كامل.

[(3)] https://salama-lawfirm.com/personal-data-protection-law/ تاريخ الزيارة 4 إبريل 2025.

رابعًا– نقل البيانات:

يضمن المشرع العُماني لصاحب البيانات الشخصية حقين أساسيين متكاملين: الحصول على نسخة من بياناته، وحق نقل هذه البيانات.

أكدت المادة (11) الفقرة (ج) من قانون حماية البيانات الشخصية والمادة (19) من لائحته التنفيذية على حق صاحب البيانات في الحصول على نسخة من بياناته الشخصية المعالجة سواء كانت بصيغة مقروءة وواضحة (إلكترونية أو ورقية) شريطة التأكد من خلوها من أي بيانات تحدد هوية شخص آخر[1]، ويُعد هذا النص خطوة تشريعية مهمة تعكس التزام السلطنة بحق الوصول إلى البيانات ومع ذلك يلاحظ الباحث أن القانون العُماني لم يشترط بعد توفير هذه النسخة بصيغة قابلة للقراءة آليًا وهو ما يمثل نقطة للتطوير المستقبلي مقارنة ببعض التشريعات الدولية.

كما عزز المشرع هذا الحق في المادة (11) الفقرة (د) من القانون والمادة (20) من اللائحة التنفيذية بمنح صاحب البيانات الحق في نقل بياناته الشخصية من متحكم إلى متحكم آخر. ويهدف هذا الحق إلى تمكين الأفراد من التحكم في بياناتهم وتسهيل تنقلهم بين الخدمات والأنظمة المختلفة، مما يعزز المنافسة والابتكار في السوق الرقمي. وقد ربطت اللائحة التنفيذية هذا النقل بشرط أساسي وهو أن يكون المتحكم الحالي ملزماً قانوناً بذلك، مع التأكيد على ضرورة

[1] المادة 11 الفقرة (جـ) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022، المادة 19 من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

نقل البيانات بتنسيق منظم وقابل للقراءة آليًا، الأمر الذي يُسهّل عمليات النقل ويعكس مواكبة للمعايير الدولية مثل اللائحة العامة لحماية البيانات (GDPR)[1].

خامسًا– محو البيانات:

تنص المادة 11 الفقرة (هـ) من قانون حماية البيانات الشخصية العُماني على حق صاحب البيانات في طلب حذف معلوماته الشخصية من المتحكم مع وجود استثناء هام؛ يتمثل في ضرورة الاحتفاظ بالبيانات لأغراض الحفظ والتوثيق الوطنية، ويجسد هذا الحق رغبة الأفراد في التحكم ببياناتهم وحمايتها من الاستخدام غير المصرح به، بينما يهدف الاستثناء إلى تحقيق التوازن بين هذه الرغبة، والمصلحة الوطنية في الحفاظ على السجلات والأرشيفات التاريخية والتراثية، وقد يشمل هذا الاستثناء حالات أخرى تستدعي الاحتفاظ بالبيانات للامتثال للقانون أو للدفاع عن الحقوق القانونية[(2)].

من وجه نظر الباحث بشكل عام تسعى هذه المادة إلى إيجاد توازن دقيق بين حقوق الأفراد والمصلحة العامة للدولة في الحفاظ على الوثائق والسجلات الوطنية.

ويُعد الحق في محو البيانات من أهم حقوق الأفراد حيث يضمن عدم الاحتفاظ ببياناتهم الشخصية إلى الأبد، ويجب أن تكون هذه البيانات مرتبطة بفترة زمنية محددة، وبعدها يتم حذفها وإزالتها تمامًا، وهذه الضمانة تمنح الأفراد شعورًا بالأمان والراحة، وتزيل عنهم القلق بشأن بقاء بياناتهم محفوظة لفترات طويلة، ويمكن تحقيق

[1] لمادة 11 الفقرة (د) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022، المادة 20 من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

[(2)] المادة 11 الفقرة (هـ) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

ذلك إما بطلب صريح من الفرد المسؤول عن تخزين البيانات لحذفها، أو بتحديد مدة زمنية مسبقة تنتهي عندها الحاجة إلى حفظ البيانات، ثم يتم إتلافها أو حذفها بشكل تلقائي [1].

فعلى سبيل المثال عندما يحصل صاحب البيانات على نسخة من معلوماته (كسجلاته المالية أو نشاطه الرقمي)؛ قد يكتشف أنها لم تعد ضرورية للجهة المتحكمة، فيحق له حينئذٍ طلب المحو إذا انطبقت شروط المادة 18من اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات (كانتهاء الغرض أو سحب الموافقة)، لكن هذا الحق ليس مطلقًا إذ يتعارض أحيانًا مع الالتزامات القانونية (مثل الاحتفاظ بالسجلات المالية لفترة محددة)، أو حسم النزاعات مما يعكس توازن المشرع بين مصلحة الفرد والمتطلبات النظامية[2]، و هذا التكامل بين الحقين يُظهر توجه القانون العُماني نحو تعزيز حقوق الأفراد مع مراعاة الضرورات العملية، مما يسهم في بناء ثقة رقمية متوازنة بين الأطراف المعنية.

سادسًا– سلامة البيانات:

يجب أن يُتاح للفرد الحق في التحقق من سلامة بياناته الشخصية؛ حيث لا يجوز أن تكون هناك بيانات خاطئة أو غير مطابقة للواقع، مما قد يؤدي إلى الإضرار به أو أن تصبح هذه البيانات قديمة وتتضمن أخطاء؛ لذلك يحق لصاحب البيانات الاطلاع عليها وتحديثها أو حتى محو البيانات التي لم تعد موجودة أو التي تم الانتهاء من الغرض منها مع إبلاغ المتحكم بالوضع القائم لتجنب أي مشاكل قد تنجم عن انتشار

---

[1] نعيم مغبغب، المرجع السابق، ص 208.

[2] المادة 18 من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

معلومات خاطئة [1]، وهذا ما أكد عليه المشرع العُماني في المادة (11) الفقرة (ب) من قانون حماية البيانات الشخصية على حق صاحب البيانات في تلقي إخطار من المتحكم في حال وقوع أي اختراق أو انتهاك لبياناته الشخصية؛ بالإضافة إلى إطلاعه على الإجراءات التي تم اتخاذها للتعامل مع هذا الوضع، ويهدف هذا الحق إلى ضمان شفافية عمل المتحكمين في التعامل مع البيانات الشخصية، وإلزامهم بإبلاغ صاحب البيانات في حال تعرض بياناته للخطر، مما يمكنه من اتخاذ الإجراءات اللازمة لحماية نفسه، كما يجب على المتحكم أن يوضح لصاحب البيانات الإجراءات التي اتخذها للحد من الأضرار الناتجة عن الاختراق أو الانتهاك، ويشمل ذلك الإجراءات الأمنية المتخذة والتحقيقات التي تم إجراؤها، وأي إجراءات أخرى تهدف إلى حماية البيانات، وبشكل عام تهدف هذه المادة إلى تعزيز ثقة الأفراد في المتحكمين من خلال ضمان إبلاغهم بأي مخاطر قد تهدد بياناتهم الشخصية، وتمكينهم من اتخاذ القرارات المناسبة لحماية أنفسهم[2].

سابعًا- ممارسة صاحب البيانات لحقوقه:

لقد نصت المادة (16) من اللائحة على حق صاحب البيانات الشخصية في تقديم طلب كتابي للمتحكم لممارسة حقوقه المنصوص عليها في المادة (11) من القانون وذلك بدون مقابل، ويلتزم المتحكم بالبت في الطلب خلال 45 يومًا من تاريخ تسلمه، كما يحق لصاحب البيانات طلب وقف معالجة بياناته الشخصية لحين البت في الطلب [3].

---

[1] محمد عبد المحسن المقاطع، المرجع السابق، ص 118

[2] المادة 11 الفقرة (ب) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[3] المادة 16 من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

من وجهة نظر الباحث بناء على ما سبق إيضاحه يتبنى المشرع العُماني في قانون حماية البيانات الشخصية نظاماً متكاملاً لحقوق أصحاب البيانات؛ حيث يجمع بين الحماية الجوهرية والضمانات الإجرائية، ففي الجانب الجوهري يمنح القانون سبعة حقوق أساسية: (1) حق الموافقة القابلة للإلغاء (المادة 11/أ)، (2) حق التصحيح والتحديث (المادة 11/ب)، (3) حق الحصول على نسخة (المادة 11/ج)، (4) حق نقل البيانات (المادة 11/د)، (5) حق المحو مع استثناءات الأرشفة الوطنية (المادة 11/هـ)، (6) حق ضمان سلامة البيانات (المادة 11/و)، و(7) حق الإخطار بالاختراقات.

أما إجرائياً فإن المادة (16) تضمن فعالية هذه الحقوق من خلال ثلاث ضمانات: آلية طلب كتابي مجاني مهلة زمنية محددة (45 يوماً) وإمكانية وقف المعالجة مؤقتاً، وهذا التكامل بين الجوهر والإجراء يعكس توازناً دقيقاً بين:

أولاً: حقوق الأفراد في التحكم ببياناتهم حيث تتجاوز الحماية العُمانية النموذج التقليدي لتشمل حقوقاً حديثة.

ثانياً: متطلبات المؤسسات عبر منحها وقتاً كافياً للاستجابة مع ضمانات ضد الإساءة.

ثالثاً: المصلحة العامة من خلال استثناءات كالأرشفة الوطنية.

هذا النموذج التشريعي رغم تأثره بالتوجيه الأوروبي؛ يمتاز بخصوصية عُمانية في الموازنة بين الحماية الرقمية ومتطلبات التنمية، مما يجعله نموذجاً يستحق الدراسة في التشريعات العربية.

الفرع الثاني- موقف المشرع الأردني من حقوق الإفراد في حماية بياناتهم الشخصية:

تم إقرار قانون حماية البيانات الشخصية رقم (24) لسنة 2023 والذي يهدف إلى تنظيم جمع ومعالجة البيانات الشخصية وحماية خصوصية الأفراد، ويُعتبر هذا القانون أول تشريع متخصص في حماية البيانات الشخصية في الأردن، ويأتي استجابة للتطورات التكنولوجية وزيادة الاعتماد على البيانات الرقمية.

نص المشرع الأردني في القانون على تعريف البيانات الشخصية بأنها "أي بيانات أو معلومات تتعلق بشخص طبيعي ومن شأنها التعريف به بطريقة مباشرة أو غير مباشرة مهما كان مصدرها أو شكلها، بما في ذلك البيانات المتعلقة بشخصه أو وضعه العائلي أو أماكن تواجده".

كما عرف البيانات الشخصية الحساسة " أي بيانات أو معلومات تتعلق بشخص طبيعي تدل بصورة مباشرة غير مباشرة على أصله أو عرقه أو تدل على آرائه او انتماءاته السياسية أو معتقداته الدينية أو أي بيانات تتعلق بوضعه المالي أو بحالته الصحية أو الجسدية أو العقلية أو الجينية أو بصماته الحيوية (البيومترية) أو بسجل السوابق الجنائية الخاص به أو أي معلومات أو بيانات يقرر المجلس اعتبارها حساسة إذا كان إفشاؤها أو سوء استخدامها يلحق ضررا بالشخص المعني بها"، وكذلك وضح بأن البيانات تشمل " البيانات الشخصية والبيانات الشخصية الحساسة"[1].

أيضًا يُلزم القانون الجهات التي تجمع أو تعالج البيانات الشخصية بالعديد من الواجبات لضمان حماية حقوق الأفراد، و تتضمن هذه الواجبات الالتزام بالشفافية من خلال إعلام الأفراد بأهداف جمع البيانات، وكيفية استخدامها والتقيد بمبدأ الحد الأدنى من البيانات من خلال جمع البيانات الضرورية فقط؛ لتحقيق الأهداف

[1] المادة رقم 2 من قانون حماية البيانات الشخصية الأردني رقم (24) / 2023

المحددة وضمان أمان البيانات من خلال اتخاذ إجراءات فنية وإدارية لحمايتها من الوصول غير المصرح به أو التسريب، ولضمان تطبيق هذه الواجبات أنشأ القانون هيئة وطنية لحماية البيانات الشخصية تتولى مسؤولية مراقبة تطبيق القانون، وفرض العقوبات على المخالفين، وتشمل هذه العقوبات غرامات مالية وإجراءات إدارية أخرى.[1] وما ورد بقانون حماية البيانات الأردني ما هو إلا تكريس لما جاء بالمادة السابعة من دستور المملكة الأردنية، والتي ورد بها أن الحرية الشخصية مصونة، وكل اعتداء على الحقوق والحريات العامة أو حرمة الحياة الخاصة للأردنيين جريمة يعاقب عليها القانون[2].

يهدف قانون حماية البيانات الشخصية إلى إرساء إطار قانوني متوازن يحقق التوفيق بين ضمان حقوق الأفراد في حماية بياناتهم الشخصية وخصوصيتهم، التي يكفلها الدستور والقوانين ذات الصلة وبين السماح بمعالجة البيانات والمعلومات والاحتفاظ بها في ظل التطور المتسارع للفضاء الإلكتروني وانتشار مفاهيم الاقتصاد الرقمي. ويسعى القانون إلى تشجيع التجارة والخدمات الإلكترونية في المملكة الأردنية الهاشمية من خلال بناء بيئة آمنة للفضاء السيبراني وتحديد الالتزامات والواجبات المفروضة على المسؤولين عن البيانات الشخصية ومعالجتها.

بناءً على ما تقدم نصت الفقرة (ب) من المادة الرابعة من قانون حماية البيانات الشخصية الأردني رقم 24 لسنة 2023 على تحديد حقوق الشخص المعني ببياناته الشخصية.

---

[1] صدور قانون حماية البيانات الشخصية في الجريدة الرسمية، https://petra.gov.jo/Include/InnerPage.jsp?ID=256806&lang=ar&name=news تاريخ الزيارة 24 فبراير 2025.

[2] المادة 7 من دستور المملكة الاردنية وفقا لآخر تعديلاته عام 2022.

وقبل الخوض في تفصيل هذه الحقوق يجدر بنا تعريف "الشخص المعني" كما ورد في الفقرة المذكورة وهو الشخص الطبيعي الذي تُعالج بياناته الشخصية ويتمتع بحق حماية هذه البيانات؛ وبالتالي لا يجوز معالجة هذه البيانات إلا بموافقته المسبقة أو في الحالات التي يجيزها القانون [1].

الحالات التي يشترط فيها القانون موافقة صاحب البيانات:

1. حق الوصول إلى البيانات الشخصية:

بموجب المادة الرابعة من قانون حماية البيانات الشخصية يتمتع الشخص المعني بحق الوصول إلى بياناته الشخصية.

يتضمن هذا الحق إمكانية الاطلاع على البيانات الموجودة لدى المسؤول والحصول على نسخة منها، والمسؤول قد يكون شخصًا طبيعيًا أو اعتباريًا داخل المملكة أو خارجها، والبيانات المعنية هي أي معلومات تتعلق بالشخص الطبيعي، سواء كانت تعريفًا مباشرًا أو غير مباشر، بغض النظر عن مصدرها أو شكلها، وتشمل البيانات المتعلقة بالشخصية والوضع العائلي وأماكن التواجد.

[1] المادة رقم 4/ ب من قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023

2. حق سحب الموافقة:

يمنح القانون الشخص المعني الحق في سحب موافقته المسبقة على معالجة بياناته الشخصية، ويترتب على سحب الموافقة محو البيانات أو إخفائها، واتخاذ التدابير اللازمة لذلك من قبل المسؤول، بناءً على طلب الشخص المعني أو الوحدة التنظيمية المختصة بحماية البيانات الشخصية (وزارة الاقتصاد الرقمي والريادة) [1].

3. حق تصحيح البيانات:

يحق للشخص المعني تصحيح، تعديل، إضافة، أو تحديث بياناته الشخصية، ويمكن للأفراد طلب تصحيح بياناتهم في حال عدم دقتها أو طلب استكمالها في حال نقصها، بالإضافة إلى ذلك يحق للشخص المعني تقييد معالجة بياناته الشخصية، وذلك بتخصيص المعالجة في نطاق محدد.

ويرى الباحث أنه وفقًا للمادة الثانية من قانون حماية البيانات الشخصية، تُعرّف المعالجة بأنها أي عملية أو مجموعة عمليات تُجرى على البيانات الشخصية، سواء كانت آلية أو غير آلية، وتشمل على سبيل المثال لا الحصر: الجمع، التسجيل، النسخ، الحفظ، التخزين، التنظيم، التنقيح، الاستغلال، الاستعمال، الإرسال، التوزيع، النشر، الربط، الإتاحة، النقل، العرض، الإخفاء، الإتلاف، الترقية، المحو، التعديل، التوصيف والإفصاح.

---

[1] أبو الليل، إبراهيم الدسوقي، التعاقد عبر الوسائل الاتصال الحديثة، الطبعة الثالثة، الملجلد الثالث، بحث منشور ضمن أعمال مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المنعقد في الفترة من 1-3 مايو 2000، ص1014.

4. التزامات المسؤول وحق الاعتراض:

يلزم القانون المسؤول بتمكين الشخص المعني من ممارسة حقوقه بما في ذلك الاعتراض على المعالجة، وسحب الموافقة والوصول إلى البيانات وتحديثها، وتوفير الوسائل الآمنة لذلك كما يحق للشخص المعني الاعتراض على معالجة بياناته الشخصية والاعتراض على التشخيص الآلي الذي يستند إلى هذه البيانات وغالبًا ما يحدث الاعتراض إذا كانت المعالجة أو التشخيص غير ضروريين لتحقيق الأغراض المشروعة أو إذا كانت المعالجة تمييزية أو مجحفة أو مخالفة للقانون [1].

5. حق نقل البيانات:

يحق للشخص المعني نقل نسخ من بياناته الشخصية من مسؤول إلى آخر، بشرط أن يحقق النقل مصالح مشروعة لكل من المسؤول والمسؤول المتلقي، وأن يكون الشخص المعني على علم كافٍ بالمسؤول المتلقي والأغراض التي ستُستخدم البيانات من أجلها.

لا يجوز أن يكون الغرض من النقل تسويق منتجات أو خدمات دون موافقة الشخص المعني، ويُعرّف المسؤول المتلقي بأنه أي شخص طبيعي أو اعتباري، داخل المملكة أو خارجها، تُنقل إليه البيانات أو تُتبادل معه من قبل المسؤول، كما يحق للشخص المعني العلم بأي خرق أو انتهاك لسلامة بياناته، بما في ذلك الوصول غير المصرح به أو النقل غير القانوني.

---

[1] وليد رمضان عبد الرازق محمود، ضوابط جمع ومعالجة البيانات الشخصية في ظل الإدارة الإلكترونية، كلية الحقوق جامعة بنى سويف، مصر، 2011، ص 4

6. حقوق إضافية وشروط الموافقة:

لا تترتب أي تبعات مالية أو تعاقدية على ممارسة الشخص المعني لحقوقه المنصوص عليها في الفقرة (ب) من المادة الرابعة من قانون حماية البيانات الشخصية الأردني، بشرط ألا يخل ذلك بحقوق المسؤول. يشترط في الموافقة المسبقة من الشخص المعني أن تكون صريحة وموثقة كتابيًا أو إلكترونيًا، وأن تكون محددة من حيث المدة والغرض، وأن يُقدّم الطلب بلغة واضحة وبسيطة وغير مضللة، وأن يكون الوصول إليه سهلًا [1].

المطلب الثاني: وسائل الحماية القانونية للبيانات الشخصية

بعد التعرف على الحق في البيانات الشخصية من حيث نطاقه وطبيعته القانونية وكيفية تنظيمه في القوانين الوطنية، ننتقل في هذا المطلب إلى استعراض وسائل حماية هذا الحق، نبدأ بالإجراءات الوقائية التي تهدف إلى منع الاعتداء على هذا الحق قبل وقوعه، مثل وضع ضوابط صارمة لجمع البيانات ومعالجتها، وضمان شفافية الجهات التي تتعامل مع البيانات، وتوفير آليات تمكن الأفراد من مراقبة بياناتهم الشخصية وإدارتها، ثم ننتقل إلى قواعد المسؤولية عن الاعتداء على هذا الحق، والتي تشمل العقوبات المالية والإدارية

[1] جمال موراي، حق الأفراد في حماية بياناتهم الشخصية وفقاً لقانون حماية البيانات الشخصية، موسوعة حماة الحق، الأردن 19 ديسمبر، 2023. https://jordan-lawyer.com/2023/12/19/%D8%AD%D9%82-%D8%A7%D9%84%D8%A3%D9%81%D8%B1%D8%A7%D8%AF-%D9%81%D9%8A-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA%D9%87%D9%85-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-%D9%88/

تاريخ الزيارة 23فبراير 2025

على الجهات التي تنتهك خصوصية الأفراد، بالإضافة إلى تعويض المتضررين عن الأضرار المادية أو المعنوية التي قد تنتج عن سوء استخدام بياناتهم الشخصية.

الفرع الأول- التدابير الوقائية لحماية البيانات الشخصية:

تتمثل الإجراءات الوقائية في الوسائل التي تهدف إلى منع المساس بالبيانات الشخصية، وهي إجراءات استباقية تسبق وقوع أي اعتداء، مما يميزها عن الوسائل القانونية التي يتم اللجوء إليها بعد وقوع الضرر، مثل التعويض المدني والعقوبات الجزائية.

وتساهم هذه الإجراءات في ردع الأفراد وحماية البيانات الشخصية من أي انتهاك، وهي متاحة لصاحب الحق حتى في غياب الضرر الفعلي، كما تتضمن هذه الإجراءات منع الوصول إلى البيانات أو نشرها، وفي حال نشرها، يحق لصاحب البيانات وقف هذا النشر.

من وجهة نظر الباحث أن صاحب البيانات في تعديل وتصحيح البيانات يمثل إجراءً وقائيًا هامًا، حيث يساهم في منع استخدام هذه البيانات بشكل خاطئ أو مسيء لصاحبها من خلال تمكين الأفراد من تحديث بياناتهم وضمان دقتها يتم تقليل المخاطر المحتملة التي قد تنجم عن الاعتماد على معلومات غير صحيحة أو قديمة، ولقد عالج القانون المدني الأردني هذه المسألة في المادة (48) حيث نص على أنه "لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر" وبالمثل ينص القانون المؤقت للمطبوعات والنشر الأردني رقم 5 لسنة 2010 في المادة (1) منه على وجوب ممارسة الصحافة لمهمتها بحرية مع احترام حدود القانون والحفاظ على الحريات

والحقوق وحرمة الحياة الخاصة للآخرين وهذا النهج يتوافق مع ما تضمنته معظم التشريعات الوطنية في الحفاظ على الحقوق الملازمة للشخصية بشكل عام والحياة الخاصة بشكل خاص [1].

بالإضافة إلى الحقوق القانونية في مقاضاة المعتدين على البيانات الشخصية؛ توفر التقنيات الحديثة مجموعة من الوسائل التي يمكن للأفراد استخدامها لحماية بياناتهم، كما سيتم استعراض هذه الوسائل:

أولاً- الوسائل التقنية:

تساهم الوسائل التقنية في تعزيز أمان الملفات والمواقع الإلكترونية الشخصية، وذلك باستخدام أحدث التقنيات المتاحة ومن بين هذه الوسائل:

1- كلمة المرور

كلمات المرور هي عبارة عن رموز وأرقام وحروف تمنع الوصول غير المصرح به إلى المواقع والملفات الشخصية. تتيح كلمات المرور لأصحاب البيانات التحكم في الوصول إلى معلوماتهم، حيث لا يمكن لأحد الاطلاع على محتويات الملفات دون معرفة كلمة المرور الصحيحة [2].

---

[1] كما يتضح في القانون المدني الفرنسي في المادة (1) منه، التي تنص على أنه "للقضاة أن يتخذوا جميع الوسائل مثل الحراسة والحجز وغيرها من الإجراءات لمنع أو لوقف أي مساس بالحياة الخاصة".

[2] كنده الشماط، الحق في الحياة الخاصة، رسالة لنيل درجة الدكتوراه في الحقوق، جامعة دمشق، سوريا،2004-2005، ص 567.

2- التشفير

التشفير هو عملية تحويل المعلومات إلى رموز غير قابلة للقراءة، ولا يمكن فهم محتوى هذه المعلومات إلا باستخدام مفتاح التشفير المناسب لفك الرموز وإعادة المعلومات إلى حالتها الأصلية. يستخدم التشفير لحماية المعلومات من الوصول غير المصرح به والتلاعب بها [1].

3- حماية البيانات من الفيروسات

تُعد البرامج المضادة للفيروسات أدوات حيوية لحماية البيانات الشخصية، حيث تواجه تهديدًا مستمرًا من الفيروسات وهي برامج خبيثة مصممة من قبل متخصصين لإلحاق الضرر بالبرامج الأخرى، كما تعمل الفيروسات على ربط نفسها بالبرامج وتنتشر بسرعة لإصابة أكبر عدد ممكن من أجهزة الحاسوب، مما قد يؤدي إلى تدمير البرامج وتعطيلها ولمواجهة هذا التهديد توجد أنظمة حماية مضادة للفيروسات تعمل على تقليل فرص الإصابة وانتشار الفيروسات.

تتطلب هذه الأنظمة تفعيلًا وتحديثًا مستمرين لضمان قدرتها على مكافحة أحدث أنواع الفيروسات وحماية البرامج من التلف [2].

4- التوقيع الإلكتروني "هوية رقمية معترف بها"

يُعتبر التوقيع بشكل عام عنصرًا أساسيًا في إثبات صحة الوثائق خاصةً في المعاملات الرقمية؛ حيث يُعرف التوقيع بأنه علامة مميزة يضعها الشخص على مستند لتأكيد هويته وموافقته على محتواه،

---

[1] كنده الشماط، المرجع السابق، ص568.

[2] محمد فهمي طلبه وآخرون، فيروسات الحاسب وأمن البيانات، المكتب المصري الحديث، القاهرة، مصر، ص 31.

وبالمثل يعمل التوقيع الإلكتروني على الوسائل الرقمية بنفس الطريقة التي يعمل بها التوقيع التقليدي على الوسائل الورقية؛ حيث يتيح للأفراد توقيع المستندات الإلكترونية لإثبات موافقتهم عليها وتأكيد هويتهم الرقمية [1].

يرى الباحث بناء على ما سبق إيضاحه أن التوقيع الإلكتروني يتجاوز دوره التقليدي في إثبات صحة الوثائق ليصبح عنصرًا أساسيًا في حماية البيانات الشخصية؛ فبالإضافة إلى استخدامه لتأكيد الموافقة على محتوى المستندات، يمكن استخدام التوقيع الإلكتروني كوسيلة للتحقق من هوية المستخدم عند الوصول إلى البرامج والبيانات الخاصة من خلال إلزام المستخدمين بإدخال توقيعهم الإلكتروني لفتح البرامج، والوصول إلى بياناتهم يتم تقييد الوصول إلى المعلومات الحساسة وحمايتها من الوصول غير المصرح به، وبذلك يصبح التوقيع الإلكتروني بمثابة مفتاح رقمي يضمن أن المستخدم المصرح له فقط هو من يمكنه الوصول إلى بياناته[2].

ثانيًا– الوسائل الفنية: بالإضافة إلى الوسائل التقنية توجد إجراءات عملية يمكن اتخاذها للوقاية من الاعتداء على البيانات الشخصية ومنها:

---

[1] عبد الفتاح بيومي حجازي، التوقيع الألكتروني في النظام القانوني المقارن، دار الفكر الجامعي، الإسكندرية، مصر، ص 14.

[2] سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية "دراسة في القانون الفرنسي" (القسم الثاني)، مجلة الحقوق الكويت، العدد الرابع، السنة الخامسة والثلاثون، ديسمبر ٢٠١١م، ص 396.

1- الابتعاد عن إدراج المعلومات الحساسة دون ضرورة

يجب تجنب تقديم معلومات حساسة غير ضرورية للمواقع الإلكترونية حيث يميل البعض إلى مشاركة جميع البيانات المطلوبة دون التحقق من مصداقية الموقع أو الحاجة الفعلية لتلك البيانات، على سبيل المثال إذا طلب موقع تواصل اجتماعي معلومات صحية أو بنكية يجب الامتناع عن تقديمها وفي حال الضرورة يمكن تقديم بيانات وهمية كحل بديل.

2- التعامل مع من يعرفه

يُنصح المستخدمون بالتعامل مع المواقع الإلكترونية المعروفة والموثوقة أو تلك التي يمكن التحقق من مصداقيتها لتجنب الوقوع في أخطاء تقديم بيانات أو التزامات غير مرغوب فيها [1].

3- تغير كلمة السر باستمرار

يُعد تغيير كلمات المرور بشكل دوري إجراءً وقائيًا فعالًا ضد محاولات الاختراق، حيث يجب تغيير كلمات مرور الحسابات والأجهزة بانتظام، بالإضافة إلى تغيير عنوان IP الخاص بالجهاز الذي يُعد بمثابة هوية رقمية يمكن استغلالها للوصول إلى البيانات الشخصية المخزنة.

[1] سامح عبد الواحد التهامي، المرجع السابق، ص 397.

الفرع الثاني- المسؤولية القانونية عن انتهاكات البيانات الشخصية:

بعد استعراض الإطار القانوني للحق في البيانات الشخصية وآليات الحماية التي توفرها التشريعات، بالإضافة إلى الوسائل الوقائية التي تهدف إلى منع وقوع الضرر ننتقل إلى موضوع بالغ الأهمية وهو المسؤولية القانونية المترتبة على الاعتداء؛ وهذا الاعتداء قد ينشأ من مزودي الخدمات الذين يعالجون البيانات أو قد يصدر من أطراف ثالثة غير مصرح لها بالوصول إلى تلك البيانات أو استخدامها.

و مع التطور المتسارع للتكنولوجيا توسعت دائرة الأفعال الضارة وتنوعت أشكالها لتشمل على سبيل المثال لا الحصر: إفشاء البيانات، و تدميرها، وتضليلها و استخدامها لأغراض غير مصرح بها، و استغلالها ماديًا، وغيرها من الأفعال التي تندرج تحت مسمى الفعل الضار، و تتسبب هذه الأفعال في إلحاق أضرار جسيمة بأصحاب البيانات وتتضاعف هذه الأضرار نظرًا لسرعة انتشارها عبر الوسائل التكنولوجية مقارنة بالوسائل التقليدية، وفي هذا السياق يبرز تساؤل مهم حول مسؤولية الأطراف المتورطة في الاعتداء على البيانات الشخصية، تحديدًا: مسؤولية الشخص الذي قام باختراق الجهاز وتسريب البيانات و مسؤولية الشخص الذي تسلم البيانات المسربة.

و يتضح من خلال تحليل الإطار القانوني للمعاملات الإلكترونية في كل من سلطنة عمان والمملكة الأردنية الهاشمية؛ أن المسألة القانونية تتشعب لتشمل تحديد المسؤوليات بوضوح وكيفية تطبيق القوانين في هذا المجال المتطور وتبرز أهمية ذلك بشكل خاص في مجال حماية البيانات الشخصية، حيث تتطلب الطبيعة المتغيرة للمعاملات الإلكترونية وضع آليات قانونية فعالة لمواجهة التحديات المتعلقة بانتهاكات البيانات؛ لذلك

سنوضح موقف كل من المشرع العُماني والمشرع الأردني من المسؤولية القانونية عن انتهاكات البيانات الشخصية مع تسليط الضوء على أبرز التشريعات والممارسات القانونية في هذا الشأن.

أولًا- المسؤلية القانونية عن انتهاكات البيانات الشخصية في ضوء التشريع العُماني:

في ظل التطور التكنولوجي السريع وزيادة الاعتماد على المعالجة الرقمية للبيانات أصبحت حماية البيانات الشخصية أولوية تشريعية، في سلطنة عُمان يُنظّم المرسوم السلطاني رقم 39 / 2025 بإصدار قانون المعاملات الإلكترونية، قانون حماية البيانات الشخصية ولائحته التنفيذية حماية هذه البيانات ويحدد المسؤولية القانونية عن انتهاكاتها.

1- نطاق الحماية والانتهاكات:

يحمي القانون البيانات الشخصية التي تُعرّف بأنها: "البيانات التي تجعل شخصًا طبيعيًا معرّفًا أو قابلًا للتعريف مباشرة أو غير مباشرة مثل الاسم أو الرقم المدني أو البيانات الصحية أو الجينية"[1].

ومن أبرز حالات الانتهاك:

أ) حظر جمع أو استخدام أو تخزين أو مشاركة البيانات الشخصية التي تتعلق بالبيانات الجينية أو الحيوية أو الصحية أو الأصول العرقية أو الحياة الجنسية أو الآراء السياسية أو الدينية أو الإدانات الجنائية أو التدابير الأمنية[2]، إلا بعد الحصول على تصريح رسمي من الوزارة، وذلك وفقًا للضوابط

---

[1] المادة رقم (1) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (5) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

والإجراءات التي تحددها اللائحة التنفيذية، كما تُلزم المادة (27) من الفصل السادس مقدم خدمات الثقة بالمحافظة على سرية المعلومات التي حصل عليها ما لم يسمح صاحب العلاقة كتابة أو إلكترونياً بنشرها وهو ما يمثل الأساس المدني للمسؤولية عن الإخلال بواجب السرية[1].

وتعتبر هذه المواد بالغة الأهمية لحماية خصوصية الأفراد وبياناتهم الحساسة، حيث تفرض قيودًا صارمة على معالجة هذه البيانات وتتطلب الحصول على تصريح رسمي من الوزارة لضمان حماية هذه البيانات من الاستخدام غير القانوني أو غير الأخلاقي.

ب) "لا يجوز جمع أو استخدام أو تخزين أو مشاركة البيانات الشخصية إلا وفقًا للشروط التالية: أن يتم ذلك بشفافية وأمانة، مع احترام كامل لكرامة الإنسان وأن يحصل المتحكم على موافقة صريحة وواضحة من صاحب البيانات الشخصية قبل البدء في أي عملية معالجة وأن يكون طلب الموافقة على معالجة البيانات الشخصية مكتوبًا بلغة واضحة ومفهومة ويجب على المتحكم الاحتفاظ بإثبات كتابي لموافقة صاحب البيانات الشخصية على معالجة بياناته" [(2)]،وتعتبر هذه المادة حجر الزاوية في قانون حماية البيانات الشخصية، حيث تضع القواعد الأساسية التي تحكم معالجة البيانات الشخصية، وتضمن حماية حقوق الأفراد في بياناتهم.

ج) تنص المادة (19) على أنه إذا تعرضت البيانات الشخصية لاختراق يؤدي إلى تدميرها أو تغييرها أو الكشف عنها أو الوصول إليها أو استخدامها بشكل غير قانوني؛ يجب على المتحكم إبلاغ كل من الوزارة وصاحب البيانات الشخصية بهذا الاختراق، وذلك وفقًا للضوابط والإجراءات التي تحددها اللائحة

[(1)] المادة رقم (27) مرسوم سلطاني رقم 39 / 2025 بإصدار قانون المعاملات الإلكترونية.

[(2)] المادة رقم (10) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

التنفيذية وتعتبر هذه المادة ضرورية لضمان الشفافية والمساءلة في حالة حدوث اختراقات للبيانات الشخصية، وتمكين كل من الوزارة وصاحب البيانات الشخصية من اتخاذ الإجراءات اللازمة لحماية البيانات وتقليل الأضرار المحتملة [1].

د) تنص المادة (23) على أنه مع مراعاة اختصاصات مركز الدفاع الإلكتروني؛ يجوز للمتحكم نقل البيانات الشخصية أو السماح بتحويلها إلى خارج سلطنة عمان، وذلك وفقًا للضوابط والإجراءات التي تحددها اللائحة التنفيذية ومع ذلك يحظر نقل البيانات الشخصية إذا كانت معالجتها مخالفة لأحكام هذا القانون أو إذا كان من شأن هذا النقل أن يلحق ضررًا بصاحب البيانات الشخصية وتعتبر هذه المادة ضرورية لتنظيم نقل وتحويل البيانات الشخصية خارج سلطنة عمان وضمان حماية هذه البيانات من الاستخدام غير القانوني أو غير الأخلاقي كما أنها تهدف إلى تحقيق التوازن بين حرية تدفق البيانات وحماية خصوصية الأفراد[2].

2- أنواع المسؤولية القانونية:

أ. **المسؤولية الجزائية:** يُعاقب على انتهاكات البيانات بغرامات مالية وفقًا لخطورة المخالفة:

- **المخالفات البسيطة:** مثل عدم إخطار صاحب البيانات بالغرض من المعالجة تنص المادة (25) على أنه يُعاقب كل من يخالف أحكام المادة (14) من القانون بغرامة مالية تتراوح بين 500 ريال عماني كحد أدنى و2000 ريال عماني كحد أقصى. [3]

---

[1] المادة قم (19) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (23) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[3] المادة رقم (25) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

- **المخالفات المتوسطة** :مثل عدم تعيين مدقق خارجي أو عدم احتفاظ المتحكم بالسجلات تنص المادة (26) على أنه يُعاقب كل من يخالف أحكام المواد (15) و(16) و(17) و(18) و(20) و(22) من القانون بغرامة مالية تتراوح بين 1000 ريال عماني كحد أدنى و5000 ريال عماني كحد أقصى [1].
- **المخالفات الجسيمة** :مثل معالجة البيانات الحساسة دون تصريح أو اختراق البيانات تنص المادة (28) على أنه يُعاقب كل من يخالف أحكام المواد (5) و(6) و(19) و(21) من القانون بغرامة مالية تتراوح بين 15000 ريال عماني كحد أدنى و20000 ريال عماني كحد أقصى [2].

المخالفات الخطيرة :مثل نقل البيانات خارج عُمان بالمخالفة للقانون تنص المادة (29) على أنه يُعاقب كل من يخالف أحكام المادة (23) من القانون بغرامة مالية تتراوح بين 100000 ريال عماني كحد أدنى و500000 ريال عماني كحد أقصى.

كما تنص المادة (30) من قانون حماية البيانات الشخصية في سلطنة عمان على أنه مع عدم الإخلال بالمسؤولية الجزائية للأشخاص الطبيعيين، يُعاقب الشخص الاعتباري بغرامة مالية تتراوح بين 5000 ريال عماني كحد أدنى و100000 ريال عماني كحد أقصى، إذا ارتكبت الجريمة باسمه أو لحسابه من قبل رئيس أو أحد أعضاء مجلس إدارته أو مديره أو أي مسؤول آخر، بموافقته أو بتستر أو إهمال جسيم منه، ولقد أكد المشرع العُماني في المادة (31) من قانون حماية البيانات الشخصية على أنه يجوز للمحكمة المختصة

---

[1] المادة رقم (26) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (28) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

بالإضافة إلى الغرامة المالية أن تحكم بمصادرة الأدوات التي استُخدمت في ارتكاب الجريمة، وذلك في إطار تطبيق أحكام هذا القانون.

أيضًا المادة (33) من الفصل السابع (العقوبات) من قانون المعاملات الالكترونية المسؤولية الجزائية حيث تعاقب بالسجن والغرامة كل من استغل المعلومات التي جُمعت عن طالب شهادة التصديق الإلكتروني لأغراض أخرى دون موافقته وكذلك كل من أفشى المعلومات أو البيانات المتعلقة بشهادة التصديق الإلكتروني دون موافقة صاحبها الكتابية[1]، هذه المادة تجرّم وتضع عقوبات مباشرة على انتهاكات البيانات الشخصية وإساءة استخدامها.

من وجهة نظر الباحث بناء على ما سبق إيضاحه يتميز التشريع العماني لحماية البيانات الشخصية بتدرج واضح في العقوبات المالية حسب خطورة الانتهاك حيث يفرض غرامات تتراوح بين 500 ريال للمخالفات البسيطة كعدم إخطار أصحاب البيانات وصولاً إلى 500 ألف ريال لمخالفات نقل البيانات خارج البلاد مع مساءلة الأشخاص الاعتباريين بغرامات تصل إلى 100 ألف ريال حال ارتكاب المخالفة بموافقة أو إهمال جسيم من إدارتهم، كما يجوز للمحكمة مصادرة الأدوات المستخدمة في الانتهاك، وبالرغم من هذه العقوبات إلا أن التشريع الحالي يعاني بعض القصور كغموض تعريف "الإهمال الجسيم" واقتصار العقوبات على الجانب المالي دون عقوبات رادعة أخرى كتعليق التراخيص أو الحبس مما يستدعي تطوير التشريع لتحديد المفاهيم الغامضة وإدراج عقوبات تكميلية وإنشاء دوائر قضائية متخصصة لتعزيز فعاليته في مواكبة التحديات الرقمية المتسارعة.

---

(1) المادة رقم (33) مرسوم سلطاني رقم 39 / 2025 بإصدار قانون المعاملات الإلكترونية.

ب- **المسؤولية الإدارية:**

تنص المادة (44) من اللائحة التنفيذية لقانون حماية البيانات الشخصية على أنه يجوز للوزير توقيع أحد الجزاءات الإدارية التالية في حالة مخالفة أحكام هذه اللائحة: الإنذار وقف التصريح لحين إزالة المخالفة وغرامة إدارية لا تزيد على ألفي ريال عماني لكل مخالفة وإلغاء التصريح [1].

ج- **المسؤولية المدنية:**

يحق لصاحب البيانات المضرور المطالبة بالتعويض عبر المحكمة المختصة عن الأضرار المادية أو المعنوية الناتجة عن الانتهاك استنادًا إلى أحكام المسؤولية التقصيرية في القانون المدني العُماني حيث تنص المادة (3) من اللائحة التنفيذية لقانون حماية البيانات الشخصية بوضوح على أن "المعالج يكون في علاقته بالغير نائباً عن المتحكم في نطاق تطبيق أحكام المسؤولية المدنية"[2]، مما يؤسس للإطار القانوني للمساءلة المدنية في حالات انتهاك البيانات كما تكمل المادة (41) هذا النص بمنح صاحب البيانات آلية عملية لممارسة هذا الحق عبر تقديم شكوى عن أي مخالفة[3]، وبذلك تُشكل المادة (3) الأساس التشريعي الذي يقرر المسؤولية المدنية عن انتهاكات البيانات الشخصية دون إخلال بالمسؤوليات الجزائية أو الإدارية المنصوص عليها.

---

[1] المادة رقم (44) من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

[2] المادة رقم (3) من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

[3] المادة رقم (41) من قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية من وزارة النقل والاتصالات وتقنية المعلومات.

ثانيًا: المسؤلية القانونية عن انتهاكات البيانات الشخصية في ضوء التشريع الأردُني:

لكن المشرع الأردني ترك تنظيم المسؤولية المدنية الناتجة عن إفشاء سرية البيانات الشخصية للقواعد العامة ولقد نص على عقوبة هذا الفعل في المادة (37) من قانون المعاملات الإلكترونية؛ لذلك سيتم بحث قواعد المسؤولية العقدية لمستلم البيانات ثم التعرض لقواعد المسؤولية التقصيرية.

1- المسؤولية العقدية لمستلم البيانات:

في إطار لمسؤولية العقدية ينص المشرع الأردني على أن المسؤولية تنتج عن الإخلال بالالتزامات العقدية المتفق عليها بين الأطراف، مما يترتب عليه ضرر للطرف الآخر وفي حالة العقد المبرم بين شركة الإنترنت (مستلم البيانات) والعميل (صاحب البيانات) فإن العقد يُعتبر "شريعة المتعاقدين" أي أن الشروط الواردة فيه تلعب دورًا رئيسيًا في تحديد طبيعة الالتزامات والمسؤوليات.

- **شروط الإعفاء من المسؤولية:**

إذا تضمن العقد شرطًا يعفي الشركة من المسؤولية عن حماية البيانات الشخصية أو يحد من التعويض في حالة الإخلال فإن هذا الشرط يُعتبر ملزمًا ما لم يكن مخالفًا للنظام العام أو للالتزامات الجوهرية في العقد ومع ذلك نظرًا للأهمية الكبيرة التي توليها التشريعات الدولية والوطنية لحماية البيانات الشخصية وضرورة الحفاظ على سريتها فإن التزام الشركة بحماية البيانات يُعتبر التزامًا جوهريًا ورئيسيًا في العقد؛ وبالتالي فإن أي شرط يعفي الشركة من المسؤولية عن إفشاء البيانات الشخصية يُعتبر باطلًا لكونه مخالفًا للالتزام الجوهري.

- **تخفيف المسؤولية أو التعويض**

إذا كان العقد يتضمن شرطًا يخفف من مسؤولية الشركة أو يحد من قيمة التعويض دون أن يعفيها تمامًا من الالتزام بحماية البيانات فإن هذا الشرط يُعتبر صحيحًا ما دام لا يلغي الالتزام الأساسي بالحماية

بمعنى آخر يمكن للشركة أن تدرج شروطًا تحد من مسؤوليتها أو تخفف من التعويض طالما أن هذه الشروط لا تتعارض مع الالتزام الرئيسي بحماية البيانات.

- **الإخلال بالالتزام العقدي**

في حالة عدم وجود شروط تعفي الشركة من المسؤولية أو تخفف منها فإن المسؤولية العقدية تنتج عن الإخلال بالالتزامات الواردة في العقد ولقيام المسؤولية يجب توافر الشروط التالية:

الإخلال بالالتزام: أي تقصير من جانب الشركة في تنفيذ التزاماتها العقدية مثل الإفشاء غير المصرح به للبيانات الشخصية، الضرر: أن يترتب على هذا الإخلال ضرر للعميل، سواء كان ماديًا أو معنويًا، علاقة السببية بينهما أن يكون الإخلال هو السبب المباشر في حدوث الضرر [1].

- طبيعة الالتزام" تحقيق نتيجة أم بذل عناية؟"

يعتمد تحديد طبيعة الالتزام (تحقيق نتيجة أم بذل عناية) على نصوص العقد المبرم بين الشركة والعميل: إذا تضمن العقد شرطًا يلزم الشركة "بتحقيق نتيجة" معينة (مثل ضمان سرية البيانات بشكل مطلق) فإن الشركة تكون مسؤولة عن أي إخلال بهذا الالتزام حتى لو بذلت العناية اللازمة أما إذا لم يتضمن العقد مثل هذا الشرط، فإن الالتزام يُعتبر "ببذل عناية" وعندها تقاس العناية المطلوبة وفقًا لمعيار الشخص المعتاد أي أن الشركة تكون مسؤولة فقط إذا ثبت أنها لم تبذل العناية الكافية لحماية البيانات [2].

---

[1] لينا ابراهيم يوسف حسان، التوثيق الألكتروني ومسؤولية الجهات المختصة به " دراسة مقارنة "، الطبعة الأولى، دار الراية للنشر والتوزيع، الجيزة، مصر، 2009، ص 159.

[2] عدنان السرحان، نوري خاطر، شرح القانون المدني" مصادر الحقوق الشخصية " دار الثقافة، عمان، الأردن، 2005، ص 238.

من وجهة نظر الباحث يُظهر المشرع الأردني موقفًا متوازنًا في تنظيم المسؤولية العقدية لمستلم البيانات حيث يعترف بحرية الأطراف في تحديد شروط العقد ("شريعة المتعاقدين") مع وضع ضوابط تحمي الالتزامات الجوهرية مثل حماية البيانات الشخصية كما يُلزم الشركة بالمسؤولية في حالة الإخلال بالالتزامات العقدية مع مراعاة طبيعة الالتزام (تحقيق نتيجة أم بذل عناية) وفقًا لنصوص العقد.

2- المسؤولية العقدية لمستلم البيانات:

وفقًا للقواعد العامة للمسؤولية التقصيرية يلتزم كل من ارتكب فعلاً ضارًا تسبب في إصابة الغير بضرر بتعويض المضرور، وتنشأ هذه المسؤولية عند عدم وجود عقد وتكون بمخالفة القواعد العامة التي تنص على عدم إحداث أي ضرر للغير، كما جاء في نص المادة (256) من القانون المدني الأردني "كل إضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر" وتتطلب المسؤولية التقصيرية، شأنها شأن المسؤولية العقدية، توافر ثلاثة أركان لقيامها، وهي الفعل الضار، والضرر، وعلاقة السببية بينهما"[1].

- **الفعل الضار**

يُعرّف الفعل الضار بأنه الانحراف عن السلوك المألوف للشخص المعتاد أي الفعل الذي يرتكبه الشخص عن خطأ ويؤدي إلى وقوع ضرر بالغير وقد أسس المشرع الأردني المسؤولية على مبدأ الإضرار كما هو منصوص عليه في المادة (256) من القانون المدني الأردني [2].

---

[1] المادة رقم 256 القانون المدني الأردني لسنة 1976 وتعديلاته حتى سنة 2025.

[2] سامح التهامي، مرجع سابق، ص 434.

- **الضرر**

يُعرَّف الضرر بأنه "الأذى الذي يصيب الشخص نتيجة المساس بحق من حقوقه أو بمصلحة مشروعة له" ويُعد الضرر الركن الثاني من أركان المسؤولية ولا تقوم المسؤولية إلا باكتمال أركانها الثلاثة، ويجب أن يكون الضرر نتيجة مباشرة للفعل الضار حتى تقوم المسؤولية وقد يكون الضرر ماديًا أو معنويًا وقد أقر المشرع الأردني التعويض عن الضرر المعنوي في المادة (1/267) من القانون المدني حيث نص على وجوب ضمان الضرر الأدبي [1]. ويُقصد بالضرر الأدبي في التعدي على الغير في حريته أو عرضه أو شرفه أو سمعته أو مركزه الاجتماعي أو اعتباره المالي وفي حالة التعاقد مع شركة اتصالات أو إنترنت و يقدم الشخص بيانات قبل إبرام العقد ويجب أن تكون هذه البيانات محمية بضمانات تمنع المساس بها وإذا تم الاعتداء على هذه البيانات تقوم المسؤولية التقصيرية، وهو ما يكفله القانون للشخص الملزم بتقديم بياناته وقد يتم المساس بالبيانات من قِبَل شخص آخر أو قراصنة الإنترنت عن طريق اختراق أجهزة الشركة وفي هذه الحالة يمكن مساءلة الشركة على أساس نظرية تحمل المخاطر أو مدى الالتزام الذي تتحمله الشركة وإذا كان الالتزام ببذل عناية، يجب التأكد من أن الشركة لم تقصر في الضمانات التي يستلزمها الشخص المعتاد[2].

---

[1] المادة رقم 1/267 القانون المدني الأردني لسنة 1976 وتعديلاته حتى سنة 2025.

[2] عبد الرزاق السنهوري، الوجيز في شرح القانون المدني الجزء الأول" نظرية الالتزام بوجة عام"، الطبعة الثانية، دار النهضة العربية، القاهرة، 1997، ص 327

- **علاقة السببية**

تُعرف علاقة السببية بأنها الرابط المباشر بين الفعل الضار والضرر الناتج عنه، حيث يجب أن يكون الضرر نتيجة للفعل نفسه لكي تقوم هذه العلاقة وهي الركن الثالث من أركان المسؤولية إذ لا يكفي وقوع الفعل الضار بل يجب أن يكون هو السبب المباشر للضرر ويرى البعض أن علاقة السببية هي الشرط الأول للالتزام بالتعويض [1].

من وجهة نظر الباحث بناء على ماسبق إيضاحه وفي سياق الأضرار عبر الإنترنت يجب النظر إلى الفعل الضار وعلاقته بالضرر سواء كان نتيجة تقصير المسؤول أو عطل في الأجهزة أو الشبكة مع ضرورة إثبات تقصير المسؤول ونظرًا لغموض وتعقيد الأفعال الضارة عبر الإنترنت وصعوبة تحديد المسؤول لكن أحيانًا يصعب ربط علاقة السببية بالضرر الناتج؛ لذا يقترح البحث قبل تحديد علاقة السببية يجب النظر إلى طبيعة التزام المسؤول سواء كان التزامًا ببذل عناية أو تحقيق نتيجة لتحديد مدى مسؤوليته عن الفعل الضار وما إذا كان يكفل الضرر أم لا.

وفي نهاية هذا الفصل بما أننا في عصر يشهد اعتمادًا متزايدًا على الإنترنت في مختلف جوانب الحياة أصبحت حماية البيانات الشخصية قضية بالغة الأهمية نظرًا للمخاطر الجمة التي تهدد خصوصية الأفراد وسلامة معلوماتهم و يُعتبر الاعتداء على البيانات الشخصية أحد أبرز التحديات التي تواجه المستخدمين في العالم الرقمي" خاصة مع تزايد حالات الاختراق والاستغلال غير المشروع للبيانات الحساسة مثل المعلومات

---

[1] عبد القادر الفار، مصادر الالتزام" مصادر الحق الشخصي في القانون المدني، دار الثقافة للنشر والتوزيع، عمان الأردن، 2006، ص 140: 142.

الصحية والمالية والعائلية" وهذا الواقع دفع العديد من الدول بما في ذلك سلطنة عُمان والمملكة الأردنية الهاشمية إلى سن تشريعات متخصصة لتنظيم جمع البيانات الشخصية ومعالجتها وحمايتها ؛ لذلك في هذا الفصل تم استعراض الإطار القانوني لحماية البيانات الشخصية مع التركيز على حقوق الأفراد وواجبات الجهات المعنية بجمع البيانات ومعالجتها حيث تناول المبحث الأول حقوق والتزامات الجهات المعنية و تم تحليل التزامات جمع البيانات الشخصية وضمانات معالجةها مع التأكيد على أهمية مشروعية الغرض من جمع البيانات ودقتها، بالإضافة إلى ضرورة تخزين البيانات بشكل آمن ولفترة زمنية محددة كما تم التطرق إلى دور المتحكم والمعالج في ضمان حماية البيانات مع تحديد التزامات كل منهما وفقًا للتشريعات العُمانية والأردنية. أما المبحث الثاني فقد ركز على التنظيم القانوني للبيانات الشخصية حيث تم استعراض حقوق الأفراد في حماية بياناتهم الشخصية مثل حق الوصول إلى البيانات، وحق التصحيح، وحق الاعتراض وحق النسيان وتم تحليل وسائل الحماية القانونية بما في ذلك الإجراءات الوقائية التي تهدف إلى منع الاعتداء على البيانات قبل وقوعه، وآليات المسؤولية القانونية التي تُفرض على الجهات التي تنتهك خصوصية الأفراد.

ومن خلال تحليل التشريعات العُمانية والأردنية يتضح أن كلا البلدين يولي أهمية كبيرة لحماية البيانات الشخصية مع وجود بعض الاختلافات في التفاصيل والآليات؛ ففي حين يركز التشريع العُماني على حقوق الأفراد مثل الاعتراض والنسيان ويتميز التشريع الأردني بتفصيل أكبر لحقوق الأفراد وإنشاء هيئة وطنية مستقلة لحماية البيانات الشخصية ومع ذلك يواجه كلا التشريعين تحديات في التطبيق الفعال خاصة في ظل التطورات التكنولوجية السريعة والحاجة إلى زيادة الوعي بحقوق الأفراد وواجبات الجهات المعنية.

في الختام يُعتبر الإطار القانوني لحماية البيانات الشخصية خطوة مهمة نحو تعزيز الثقة في البيئة الرقمية وضمان حقوق الأفراد في الخصوصية ومع ذلك يبقى التحدي الأكبر في تطبيق هذه التشريعات بشكل

فعال ومواكبة التطورات التكنولوجية المتسارعة. يتطلب ذلك تعزيز التعاون بين الجهات الحكومية والقطاع الخاص وزيادة الوعي بين الأفراد حول كيفية حماية بياناتهم الشخصية وتبني أفضل الممارسات الدولية في مجال حماية البيانات.

المبحث الثاني: شروط جمع ومعالجة البيانات الشخصية والضمانات القانونية لحمايتها

يشهد عالمنا تحولاً رقمياً متسارعاً، حيث أصبحت البيانات الشخصية ذات قيمة عالية وأهمية متزايدة في مختلف جوانب حياتنا، ومع هذا التطور تزايدت المخاطر المتعلقة بجمع ومعالجة هذه البيانات؛ مما استدعى ضرورة وضع إطار قانوني متكامل لحماية الأفراد وضمان حقوقهم.

يهدف هذا المبحث إلى تسليط الضوء على حقوق والتزامات الجهات المعنية بجمع ومعالجة البيانات الشخصية؛ وذلك من خلال تحليل دقيق لأهم الضمانات القانونية التي تكفل حماية فعالة للبيانات الشخصية، حيث يتناول المبحث التزامات جمع البيانات الشخصي، كما يتم التطرق إلى مشروعية الغرض من جمع البيانات وصحتها بالإضافة إلى مشروعية معالجة جمع البيانات والاحتفاظ بها، أيضًا نتناول ضمانات معالجة البيانات الشخصية؛ حيث يتم التركيز على التحكُّم في البيانات والتزامات المُتحكم بالإضافة إلى معالجة البيانات والتزامات المُعالج؛ وذلك بهدف تقديم تحليل شامل ومتعمق لحقوق والتزامات الجهات المعنية بالبيانات الشخصية؛ لذلك سنتناول في هذا المبحث مطلبين :

نتناول في المطلب الأول: شروط جمع ومعالجة البيانات الشخصية والضمانات القانونية لحمايتها، ونتناول في المطلب الثاني: ضمانات معالجة البيانات الشخصية.

المطلب الأول: شروط جمع ومعالجة البيانات الشخصية والضمانات القانونية لحمايتها

أجمعت المؤسسات الحكومية والخاصة على اختلاف أنواعها كميات هائلة من البيانات الشخصية التي تتراوح بين معلومات بسيطة، كالأسم والعمر والجنس وصولاً إلى بيانات بالغة الخصوصية كالمعلومات الصحية والمالية، و تُخزن هذه البيانات في ملفات وقواعد بيانات ويمكن تشبيه الفرق بينهما بالفرق بين صفحة في كتاب ومكتبة ضخمة؛ فقواعد البيانات تتميز بتنظيمها الهيكلي الذي يسهل عملية البحث عن المعلومات واسترجاعها وتحديثها، على عكس الملف الذي قد يكون البحث فيه عن معلومة معينة أمراً بالغ الصعوبة، وبفضل التطور التكنولوجي أصبح نقل هذه البيانات عبر البلدان أمراً في غاية السرعة، حيث يمكن أن يتم ذلك في ثوانٍ معدودة[1]؛ لذلك سنتناول في هذا المطلب فرعين: الأول مشروعية الغرض من جمع البيانات وصحتها، الثاني مشروعية معالجة جمع البيانات والاحتفاظ بها.

الفرع الأول– مشروعية الغرض من جمع البيانات وصحتها:

مشروعية الغرض من جمع البيانات وصحتها حجر الزاوية في أي عملية لجمع البيانات الشخصية فجمع البيانات يجب أن يستند إلى غرض مشروع ومحدد بوضوح وأن يكون الهدف من جمع البيانات متوافقاً مع القوانين واللوائح ذات الصلة، بالإضافة إلى ذلك يجب أن تكون البيانات التي يتم جمعها صحيحة ودقيقة حيث أن جمع بيانات غير صحيحة أو غير دقيقة يمكن أن يؤدي إلى اتخاذ قرارات خاطئة أو إلى الإضرار بالأفراد.

---

[1] عثمان بكر عثمان، المسؤلية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2013، ص 8.

أولًا- مشروعية الغرض الذي يتم من أجله جمع البيانات:

أدت تكنولوجيا المعلومات إلى اعتماد الأفراد في معاملاتهم اليومية على الحاسوب مما أدى إلى ظهور ما يسمى ببنوك المعلومات والتي يُقصد بها (تكوين قاعدة بيانات تخدم موضوعاً معيناً وتهدف لخدمة غرض معين تتم معالجتها بواسطة الحواسيب وإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض معينة)[1]، و تهدف قواعد البيانات إلى تنظيم ومعالجة المعلومات لخدمة أغراض محددة ولكنها قد تشكل خطرًا على خصوصية الفرد وحريته فجمع وتخزين ومعالجة ونشر البيانات الشخصية بواسطة الحاسوب يحوّل الفرد إلى محور لعمليات آلية تمس جوانب حياته كافة مما يحد من انطلاقته وإبداعه ومشاركته في الحياة العامة و يصبح الفرد أسيرًا للمعلومات التي جمعتها الآلة عنه، مما يهدد حياته الخاصة[2]، كما أن ظهور "بنوك المعلومات" مع التكنولوجيا والتي يُقصد (بها تكوين قاعدة بيانات تخدم غرضاً معيناً أدى إلى تضييق انطلاقات الفرد وإبداعه ومشاركته في شؤون الحياة العامة فالحاسوب يقوم بجمع وتخزين ومعالجة ونشر المعلومات الشخصية للأفراد وكل من هذه الأمور يشكل خطراً على حياة الإنسان الخاصة ويهددها مما يجعل الفرد أسيراً للمعلومات التي جمعتها الآلة عنه).[3]

---

[1] محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، القاهرة، مصر، 2018، ص 129.

[2] محمد رشيد حامد، الحماية الجزائية للمعلومات الشخصية في مواجهة أخطار البنوك، رسالة ماجستير، كلية الحقوق، جامعة آل البيت، عمان، الأدرن، ص 4.

[3] يونس عرب، المخاطر التي تهدد الخصوصية وخصوية المعلومات في العصر الرقمي اتحاد المصارف العربية، الطبعة الأولى، 2002، ص 9.

من وجهة نظر الباحث ونظراً لتفاقم الاعتداءات على البيانات الشخصية فقد توجه المشرع نحو حماية دستورية حيث كشفت خصوصية جرائم الاعتداء على الحياة الخاصة أو البيانات الشخصية عن مشكلة في المكافحة الإجرائية للجريمة المعلوماتية ونتيجة لذلك تحرك المشرع وقد تجسد هذا التدخل التشريعي في سلطنة عُمان من خلال سن التشريعات والقوانين مثل قانون حماية البيانات الشخصية ويهدف هذا التحرك إلى مواكبة التطورات المتسارعة في مجال الجرائم الإلكترونية مما يساهم في تعزيز مكانة سلطنة عُمان كبيئة رقمية آمنة وموثوقة.

ثانيًا- يجب أن تكون البيانات صحيحه وسليمة:

تؤكد سياسة حماية البيانات الشخصية في سلطنة عمان (تعميم رقم 6 / 2024) على أن دقة وسلامة البيانات هما أساس أي نظام فعال لحماية البيانات الشخصية. فالبيانات غير الصحيحة قد تضر بالأفراد؛ لذلك يجب على المؤسسات التي تتعامل مع البيانات الشخصية اتخاذ جميع التدابير لضمان دقتها لأن ذلك ضروري لحماية حقوق الأفراد وحرياتهم وضمان العدالة في القرارات، وتعزيز كفاءة العمليات ومصداقية المؤسسات[1].

كما عرف المشرع العُماني الاختراق في القرار الوزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية في المادة الأولى الفقرة الخامسة بأنه "الدخول غير المشروع إلى البيانات الشخصية بشكل يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير

(1) مقدمة تعميم رقم 6 / 2024 بشأن سياسة حماية البيانات الشخصية لوحدت الجهاز الإداري للدولة، وزارة النقل والاتصالات وتقنية المعلومات.

قانونية"[1]، ويجب على المتحكم إبلاغ الإدارة المختصة خلال 72 ساعة من علمه بالاختراق إذا كان من شأنه أن يؤدي إلى خطر يهدد حقوق أصحاب البيانات الشخصية[2]، و في التشريع الأردني يُشير مصطلح "الإخلال بأمن وسلامة البيانات" إلى أي وصول غير مصرح به إلى البيانات أو أي عملية أو نقل أو إجراء غير مصرح به عليها، ويولي المشرع الأردني أهمية كبيرة لضمان صحة وسلامة البيانات؛ ويتضح ذلك من خلال عدة قوانين وتشريعات، منها قانون حماية البيانات الشخصية الذي يهدف إلى حماية البيانات الشخصية للأفراد، ويشدد على ضرورة أن تكون البيانات صحيحة ودقيقة وحديثة، ويمنح الأفراد الحق في تصحيح بياناتهم الشخصية إذا كانت غير صحيحة أو غير كاملة، وقانون المعاملات الإلكترونية الذي ينظم المعاملات الإلكترونية ويحدد شروط صحة البيانات والمستندات الإلكترونية؛ ويشترط أن تكون البيانات صحيحة وكاملة وموثوقة، وقانون الجرائم الإلكترونية الذي يجرم الأفعال التي تمس بسلامة البيانات؛ مثل الدخول غير المشروع إلى الأنظمة المعلوماتية أو تغيير البيانات أو إتلافها أو نشر بيانات كاذبة أو مضللة[3]، و بمقارنة بين التشريع العُماني والأردني فيما يتعلق بحماية البيانات الشخصية؛ نجد أن كلا التشريعين يهتمان بحماية البيانات الشخصية ويشددان على ضرورة دقة وسلامة البيانات، كما يُجرِّم كلا النظامين الأفعال التي تهدد أمن البيانات، مثل الدخول غير المشروع أو التغيير غير المصرح به ويُلزمان المتحكمين بإبلاغ الجهات المختصة في حال حدوث اختراق للبيانات، ومع ذلك توجد بعض الاختلافات بينهما؛ فالتشريع العُماني يُفصِّل إجراءات نقل البيانات خارج الحدود ويشترط موافقة صريحة من صاحب البيانات بينما يركز التشريع الأردني أكثر على

---

[1] المادة رقم (1 /5) من القرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية، استنادًا إلى المرسوم السلطاني رقم 6/ 2022.

[2] المادة رقم 30 من القرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية، استنادًا إلى المرسوم السلطاني رقم 6/ 2022.

[3] المادة رقم 2 من قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023.

حماية البيانات داخل النطاق الوطني و بالإضافة إلى ذلك يحدد التشريع العُماني بشكل واضح مهام مسؤول حماية البيانات الشخصية وهو جانب لا يتطرق إليه التشريع الأردني بنفس التفصيل.

ومن وجهة نظر الباحث تُعد صحة وسلامة البيانات ضرورية لتعزيز الثقة وحماية حقوق الأفراد ومنع الجرائم الإلكترونية؛ لذا تحرص التشريعات العمانية والأردنية على ضمان ذلك عبر سن قوانين تنظم البيانات الشخصية والمعاملات الإلكترونية وتُجرم التجاوزات.

الفرع الثاني- مشروعية معالجة جمع البيانات والاحتفاظ بها:

في عصر الرقمية تُمثل البيانات الشخصية ثروة قيمة ولكنها تحمل في طياتها مخاطر جمة إذا لم تُعالج ويُحتفظ بها بشكل مسؤول، واستكشاف الأسس القانونية والأخلاقية لمعالجة البيانات الشخصية مع التركيز على مبدأي المشروعية والتناسب؛ إذ يجب معالجة البيانات ومعالجتها وفقًا للقانون وأن تكون ملائمة للأغراض المحددة مع ضمان تخزينها بشكل آمن ومسؤول.

أولًا- أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها:

لا يكتفي القانون العماني بضمان جمع البيانات بشكل مشروع بل يشدد على معالجتها بما يتناسب مع الغرض المحدد الذي جُمعت من أجله، مما يمنع معالجة أي بيانات شخصية بطرق غير قانونية أو دون موافقة صريحة وواضحة من صاحبها كامل الأهلية، ويتوجب على المسؤولين عن المعالجة إبلاغ الأفراد بكيفية جمع بياناتهم، الغرض منها، وأنواع البيانات التي يتم جمعها كما تلزم اللائحة التنفيذية لقانون حماية البيانات الشخصية

المتحكمين بالإبلاغ عن أي اختراق للبيانات خلال 72 ساعة من اكتشافه مما يؤكد التزام التشريع العماني بشفافية وأمن البيانات الشخصية[1].

وتتطلب هذه المعايير أن تتم معالجة البيانات بدقة وأمانة من قبل المسؤولين مع حظر استخدام أي وسائل احتيالية أو غير مشروعة لجمعها أو معالجتها كما يُمنع جمع البيانات الشخصية لأغراض غير قانونية أو مخالفة للنظام العام أو جمع بيانات غير صحيحة أو غير ضرورية لعملية المعالجة[2].

كما يتبنى المشرع الأردني موقفًا واضحًا في حماية البيانات الشخصية حيث يمنح كل فرد الحق في حماية بياناته ولا يجوز معالجتها إلا بموافقة مسبقة أو في حالات مصرح بها قانونًا مع مراعاة المادة (6) من القانون ويتمتع الأفراد بحقوق واسعة تشمل العلم والاطلاع على البيانات وسحب الموافقة وتصحيح البيانات وتخصيص المعالجة وحذف البيانات والاعتراض على المعالجة إذا كانت غير ضرورية كما يهدف هذا النهج إلى ضمان معالجة البيانات بشكل مشروع وشفاف مع احترام حقوق الأفراد وحرياتهم[3].

من وجهة نظر الباحث القانون العُماني لم يكتفِ بضرورة جمع البيانات بطريقة مشروعة فقط بل ألزم أيضًا بمعالجة هذه البيانات بما يتناسب مع الأغراض التي جُمعت من أجلها هذا يعني أنه لا يجوز جمع أو

---

[1] المادة رقم 4 من اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بموجب القرار الوزاري رقم ٣٤ / ٢٠٢٤، والتي تستند إلى المرسوم السلطاني رقم ٦ / ٢٠٢٢، والتي تنص على"يلتزم المتحكم قبل معالجة البيانات الشخصية بالحصول على الموافقة الصريحة لصاحب البيانات الشخصية، ويشترط للاعتداد بالموافقة الآتي:١ – أن تصدر الموافقة من شخص كامل الأهلية.٢ – أن تصدر الموافقة بطريقة واضحة ودون إكراه.٣ – أن تكون الموافقة كتابية أو إلكترونية أو بأي وسيلة أخرى يحددها المتحكم."

[2] سامح عبد الواحد التهامى، الحماية القانونية للبيانات الشخصية " دراسة القانون الفرنسي"، القسم الأول، مجلة الحقوق، جامعة الكويت، مج35، ع 11، 2011، ص 404

[3] المادة رقم 6 من قانون حماية البيانات الشخصية الأردني رقم (24) / 2023

معالجة أي بيانات شخصية أو معلومات بأساليب غير قانونية أو دون موافقة صاحبها، كما يشدد القانون العُماني على أهمية إبلاغ صاحب البيانات بجمعها وطريقة الجمع والغرض منه وأنواع البيانات التي جُمعت، و تعكس هذه الإجراءات الالتزام بحماية البيانات الشخصية وخصوصية الأفراد وضمان أن البيانات التي يتم جمعها تُستخدم بشكل قانوني وأخلاقي؛ و يشير هذا النهج إلى ضرورة وجود شفافية في عملية جمع البيانات ومعالجتها وهو ما يعزز الثقة بين الأفراد والمؤسسات المسؤولة عن جمع البيانات.

تتوافق هذه الإجراءات مع التشريعات الأوروبية التي تؤكد على ضرورة معالجة البيانات الشخصية بطريقة مشروعة وعادلة وشفافة، وتطالب بمعالجتها بدقة وأمانة مع حظر استخدام أي وسائل احتيالية أو غير مشروعة لجمعها أو معالجتها، كذلك يمنح المشرع الأردني كل فرد الحق في حماية بياناته ويشترط موافقة مسبقة لمعالجتها إلا في حالات مصرح بها قانونًا، يعزز هذا النهج حماية حقوق الأفراد وخصوصياتهم ويزيد من ثقة الأفراد في المؤسسات التي تجمع بياناتهم، و مع ذلك قد تؤدي المتطلبات القانونية الصارمة إلى تعقيد عمليات جمع البيانات وزيادة التكاليفمما يتطلب موارد إضافية وإجراءات تنظيمية معقدة؛ لذا لتعزيز فعالية هذا النهج يُقترح تطوير برامج توعية شاملة للمؤسسات والأفراد حول أهمية حماية البيانات الشخصية وتقديم دعم فني وتقني للمؤسسات لضمان الامتثال وتبسيط الإجراءات القانونية لتحقيق توازن بين حماية البيانات وفعالية العمليات.

بناء على ماسبق إيضاحه نتفق مع الرأي الفقهي الذي يؤكد على ضرورة أن تكون البيانات المراد تسجيلها متناسبة وضرورية للغرض المقصود وأن يكون الهدف مرتبطًا بمهمة الجهة القائمة على الحاسب الآلي

مع مراعاة حق الخصوصية فمثلاً إذا كان من الضروري لوزارة الاتصالات توضيح أرقام المكالمات الهاتفية يجب عليها إخفاء بعض أرقام المشترك المطلوب حفاظاً على سرية الاتصالات[1].

ثانيًا- تخزين البيانات من أجل الغرض المحدد لها:

يحظر المشرع العُماني بموجب المادة 17 من قانون حماية البيانات الشخصية الاحتفاظ بالبيانات التي تمت معالجتها لمدة زمنية تتجاوز الفترة اللازمة لتحقيق الغرض المحدد الذي جُمعت البيانات من أجله و يحدد هذا النص قاعدة أساسية مفادها أن تخزين البيانات يجب أن يكون مؤقتًا ومحددًا بفترة زمنية معينة وليس دائمًا و الغرض المحدد هنا هو نقطة الارتكاز حيث يلتزم المسؤول عن معالجة البيانات بتحديد هذه المدة بناءً على مدى الحاجة إليها لتحقيق الأهداف المشروعة التي أُجريت المعالجة لأجلها في البداية كتقديم خدمة أو إتمام معاملة أو استيفاء التزام قانوني؛ مما يضمن تقليل البيانات المُخزنة وعدم استغلالها بعد زوال الحاجة إليها[2].

تُكمل المادة 27 من اللائحة التنفيذية لقانون حماية البيانات الشخصية المبدأ الوارد في المادة 17 حيث تفرض التزامًا على المتحكم أو المعالج بالاحتفاظ بمستندات عمليات المعالجة ذاتها ولكن وفق ضوابط صارمة تخدم مبادئ المشروعية وسلامة البيانات و هذه الضوابط تشمل التأكيد على أن يكون سبب الاحتفاظ مشروعًا ومحددًا بوضوح وأن تكون المدة الزمنية للاحتفاظ محددة ومتناسبة مع الغرض منه دون تجاوز الضرورة

---

[1] علاء عيد طه، الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية، مجلة كلية الحقوق والعلوم السياسية، جامعة الملك سعود، مجلد 32، 2016، ص 3.

[2] المادة 17 من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

و علاوة على ذلك تؤكد المادة على أهمية توفير أنظمة حماية فنية متطورة لضمان الاحتفاظ الآمن لهذه المستندات مما يعزز الثقة في عملية المعالجة ويقلل من مخاطر الوصول غير المصرح به أو الانتهاك.[1]

يتبنى المشرع الأردني نهجًا شاملًا ودقيقًا في تنظيم معالجة البيانات مما يضمن أن عملية تخزين البيانات نفسها تلتزم بمبدأ تحديد الغرض ويُعرّف القانون الأردني "المعالجة" بأنها أي عملية تُجرى على البيانات، سواء كانت يدوية أو آلية، تشمل على وجه التحديد: جمعها، تسجيلها، نسخها، حفظها، تخزينها تنظيمها وإلى آخر ذلك من الإجراءات التي تشتمل حتى على إتلافها أو محوها و هذا التعريف الواسع يعكس حرص المشرع على تغطية جميع جوانب التعامل مع البيانات، بدءًا من التخزين حتى الإتلاف والهدف الأساسي من ذلك هو ضمان حمايتها من أي استخدام غير مشروع أو خارج عن الغرض المحدد لها مسبقًا؛ وبالتالي يفرض هذا الإطار القانوني أن يكون تخزين البيانات مقيدًا دائمًا بالغرض الذي جُمعت من أجله[2].

يعتقد الباحث أن قانون حماية البيانات الشخصية العُماني يحظر بشكل صريح الاحتفاظ بالبيانات التي تتم معالجتها لمدة تتجاوز المدة اللازمة لتحقيق الغرض المحدد لها؛ ما يعني أن الاحتفاظ بالبيانات لا يجوز أن يكون دائمًا بل يجب أن يكون مؤقتًا ومحددًا بفترة زمنية معينة، كما يتعين على المسؤول عن معالجة البيانات أن يحفظ البيانات لمدة زمنية محددة، بحيث لا تتجاوز المدة المطلوبة للأغراض التي جمعت من أجلها؛ و يعكس هذا النهج التزام المشرع العُماني بضمان حماية البيانات الشخصية وخصوصية الأفراد من

---

[1] المادة رقم 27من القرار **الوزاري رقم** 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية، استنادًا إلى **المرسوم السلطاني رقم 6 /** 2022.

[2] المادة رقم 2 من قانون حماية البيانات الشخصية الأردني رقم (24) / 2023

خلال تنظيم صارم وواضح لعمليات الاحتفاظ بالبيانات ومعالجتها ويعزز الشفافية والمسؤولية في التعامل مع البيانات.

وبعد أن أوضحنا اتجاه المشرع العُماني والأردني في تخزين البيانات، نجد كلا الاتجاهين لهما من الإيجابيات والسلبيات سنوضحها على النحو التالي:

الإيجابيات: قانون حماية البيانات الشخصية العُماني يحظر بشكل صريح الاحتفاظ بالبيانات التي تتم معالجتها لمدة زمنية تتجاوز المدة اللازمة لتحقيق الغرض المحدد لها مما يعزز مبدأ الشفافية والمسؤولية. هذا يعني أن الاحتفاظ بالبيانات يجب أن يكون مؤقتًا ومحددًا بفترة زمنية معين، ويجب إبلاغ صاحب البيانات بجمعها وطريقة الجمع والغرض منه وأنواع البيانات التي جُمعت، ويتماشى هذا النهج مع التشريعات الأوروبية التي تؤكد على ضرورة معالجة البيانات الشخصية بطريقة مشروعة وعادلة وشفافة، وضمان حمايتها من أي استخدام غير مشروع.

السلبيات: على الرغم من أهمية المتطلبات القانونية لحماية البيانات إلا أنها قد تُنشئ تعقيدات وتحديات تشغيلية كبيرة للمؤسسات فغالبًا ما تؤدي هذه القواعد الصارمة إلى تعقيد عمليات جمع البيانات ومعالجتها؛ مما يستلزم مخصصات إضافية من الموارد البشرية والتقنية وإجراءات تنظيمية معقدة وتتفاقم هذه الصعوبة عندما تعمل المؤسسة في نطاقات جغرافية متعددة حيث تواجه تحدي التوافق مع تشريعات مختلفة ومتضاربة أحيانًا كما يشكل هذا الالتزام القانوني عبئًا ماليًا وإجرائيًا خاصًا على المؤسسات الصغيرة والمتوسطة التي تفتقر إلى الموارد الكافية للامتثال الكامل و علاوة على ذلك يمكن أن تتسبب القيود المتعلقة بفترات الاحتفاظ الزمنية

المحددة للبيانات في مشكلات عند ظهور حالات استثنائية أو قضايا تتطلب الاحتفاظ بالبيانات لفترات أطول مما هو مُقرر سواء لأسباب ق**انونية قاهرة أو لضرورات تشغيلية.**

المطلب الثاني: ضمانات معالجة البيانات الشخصية

في عالم اليوم الرقمي المترابط أصبحت البيانات الشخصية سلعة ثمينة، مما يستدعي وضع ضمانات قوية لحمايتها من الاستغلال غير المشروع، ويهدف هذا المطلب إلى استعراض الضمانات القانونية والتنظيمية التي تكفل معالجة البيانات الشخصية بشكل آمن وشفاف؛ مع التركيز على دور كل من المتحكم والمعالج في هذا الإطار.

لذلك يتم تناول فالأول مفهوم التحكم في البيانات والتزامات المتحكم، بينما يُلقي الثاني الضوء على معالجة البيانات والتزامات المعالج، وذلك في إطار جهود متكاملة لحماية حقوق الأفراد في عصر البيانات.

الفرع الأول- التحكُم في البيانات والتزامات المُتحكم:

يُعرّف قانون حماية البيانات الشخصية العُماني في المادة الأولى منه "المتحكم" بأنه (الشخص الذي يتولى تحديد أهداف ووسائل معالجة البيانات الشخصية سواء قام بهذه المعالجة بنفسه أو عهد بها إلى طرف آخر)، هذا التعريف يُحدد بوضوح مسؤولية المتحكم في تحديد الغرض من معالجة البيانات وكيفية تنفيذها، مما يجعله المسؤول الأساسي عن ضمان حماية البيانات الشخصية[1].

[1] المادة الأولى من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022

أيضًا يُعرّف المشرع العُماني في التعميم رقم 6 / 2024 بشأن سياسة حماية البيانات الشخصية "وحدة التحكم" بأنها الكيان الذي يحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك، سواء باشرت معالجة البيانات بنفسها أو عن طريق وحدة معالجة أخرى. هذا التعريف يوضح أن وحدة التحكم هي المسؤولة عن تحديد الغاية من معالجة البيانات ووضع الإجراءات اللازمة لذلك بغض النظر عمن يقوم فعليًا بتنفيذ هذه الإجراءات[1].

ويُعرّف المشرع الأردني "مراقب البيانات" بأنه الشخص الطبيعي المعين للإشراف على قواعد البيانات والمعالجة وفقًا لأحكام القانون ، ويؤدي مراقب البيانات دورًا حيويًا في ضمان التزام المسؤولين عن معالجة البيانات بالتشريعات والقوانين المعمول بها، والمتلقي" بأنه أي شخص طبيعي أو اعتباري سواء كان داخل المملكة أو خارجها، يتم نقل البيانات إليه أو تبادلها معه من المسؤول، ويضع المشرع الأردني ضوابط صارمة لعمليات نقل البيانات إلى المتلقين وذلك لضمان حماية البيانات الشخصية من أي استخدام غير مشروع [2]، كما تُعرِّف اللائحة العامة لحماية البيانات الشخصية **المتحكم** بأنه الشخص الطبيعي أو الاعتباري، أو السلطة العامة، أو الوكالة، أو أي هيئة أخرى تحدد بمفردها أو بالاشتراك مع آخرين أغراض ووسائل معالجة البيانات الشخصية؛ هذا التعريف يوضح أن المتحكم هو المسؤول عن تحديد الغايات من معالجة البيانات وكيفية تنفيذها، سواء قام بذلك بمفرده أو بالتعاون مع جهات أخرى[3].

---

[1] التعاريف والمصطلحات الوارة في تعميم رقم 6 / 2024 بشأن سياسة حماية البيانات الشخصية لوحدت الجهاز الإداري للدول، وزارة النقل والاتصالات وتقنية المعلومات.

[2] المادة رقم 2 من قانون حماية البيانات الشخصية الأردني رقم (24) / 2023.

[3] منذر بن عيسى بن سليمان الكيومي وآخرون، التزام الشركات التجارية بحماية البيانات الشخصية في القانون العماني دراسة مقارنة، رسالة ماجستير، جامعة السلطان قابوس، مسقط، 2023، ص 28.

من وجهة نظر الباحث وبناء على ما سبق نجد أن التشريع العُماني يركز على تحديد مسؤوليات "المتحكم" و"وحدة التحكم" بشكل واضح في حين يركز التشريع الأردني على "مراقب البيانات" و"المتلقي" مع وضع ضوابط صارمة لنقل البيانات، وكلا التشريعين يسعيان لضمان حماية البيانات الشخصية من خلال تحديد الأدوار والمسؤوليات بوضوح ووضع معايير صارمة لمعالجة البيانات.

وبما أن التحكم في البيانات والمتحكم يعد طرفاً رئيسياً ومحورياً في مجال معالجة البيانات الشخصية ولضمان أن تتم معالجة البيانات الشخصية دون إنتهاك أو إعتداء على حرمة تلك البيانات فقد حدد المشرع العُماني عدداً من الإلتزامات للقيام بعملية التحكم وعدد من الالتزمات على المتحكم الإلتزام بها:

أولًا- إلتزمات وحدة التحكم:

في التشريع العُماني بناء على ماورد من التعاريف والمصطلحات الوارة في تعميم رقم 6 / 2024 بشأن سياسة حماية البيانات الشخصية لوحدات الجهاز الإداري؛ نجد أن إلتزامات وحدة التحكم:

1- مراعاة جمع البيانات عبر وسائل مشروعة ونزيهة.

2- أن يكون الجمع مقتصرًا على الضروري.

3- أن تكون المعالجة منصفة ومشروعة والبيانات صحيحة ودقيقة وخاضعة للتحديث.

4- ألا تبقى في صورة تسمح بالتعرف على صاحب البيانات بعد انتهاء الغرض منها.

5- طلب الحد الأدنى من البيانات والمستندات.

6- التأكد من موافقة صاحب البيانات على المعالجة.

7- تطبيق التدابير الأمنية والتنظيمية اللازمة للحماية من الإتلاف والفقد والاختراق، ووضع احتياطات أمنية للأنظمة ووسائط التخزين، وفي حال تكليف وحدة معالجة أو طرف ثالث، يجب التأكد من توفير الضمانات وتطبيق التدابير الفنية والتنظيمية وأن تتم المعالجة وفق عقد مكتوب يتضمن شروط الاستبقاء والحذف والتدقيق، ويجب الإفصاح عن البيانات المكتسبة أو المستحدثة ونشر بيان الخصوصية ووضع آليات للإتلاف الآمن وإخطار مركز الدفاع الإلكتروني في حال حدوث اختراق، ومعالجة البيانات داخل حدود سلطنة عمان، والحصول على موافقة المركز قبل نقلها للخارج.[1]

ثانيًا- التزامات المتحكم في البيانات:

تنص المادة (13) من قانون حماية البيانات الشخصية على التزام المتحكم بوصفه الجهة التي تقرر غرض وطريقة معالجة البيانات بوضع إطار شامل من الضوابط والإجراءات لضمان سلامة هذه المعالجة وحماية حقوق الأفراد؛ وتتمثل التزاماته الأساسية في ضرورة تحديد وتقييم المخاطر التي قد يتعرض لها صاحب البيانات جراء المعالجة ووضع إجراءات وضوابط واضحة لنقل وتحويل البيانات بشكل آمن بالإضافة إلى تطبيق التدابير الفنية والإجرائية؛ لضمان أن عملية المعالجة تتوافق تماماً مع أحكام القانون مع الالتزام بأي ضوابط أو إجراءات إضافية تُحددها اللائحة التنفيذية مستقبلاً كالآتي [2]:

---

[1] التعاريف والمصطلحات تعميم رقم 6 / 2024 بشأن سياسة حماية البيانات الشخصية لوحدت الجهاز الإداري للدول وزارة النقل والاتصالات وتقنية المعلومات "أحكام السياسة"

[2] المادة 13 من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

1- **اتخاذ التدابير التقنية والتنظيمية:** يُفرض على المتحكم التزامًا قانونيًا باتخاذ كافة الإجراءات والتدابير التقنية والتنظيمية اللازمة لتأمين البيانات الشخصية وحمايتها؛ وذلك بهدف الحفاظ على سريتها وخصوصيتها وضمان حمايتها من أي اختراق أو إتلاف أو تغيير أو عبث غير مصرح به، ويتعين على المتحكم أن يضع في اعتباره طبيعة ونطاق وأغراض معالجة البيانات، وأن يقوم بتقييم شامل للمخاطر المحتملة التي قد تهدد سرية وخصوصية البيانات الشخصية[1].

2- **التدابير الملائمة أثناء المعالجة:** يجب على المتحكم أن يطبق التدابير المناسبة ليس فقط عند تحديد وسائل معالجة البيانات؛ ولكن أيضًا أثناء عملية المعالجة نفسها، وهذه التدابير تهدف إلى ضمان الالتزام الكامل بأحكام القانون، كما يتعين على المتحكم استخدام آليات لإخفاء البيانات، مثل التشفير وذلك لضمان حماية البيانات بشكل فعال أثناء عملية المعالجة[2].

3- **التدابير التقنية والتنظيمية للإعدادات التلقائية:** يلتزم المتحكم بتطبيق التدابير التقنية والتنظيمية المناسبة في الإعدادات التلقائية لضمان أن تقتصر معالجة البيانات الشخصية على الأغراض المحددة لها فقط، ويتضمن هذا الالتزام تحديد حجم ونوع البيانات التي يتم جمعها ونوع المعالجة التي ستتم عليها ومدة تخزين البيانات ومدى إمكانية الوصول إليها.

---

[1] حبيبة سيف سالم راشد الشامسي، حماية البيانات الشخصية في ضوء القانون الاتحادي رقم 45 لسنة 2021: دراسة مقارنة، مجلة الأمن والقانون، المجلد 31، العدد 1، 2023، ص 34.

[2] نظام حماية البيانات الشخصية على الرابط الالكتورني التالي:
https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1 . تاريخ الزيارة 27 سبتمبر 2025.

4- **مسك سجل خاص للبيانات الشخصية:** يتعين على المتحكم الاحتفاظ بسجل خاص بالبيانات الشخصية يتضمن معلومات مفصلة حول بيانات المتحكم، ومسؤول حماية البيانات، ووصف لفئات البيانات الشخصية، وأسماء الأشخاص المصرح لهم بالوصول إلى البيانات، والفترات الزمنية للمعالجة، وقيودها، وآلية محو البيانات أو تعديلها، بالإضافة إلى معلومات حول حركة البيانات عبر الحدود، والإجراءات التقنية والتنظيمية الخاصة بأمن المعلومات، ويكون المتحكم ملزمًا بتقديم هذا السجل إلى مكتب المعلومات عند الطلب.

5- **تعيين المعالج:** يلتزم المتحكم بتعيين معالج يضمن تطبيق التدابير التقنية والتنظيمية اللازمة، وذلك لضمان توافق عملية معالجة البيانات مع متطلبات القانون ولائحته التنفيذية.

6- **تزويد المكتب بالمعلومات:** يلتزم المتحكم بتزويد مكتب المعلومات بأي معلومات يطلبها، وذلك بناءً على قرار صادر من الجهة القضائية المختصة شريطة أن تكون هذه المعلومات متعلقة باختصاصات المكتب المحددة في القانون ولائحته التنفيذية.

7- **يلتزم المتحكم بالإبلاغ بمجرد علمه بوجود أي إختراق أو إنتهاك للبيانات الشخصية:** يجب على المتحكم إبلاغ الوزارة وصاحب البيانات الشخصية عن أي اختراق أو انتهاك للبيانات الشخصية قد يمس خصوصية وسرية بيانات أصحابها وتقديم نتائج التحقيق في هذا الشأن[1]، وتفرض المادة (14) من قانون حماية البيانات التزاماً استباقياً على المتحكم بضرورة إخطار صاحب البيانات كتابة قبل البدء بالمعالجة ويشمل هذا الإخطار بيانات المتحكم والمعالج، وتفاصيل الاتصال بـ

[1] سيد أحمد محمود أحمد، حماية البيانات الشخصية الرقمية وفقا لأحكام القانون المصري رقم 151 لسنة 2020: حماية البيانات الشخصية المعالجة الكترونيا بين الواقع والمأمول، مجلة العلوم القانونية والاقتصادية، المجلد 66، العدد 1، 2024، ص 1462.

مسؤول حماية البيانات الشخصية والغرض من المعالجة ووصفها الدقيق، وحقوق صاحب البيانات (كالحق في الوصول والتصحيح والنقل)[1]، كما تؤكد المادة (20) على الجانب التنظيمي الداخلي حيث تُلزم المتحكم بتعيين مسؤول حماية البيانات الشخصية وتحدد اللائحة ضوابط اختياره ومهامه، مما يضمن وجود نقطة اتصال متخصصة ومسؤولة داخل الكيان للإشراف على تطبيق هذه الالتزامات والتعامل مع أي انتهاكات محتملة[2].

كما تشمل التزامات وحدة التحكم وفق تعميم رقم 6/2024حماية جميع البيانات جمعها بوسائل مشروعة، و الاقتصار على الضروري، و تطبيق التدابير الأمنية، ونشر بيان الخصوصية، و تتلخص التزامات المتحكم في البيانات، وفقاً للمواد من (13) إلى (23) من قانون حماية البيانات الشخصية في مجموعة من التدابير التي تهدف لضمان أقصى درجات الحماية والشفافية في عملية المعالجة كما يلتزم المتحكم باتخاذ التدابير التقنية والتنظيمية لحماية البيانات وتطبيق التدابير الملائمة أثناء المعالجة لضمان سلامتها كما يجب عليه مسك سجل خاص بالبيانات الشخصية لتوثيق عمليات المعالجة وله الحق في تعيين معالج لضمان توافق معالجة البيانات مع القانون بالإضافة إلى تزويد الوزارة بالمعلومات اللازمة للرقابة والامتثال و الهدف النهائي لهذه الالتزامات المتكاملة هو ضمان حماية البيانات الشخصية من أي انتهاك أو استخدام غير مشروع وفي الوقت نفسه تعزيز الشفافية والعدالة في عملية معالجة البيانات بما يحفظ حقوق أصحابها.

---

(1) المادة رقم (14) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

(2) المادة رقم (20) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

الفرع الثاني- معالجة البيانات والتزامات المعالج:

عـرف المشـرع العُمـاني المعـالج بموجـب المـادة الأولـى مـن قـانون حمايـة البيانـات الشخصـية بأنـه: " الشـخص الـذي يقـوم بمعالجـة البيانـات الشخصـية نيابـة عـن المـتحكم"[1]. وعرُفـت عمليـة المعالجـة بأنهـا: "أي عمليـة تجـرى علـى البيانـات الشخصـية بـأي وسـيلة كانـت يدويـة أو آليـة كعمليـات الجمـع، والتسـجيل أو التحليـل أو التنظـيم أو التخـزين أو التعـديل أو التحـوير أو الاسـترجاع أو المراجعـة أو التنسـيق أو ضـم بعضـها لـبعض أو حجبهـا أو محوهـا أو إلغاءهـا أو الإفصـاح عنهـا، عن طريق إرسالها أو توزيعها أو نقلها أو تحويلها أو إتاحتها بوسائل أخرى".[2]

في التشريع الأردني عرف المعالج بأنه " الشخص الطبيعي أو الاعتباري الذي كون مختصا بمعالجة البيانات"، أما عملية المعالجة هى:"عملية واحدة أو أكثر يتم اجراؤها بأي شكل أو وسيلة بهدف جمع البيانات أو تسجيلها أو نسخها أو حفظها أو تخزينها أو تنظيمها أو نقيحها أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو ربطها ببيانات أخرى أو إتاحتها أو نقلها أو عرضها أو إخفاء هويتها أو ترميزها أو إتلافها أو تقييدها أو محوها أو تعديلها أو توصيفها أو الافصاح عنها بأي وسيلة كانت"[3].

و الأصل في معالجة البيانات الشخصية هو أن يتحكم بها الشخص المسؤول حيث يقوم بوضع السياسات والإجراءات اللازمة للمعالجة كما هو الحال في الشركات التي تُحدّث بيانات العملاء باستمرار سواء

---

[1] 1 من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] مقدمة تعميم رقم 6 / 2024 بشأن سياسة حماية البيانات الشخصية لوحدات الجهاز الإداري للدولة، وزارة النقل والاتصالات وتقنية المعلومات.

[3] المادة رقم 2 من قانون حماية البيانات الشخصية الأردني رقم (24) / 2023.

بالحذف أو الحجب أو الإضافة أو التشفير أو الدمج أو الإتاحة أو غيرها من العمليات أما شركات تقنية المعلومات التي تُعالج البيانات والأسماء وتُطور البرامج للمحاكم فتُعتبر معالجًا للبيانات الشخصية؛ لأنها تقوم بذلك نيابة عن المحاكم وتُمارس عمليات المعالجة وتحتفظ بسجلات البيانات الشخصية للمتقاضين وتؤرشفها وبالمثل تُعتبر الشركات القانونية التي تتعامل مع مكاتب المحاماة وتُخزن بيانات العملاء وتحتفظ بها في برامج خاصة معالجًا للبيانات الشخصية حيث تُنفذ عمليات المعالجة والتحديث وغيرها نيابة عن مكاتب المحاماة[1].

من وجهة نظر الباحث بناء على ما سبق إيضاحه نجد ان المشرع العُماني والأردني اتفقا في أن كلا التشريعين، يُعرّفان المعالج بأنه الشخص الطبيعي أو الاعتباري الذي يتولى معالجة البيانات الشخصية، ويشمل تعريف المعالجة في كلا التشريعين جميع العمليات التي تُجرى على البيانات الشخصية بأي وسيلة، سواء كانت يدوية أو آلية، بما في ذلك الجمع، التسجيل، التحليل، التخزين، التعديل، الإفصاح، والنقل. هذه الأوجه المشتركة تعكس التزام كلا التشريعين بحماية البيانات الشخصية من خلال وضع إطار واضح لعمليات المعالج، لكنهما اختلاف في أن التشريع العُماني يُعرّف المعالج بأنه "الشخص الذي يقوم بمعالجة البيانات الشخصية نيابة عن المتحكم"، مما يركز على دور المعالج في العمل نيابة عن المتحكم. أما التشريع الأردني فيُعرّف المعالج بأنه "الشخص الطبيعي أو الاعتباري الذي يكون مختصاً بمعالجة البيانات"، مشيرًا إلى أن المعالج قد يكون لديه اختصاص محدد في معالجة البيانات.

كما يفصل التشريع الأردني في تعريف المعالجة بشكل أكثر تفصيلاً من التشريع العُماني، حيث يشمل عمليات إضافية مثل "إخفاء الهوية" و"ترميز البيانات"؛ مما يُظهر حرص المشرع الأردني على تغطية جميع

[1] منذر بن عيسى بن سليمان الكيومي وآخرون، مرجع السابق، ص 42.

جوانب معالجة البيانات الشخصية، وبهذا يمكن القول إن التشريعين يتشابهان في التركيز على حماية البيانات الشخصية من خلال تحديد الأدوار والمسؤوليات بوضوح إلا أن التشريع العُماني يُركز على دور المعالج في العمل نيابة عن المتحكم بينما يُركز التشريع الأردني على اختصاص المعالج ويُفصل في العمليات المشمولة في المعالجة بشكل أكثر تفصيلا [1]:

1- **التدقيق الخارجي لمعالجة البيانات:** بناءً على طلب الوزارة، يلتزم كل من المتحكم والمعالج بتعيين مدقق خارجي مستقل، ويهدف هذا التدقيق إلى التحقق من أن إجراءات معالجة البيانات الشخصية تتوافق مع أحكام هذا القانون، وكذلك مع الإجراءات والضوابط التي يحددها المتحكم في المادة (13)، وقد تم تحديد ضوابط وإجراءات تعيين المدقق الخارجي في اللائحة التنفيذية، كما يتوجب على المتحكم والمعالج تزويد الوزارة بنسخة من تقرير المدقق الخارجي بعد الانتهاء من عملية التدقيق.
2- **الاحتفاظ بمستندات معالجة البيانات: يجب** على كل من المتحكم والمعالج الاحتفاظ بسجلات ووثائق عمليات معالجة البيانات الشخصية، وقد تم تحديد المدد والإجراءات اللازمة لهذا الاحتفاظ في اللائحة التنفيذية.
3- **التعاون مع الوزارة في تقديم البيانات:** يتوجب على كل من المتحكم والمعالج التعاون بشكل كامل مع الوزارة، وتزويدها بأي بيانات أو مستندات تطلبها لممارسة اختصاصاتها وفقًا لأحكام هذا القانون، كما تم تحديد المدة الزمنية اللازمة لتقديم هذه البيانات والمستندات في اللائحة التنفيذية.
4- **الإبلاغ عن اختراق البيانات الشخصية:** في حالة حدوث أي اختراق للبيانات الشخصية يؤدي إلى تدميرها، أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بشكل غير قانوني ويلتزم المتحكم بإبلاغ الوزارة

[1] المواد من المادة 16 إلى 23 المادة من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022

وصاحب البيانات الشخصية بهذا الاختراق ويتم تحديد الضوابط والإجراءات اللازمة لهذا الإبلاغ في اللائحة التنفيذية.

5- **تعيين مسؤول حماية البيانات الشخصية:** يلتزم المتحكم بتعيين مسؤول لحماية البيانات الشخصية داخل مؤسسته ويتم تحديد ضوابط اختيار هذا المسؤول ومهامه في اللائحة التنفيذية.

6- **ضمان سرية البيانات الشخصية:** يلتزم المتحكم بضمان سرية البيانات الشخصية، وعدم نشرها أو الإفصاح عنها إلا بموافقة صريحة ومسبقة من صاحب البيانات الشخصية، ويتم تحديد التفاصيل والإجراءات المتعلقة بهذا الالتزام في اللائحة التنفيذية.

7- **الموافقة الكتابية على المواد الإعلانية:** قبل مواد إعلانية أو تسويقية ذات طابع تجاري إلى صاحب البيانات الشخصية، يجب على المتحكم الحصول على موافقة كتابية صريحة منه.

8- **نقل البيانات الشخصية خارج سلطنة عمان:** مع عدم الإخلال باختصاصات مركز الدفاع الإلكتروني يجوز للمتحكم نقل البيانات الشخصية أو السماح بنقلها خارج حدود سلطنة عمان، وذلك وفقًا للضوابط والإجراءات التي تحددها اللائحة التنفيذية، ويُحظر على المتحكم نقل البيانات الشخصية إذا كانت معالجتها مخالفة لأحكام هذا القانون، أو إذا كان من شأن هذا النقل إلحاق ضرر بصاحب البيانات الشخصية.

أما المشرع الأردني نجده قد وضع ضوابط لعملية المعالجه في المادة 6 من قانون حماية البيانات الشخصية تتمثل في الآتي[1]:

أ- يجوز معالجة البيانات دون الحاجة لموافقة مسبقة من الشخص المعني في الحالات التالية:

([1]) المادة 6 من قانون حماية البيانات الشخصيَّة الأردني / 2021م.

1. **المهام الحكومية:** إذا كانت المعالجة ضرورية لتنفيذ مهام جهة حكومية مختصة، أو من خلال جهات متعاقدة معها، بشرط الالتزام بقواعد هذا القانون.
2. **الرعاية الصحية:** إذا كانت المعالجة ضرورية لأغراض طبية وقائية، أو للتشخيص الطبي، أو لتقديم الرعاية الصحية من قبل ممارس طبي مرخص.
3. **حماية الأرواح:** إذا كانت المعالجة ضرورية لحماية حياة الشخص المعني أو مصالحه الحيوية.
4. **منع الجريمة:** إذا كانت المعالجة ضرورية لمنع جريمة أو كشفها من قبل جهة مختصة، أو لملاحقة الجرائم.
5. **الالتزام بالقانون:** إذا كانت المعالجة مطلوبة بموجب أي قانون أو قرار قضائي.
6. **القطاع المالي:** إذا كانت المعالجة مطلوبة لعمل البنوك والجهات الخاضعة لرقابة البنك المركزي، بما في ذلك تبادل البيانات داخل وخارج المملكة.
7. **الحالات المنصوص عليها في النظام:** إذا كانت المعالجة تتم وفقًا لنظام صادر بموجب هذا القانون.
8. **البحث العلمي والإحصائي:** إذا كانت المعالجة ضرورية لأغراض البحث العلمي أو التاريخي أو الإحصائي، بشرط عدم استخدامها لاتخاذ قرارات تخص أفرادًا محددين، أو لمتطلبات الأمن الوطني أو لتحقيق المصلحة العامة.
9. **البيانات المتاحة للجمهور:** إذا كانت البيانات متاحة للجمهور من قبل الشخص المعني.

ب- **التخلص من البيانات:** يجب التخلص من البيانات بعد انتهاء الغرض من معالجتها، إلا إذا نص القانون على خلاف ذلك[1].

كما يتحمل القائم بمعالجة البيانات مسؤولية كبيرة في ضمان حمايتها و يجب عليه اتخاذ جميع التدابير والإجراءات اللازمة، ضمن نطاق الغرض المحدد للمعالجة وخلال المدة الزمنية المطلوبة و يُمنع منعًا باتًا على القائم بالمعالجة القيام بأي فعل يتعارض مع الضوابط المحددة لحماية البيانات الشخصية؛ حيث أن أي مخالفة تعرضه للمساءلة القانونية، وقد تم توسيع نطاق المسؤولية ليشمل المشاركة في معالجة البيانات مع اشتراط وجود عقد مكتوب ينظم هذه المشاركة، وفي حال عدم وجود هذا العقد، يعتبر جميع المشاركين مسؤولين بالتضامن عن أي إجراء مخالف، كما يُلزم القائم بالمعالجة بتأمين عملية المعالجة والأجهزة المستخدمة فيها لضمان سلامة البيانات وحمايتها من أي تهديدات[(2)].

المشرعين بينهما أوجه اختلاف حيث أن التشريع العُماني يركز على تحديد مسؤوليات المتحكم والمعالج بشكل واضح ويُلزم بتعيين مدقق خارجي والاحتفاظ بسجلات ووثائق عمليات المعالجة، التعاون مع الوزارة في تقديم البيانات، الإبلاغ عن اختراق البيانات، تعيين مسؤول حماية البيانات، ضمان سرية البيانات، الموافقة الكتابية على المواد الإعلانية وتنظيم نقل البيانات خارج سلطنة عمان.

---

[1] حماية الخصوصية في العصر الرقمي في ظل قانون حماية البيانات الشخصية الأردني على الرابط الالكتروني : حماية الخصوصية في العصر الرقمي في ظل قانون حماية البيانات الشخصية الأردني - نصير ومشاركوه تاريخ الزيارة 25 سبتمبر 2025.

[(2)] عبد السلام أحمد خلف العرمان، الحماية الجزائية للبيانات الشخصية في التشريع الأردني دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، عمان، 2022، ص 68.

في المقابل المشرع الأردني وضع ضوابط لعملية المعالجة، بما في ذلك الحالات التي يمكن فيها معالجة البيانات دون الحاجة لموافقة مسبقة، مثل المهام الحكومية، الرعاية الصحية، حماية الأرواح، منع الجريمة، الالتزام بالقانون، القطاع المالي البحث العلمي والإحصائي، والبيانات المتاحة للجمهور، كما يُلزم القانون الأردني بالتخلص من البيانات بعد انتهاء الغرض من معالجتها.

بوجه عام نرى أن التشريع العُماني يركز على الإجراءات والضوابط الصارمة لضمان حماية البيانات الشخصية، بينما يحدد التشريع الأردني حالات محددة لمعالجة البيانات دون موافقة مسبقة مع وضع ضوابط لضمان حماية البيانات.

الفصل الثاني
جرائم انتهاك البيانات الشخصية في العصر الرقمي

تمهيد:

لقد أحدث ظهور الإنترنت وأنظمة المعلومات مدعومًا بالتكنولوجيا والأجهزة الحديثة ثورة هائلة في وسائل الاتصال مما أدى إلى تحولات جذرية في العديد من المفاهيم والقيم العالمية وظهور أنواع جديدة وغير مسبوقة من الجرائم، وهذا التطور وما نتج عنه من أفعال إجرامية ومسائل قانونية معقدة بشأن مدى انطباق النصوص العقابية التقليدية عليها أثار إشكاليات حول تطبيق المبادئ العامة في قوانين العقاب على جرائم الإنترنت الحديثة، مما استدعى تدخل المشرعين لمواجهة هذه التحديات المستجدة[1].

فالبصمة الواضحة لثورة الاتصالات والمعلوماتية أصبحت تستلزم بالضرورة وضع تعريفات جديدة ومبتكرة للجريمة، تعريفات تكون قادرة على استيعاب الواقع المعقد والمتغير للجرائم الحديثة والمتقدمة التي لم يشهدها العالم من قبل وهذه الجرائم بطبيعتها المتطورة والمتشعبة غالبًا ما تتجاوز القدرة الاستيعابية للتعريفات التقليدية للجريمة مما يستدعي جهدًا تشريعيًا مضاعفًا فالجريمة الحديثة في عصرنا الراهن قد تعتمد بشكل أساسي على النظام المعلوماتي وشبكاته المعقدة، أو قد تُرتكب بشكل كامل أو جزئي بواسطة هذه الأنظمة.

وانطلاقًا من حرص المشرع العُماني على معالجة هذه الجرائم المستحدثة، وقد استجابت سلطنة عُمان لهذه التحديات من خلال إرساء إطار تشريعي شامل يهدف إلى تنظيم هذا المجال وضمان الحماية الجزائية

---

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت "دراسه مقارنة"، الطبعة الثانية، دار النهضة العربية للنشر، القاهرة، مصر، 2009، ص 17، 18

للبيانات الشخصية وتُشكّل هذه المنظومة القانونية شبكة من التشريعات الأساسية التي تشمل قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم (2022/6) ولائحته التنفيذية (2024/34)، وقانون الجزاء العُماني الصادر بالمرسوم السلطاني رقم (2018/7) إلى جانب قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2011/12)، وغيرها من التشريعات ذات الصلة؛ لتعمل جميعها معاً على مواجهة الجرائم المعلوماتية وحماية الفضاء الرقمي في السلطنة.

ويعكس هذا التوجه التشريعي المتزايد الحاجة الملحة لتجريم هذه السلوكيات الحديثة في إطار قانوني مستحدث وقادر على ملاحقة مرتكبيها جنائيًا، وذلك نظرًا للتعاظم الكبير في اعتماد الأفراد والمؤسسات الحكومية والخاصة في سلطنة عُمان على تقنية نظم المعلومات في مختلف جوانب العمل والحياة الشخصية؛ لذلك سنتناول في هذا الفصل مبحثين:

المبحث الأول: الجرائم الناتجه عن إساءة استخدام وسائل الفضاء الرقمي.

المبحث الثاني: المسؤولية الجزائية عن انتهاك البيانات الشخصية.

المبحث الأول:

الجرائم الناتجه عن إساءة استخدام وسائل الفضاء الرقمي

لقد أدت التطورات المتسارعة في تكنولوجيا الاتصالات ونظم المعلومات التجارية إلى إحداث تحولات جذرية في مختلف جوانب الحياة وباتت هذه المبادرة التكنولوجية قوة دافعة حتمية للمشرعين في سعيهم الدؤوب لتطوير وتحديث نظرية الجريمة ويتجلى هذا التطوير بشكل خاص في إعادة صياغة المفاهيم المتعلقة بسلوك الجاني وطبيعة الفعل الإجرامي وذلك للانتقال تدريجيًا من الإطار التقليدي الذي نشأت فيه القوانين الجنائية إلى مفاهيم قانونية حديثة ومتجددة تكون أكثر قدرة وفعالية في مواجهة التحديات التي تفرضها الجرائم المستجدة والمعاصرة، ونظرًا للطبيعة الفريدة للفضاء الرقمي وتنوع الأفعال الإجرامية التي يمكن ارتكابها من خلاله أو بالاستعانة بأدواته فقد بات من الضروري إعادة تقييم وتحديد مسؤولية الفاعل الإجرامي بآليات تتناسب مع هذه البيئة الرقمية المستحدثة وبشكل يختلف جوهريًا عن آليات تحديد الفاعل في الجرائم التقليدية، ويهدف هذا المبحث بشكل أساسي إلى التعمق في دراسة هذا التحول التشريعي الضروري وتجلياته في النظام القانوني العماني، وكيف يسعى هذا النظام لمواكبة هذه التحديات الجنائية الجديدة؛ لذلك ينقسم هذا المبحث إلى مطلبين:

المطلب الأول: جرائم انتهاك البيانات الشخصية الواقعة على النظام المعلوماتي.

المطلب الثاني: جرائم انتهاك البيانات الشخصية الواقعة بواسطة استغلال الاتصالات المعلوماتية.

المطلب الأول:

جرائم انتهاك البيانات الشخصية الواقعة على النظام المعلوماتي

إن جرائم الاتصال الحديثة يمكن أن تستهدف المعلومات النظامية ذاتها إذا توافرت أركانها المعنوية حيث تشكل المعلومات المتمثلة في البيانات أو المعلومات الإلكترونية بكافة أشكالها محلًا للاعتداء فقد تتعرض هذه المعلومات للتشغيل غير المصرح به أو الإتلاف أو التزوير أو التلاعب بها وغير ذلك من الأفعال غير المشروعة التي قد ترقى إلى مرتبة الجرائم ولا يقتصر الأمر هنا على إخفاء أو تغيير الواقع المتعلق بالبيانات الكاملة المخزنة على أجهزة الحاسب الآلي أو الأجهزة المصرح بها أو غيرها بل يشمل أيضًا استهداف وإخفاء المعلومات المعنوية المتكاملة التي تتضمنها هذه البيانات أو المعلومات الإلكترونية[1]، وبينما لا تثير الجرائم الواقعة على المكونات المادية للنظام المعلوماتي إشكالات قانونية كبيرة لكونها مشمولة بالحماية الجنائية التقليدية فإن هذا المطلب سيتناول أبرز الجرائم المعلوماتية التي تستهدف المكونات المعنوية للنظام المعلوماتي والتي يغلب عليها الطابع المالي على سبيل المثال لا الحصر؛ لذلك سنتناول في هذا المطلب فرعين: الفرع الأول: جريمة السرقة التقنية، والفرع الثاني: جريمة الاعتداء والاختراق التقني للبرامج والنظم المعلوماتية.

---

[1] نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 97.

الفرع الأول- جريمة السرقة المعلوماتية:

كما هو الحال في العديد من التشريعات المعترف بها أولى المشرع العُماني حق الملكية أهمية قصوى وجعل من حمايته القانونية ضمانة أساسية، وقد تجلى ذلك في تجريم أي فعل غير مشروع يستهدف المال ويحرم صاحبه منه كليًا أو جزئيًا بأي وسيلة كانت سواء بعلمه أو بغير رضاه وفي ظل التطور التكنولوجي برزت صور مستحدثة للسرقة مثل سرقة المعلومات المخزنة ونظرًا للقيمة التكنولوجية الكبيرة التي تحتلها هذه المعلومات؛ لذا يهدف هذا الفرع إلى التعرف على جريمة السرقة التقنية وتبيان طرق إثباتها ومحلها.

أولًا- تعريف السرقة المعلوماتية:

نصت المادة رقم (3) من قانون مكافحة جرائم تقنية المعلومات التي تجريم الدخول غير المصرح به إلى المواقع أو الأنظمة المعلوماتية بهدف إلغاء أو تغيير أو نسخ أو تدمير أو نشر بيانات ومعلومات إلكترونية إذا كان هذا الفعل يتم بنية الاستيلاء على تلك البيانات والمعلومات وحرمان صاحبها منها، فقد يرقى إلى مفهوم السرقة اللا تقنية[1]، أيضًا المادة 278 من القانون الجزائي العُماني رقم 7 عرفت السرقة بأنها" الاستيلاء على مال مملوك للغير وقابل للنقل بطريقة غير قانونية"[2]، وتوسع هذه المادة نطاق مفهوم المال المنقول ليشمل القوى التي يتم حيازتها والسيطرة عليها مثل الماء والكهرباء والغاز حيث تعتبرها في حكم الأشياء المنقولة عند تطبيق أحكام القانون الجنائي المتعلقة بالسرقة و هذا يعني أن الاستيلاء غير المشروع على هذه القوى يخضع للعقوبات المقررة لجريمة السرقة تمامًا كسرقة الأشياء المادية المنقولة.

---

[1] المادة رقم (3) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] المادة رقم (28) من القانون الجزائي العُماني الصادر بالمرسوم السلطاني رقم 7 / 1974.

من وجهة نظر الباحث بناء على المادة السابقة السرقة هى الاستيلاء غير المشروع على مال مملوك للغير وقابل للنقل وبذلك تجرم الاعتداء على ملكية الغير للأشياء ذات القيمة وحقهم في الاستئثار بها ويوضح هذا التعريف وحدة نطاق التجريم سواء كانت الوسيلة تقنية أو تقليدية حيث تعتبر جريمة تطال الأشخاص الذين يستولون على المال دون المساهمة بالضرورة في إخراجه من حيازة صاحبه ويكفي اشتراكهم في وجود المال في حيازة الفاعل بطريقة ما مع اختلافهم في طريقة ارتكاب الفعل لكن الفرق بين السرقة العادية والسرقة التقنية يتمثل في السلوك والإثبات.

ثانيًا- السلوك:

تتشابه السرقة التقنية مع السرقة العادية من حيث الهدف وهو الاستيلاء على ملكية الغير للأشياء ذات القيمة وحرمان الضحية من حق التصرف فيها إلا أن السلوك الجرمي في السرقة التقنية يعتمد على تحوير المفهوم التقليدي للركن المادي حيث يستخدم الفاعل وسائل إلكترونية متطورة لتحقيق الاستيلاء دون حاجة إلى فعل مادي ملموس كما في السرقة التقليدية فبدلاً من الكسر أو الخلع الجسدي يتم الاختراق الرقمي لنظم المعلومات (مثل تحويل الأموال إلكترونيًا من حسابات البنوك عبر الإنترنت) مما يمكن الجاني من تنفيذ الجريمة دون بذل جهد عضلي أو وجود مادي في مكان الجريمة، وهذا التطور أحدث تحولًا جذريًا في النظام القانوني التقليدي خاصة فيما يتعلق بركن فعل الأخذ الذي لم يعد يتطلب حركة فيزيائية مباشرة، بل تحول إلى فعل افتراضي يتم عبر الفضاء الرقمي[1].

[1] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الاسكندرية، مصر، 2006، ص 203.

وبناء على ما نصت عليه المادة رقم (3) من قانون مكافحة جرائم تقنية المعلومات فإن سلوك جريمة السرقة التقنية يتمثل في الاستخدام المتعمد لوسائل تقنية المعلومات للوصول غير المصرح به إلى البيانات والمعلومات الإلكترونية، والاستيلاء عليها أو نسخها أو نقلها بنية الحرمان أو تحقيق منفعة غير مشروعة، وغالبًا ما يتم هذا السلوك عن بعد ويتضمن تجاوز الإجراءات الأمنية هذه السلوكيات مجرمة بموجب مواد متعددة في قانون مكافحة جرائم تقنية المعلومات وإن لم يرد مصطلح "السرقة التقنية" صراحة.

ثالثًا– الإثبات:

إثبات جريمة السرقة التقنية يعتمد على جمع الأدلة الرقمية والرقمية المادية التي تدين المتهم ويمكن أن تشمل هذه الأدلة:

1. سجلات الوصول والولوج: تحتفظ الأنظمة والخوادم بسجلات مفصلة لمحاولات الوصول والولوج يمكن تحليل هذه السجلات لتحديد عناوين IP، والأوقات والحسابات المستخدمة في الوصول غير المصرح به إلى البيانات أو المعلومات الإلكترونية هذه السجلات قد تثبت أن المتهم قام بالدخول إلى نظام محمي دون إذن، كما هو مجرم في المادة (3) والمادة (6) من قانون مكافحة جرائم تقنية المعلومات.
2. آثار البرامج الضارة: في حال استخدام برامج خبيثة لسرقة البيانات يمكن تحليل الأجهزة والأنظمة المصابة للعثور على آثار هذه البرامج مثل الملفات المصابة والعمليات المشبوهة والتعديلات في النظام. وجود هذه الآثار قد يربط المتهم بالجريمة إذا تم العثور على أدلة تشير إلى قيامه بنشر أو استخدام هذه البرامج كما

قد يندرج تحت المادة (9) من قانون مكافحة جرائم تقنية المعلومات المتعلقة بإدخال ما يعطل النظام أو يتلف البيانات[1].

3. تحليل حركة مرور الشبكة: يمكن تحليل بيانات حركة المرور على الشبكات لتحديد عمليات نقل البيانات غير المصرح بها أو المشبوهة. يمكن أن يكشف هذا التحليل عن نسخ أو نقل بيانات حساسة من نظام إلى آخر دون وجه حق، مما قد يشير إلى سرقة البيانات.
4. الأدلة الجنائية الرقمية: يتضمن ذلك فحص الأجهزة الرقمية المضبوطة (مثل الحواسيب والهواتف المحمولة والأقراص الصلبة) لاستعادة البيانات المحذوفة وتحليل الملفات وتتبع الأنشطة التي قام بها المستخدم، ويمكن أن يكشف هذا الفحص عن أدلة تثبت قيام المتهم بنسخ أو نقل أو استخدام البيانات المسروقة.
5. اعترافات المتهم والشهود: كغيرها من الجرائم يمكن أن يكون اعتراف المتهم أو شهادات الشهود دليلًا على ارتكاب السرقة المعلوماتية.
6. الأدلة المادية: قد تشمل الأجهزة أو الأدوات التي استخدمت في ارتكاب الجريمة، مثل أجهزة تخزين خارجية تم نسخ البيانات إليها بشكل غير قانوني.

أدّت ثورة نظم المعلومات وتقنيات الاتصالات إلى ظهور ما يُعرف بالنقد الإلكتروني (أو البنك الرقمي) الذي بات يحل محل النقد التقليدي في التعاملات المالية اليومية و يقوم هذا النظام على تحويل الأموال الحقيقية المودعة في الحسابات البنكية إلى رصيد إلكتروني مُخزَّن في بطاقات ممغنطة كبطاقات الائتمان أو الصرف الآلي؛ مما يتيح لحاملها إجراء معاملاته دون الحاجة لأموال ملموسة ورغم المزايا الكبيرة والتقنيات الأمنية المصممة لحماية هذه الأنظمة فقد جعل هذا التطور الأموال الإلكترونية عرضة للجرائم الحديثة مثل الاعتداء

[1] المادة رقم (9) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

على الذمة المالية وسرقة الأموال أو تزوير البطاقات أو الاستيلاء عليها عبر الاختراق الإلكتروني وقد شكّل هذا تحديًا كبيرًا أمام التشريعات الجزائية التقليدية؛ حيث أظهرت هذه الجرائم الجديدة قصورًا في النماذج التجريمية الكلاسيكية (مثل جريمة السرقة العادية) عن ملاحقة الفاعلين بفعالية و هذا القصور بالإضافة إلى تعقيدات تحديد المسؤولية في البيئة الرقمية وضع العديد من التشريعات العالمية أمام ضرورة إعادة النظر في كيفية معالجة هذه الجرائم بشكل يتناسب مع طبيعتها الإلكترونية المستحدثة[1].

إلا أن المُشرّع العُماني سارع إلى توفير حماية قانونية صارمة للبطاقات المالية سواءً من العبث بمعلوماتها أو بياناتها من قِبَل أي شخص(بما في ذلك حامل البطاقة نفسه) نظرًا للآثار الخطيرة التي تترتب على هذه الجرائم، والتي تُهدد استقرار المعاملات المالية وزعزعة الثقة في الاقتصاد الوطني وقد نصت المادة (28) من قانون مكافحة جرائم تقنية المعلومات على عقوبات رادعة لكل من يقوم بتزوير بطاقة مالية أو يصنع أجهزة أو مواد تُسهل ذلك أو يستولي على بياناتها أو يستخدمها دون وجه حق عبر الشبكة المعلوماتية، حيث تتراوح العقوبة بين الحبس من شهر إلى ستة أشهر وغرامة مالية من 500 إلى 1000 ريال عُماني.

أما إذا ارتُكبت هذه الأفعال بقصد الاستيلاء على أموال الغير أو الاستفادة من خدمات البطاقة تزيد العقوبة إلى سجن من ستة أشهر إلى سنة مع غرامة من 1000 إلى 5000 ريال، وفي حال تحقق الاستيلاء الفعلي تشدد العقوبة لتصل إلى سجن من سنة إلى ثلاث سنوات وغرامة من 3000 إلى 10,000 ريال عُماني،

[1] أحمد خليفة الملط، المرجع السابق، ص 235.

مما يعكس حرص المشرع على مواكبة التحديات الأمنية الناشئة عن التطور التقني وحماية الاقتصاد الرقمي من الجرائم المستحدثة[1].

من وجهة نظر الباحث بناء على ما سبق إيضاحه إثبات جريمة السرقة التقنية يتطلب تضافر الأدلة الرقمية والرقمية المادية وتحليلها من قبل خبراء متخصصين في مجال الأدلة الجنائية الرقمية لتقديمها للمحكمة بشكل قانوني ومقنع وعلى الرغم من أن القانون لا يحدد مادة خاصة بالإثبات فإن طبيعة الجرائم المنصوص عليها فيه تستلزم الاعتماد على هذه الأنواع من الأدلة لإدانة المتهمين.

رابعًا– محل جريمة السرقة المعلوماتية:

يُعرّف قانون مكافحة جرائم تقنية المعلومات المادة (3) ويُجرّم الدخول غير المصرح به إلى الأنظمة الإلكترونية أو المواقع كما يُشدد العقوبة على هذا الفعل إذا نتج عنه تدمير أو نسخ أو نشر البيانات المخزنة وتُصعّد العقوبة إلى السجن مدة لا تقل عن سنة وغرامة تصل إلى ثلاثة آلاف ريال عماني إذا كانت البيانات التي تم انتهاكها هي بيانات شخصية ما يؤكد على حماية البيانات الحساسة المخزنة في الأنظمة المعلوماتية[2]، سواءً كانت نصوصًا أو رموزًا أو إشارات – طالما كانت قابلة للاستخدام كمعلومات وتشمل هذه البيانات سواءً تلك المخزنة على أجهزة الحاسوب أو الهواتف الذكية أو غيرها من الوسائط الرقمية أو تلك المتبادلة عبر شبكة الإنترنت والتي تُعد الأكثر عرضةً للهجمات الإلكترونية؛ ويُطلق على الجرائم التي تستهدف هذه البيانات

---

[1] المادة رقم (28) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] المادة رقم (3) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

تسميات مثل" جرائم تشفير المعلومات "أو الاختراق نظرًا لتركيزها على استغلال الثغرات في الأنظمة الرقمية لسرقة أو العبث بالبيانات الحساسة.[1]

الفرع الثاني- جريمة الاعتداء على البرامج والنظم المعلوماتية:

شهدت برامج تقنية المعلومات تطوراً هائلاً على المستويين التقني والوظيفي، حيث امتد هذا التطور ليشمل أساليب عمل البرامج الحاسوبية والأجهزة الذكية، مما أسهم في تحقيق عوائد اقتصادية كبيرة للعديد من القطاعات، ومع هذا التسارع التقني وما رافقه من تطور في المكونات التكنولوجية برزت مخاطر متزايدة للاعتداءات الإلكترونية، وفي هذا السياق سنتناول في هذا الفرع أربعة محاور رئيسية: أولاً مفهوم البرنامج المعلوماتي، ثانياً محل الجريمة المعلوماتية، وثالثاً أركان الجريمة المعلوماتية، رابعًا عقوبة جريمة الاعتداء على البرامج المعلوماتية.

أولاً – مفهوم البرنامج المعلوماتي:

تقنية المعلومات تشير إلى الاستخدام المنهجي والمنظم للحوسبة والإلكترونيات وشبكات الاتصالات بهدف معالجة البيانات والمعلومات وتخزينها واسترجاعها ونقلها وتوزيعها بأشكالها المتنوعة سواء كانت نصوصًا أو صورًا أو أصواتًا أو مقاطع فيديو أو غيرها من الصيغ الرقمية وذلك لتسهيل الوصول إلى المعرفة وتحسين كفاءة العمليات المختلفة في شتى المجالات[2]، و البرنامج المعلوماتي يمثل مجموعة منظمة من البيانات

---

[1] رجاء عايد الخلايلة، المسؤولية التقصيرية الالكترونية "دراسة مقارنة"، درا الثقافة لنشر والتوزيع، 2011، ص 100 وما يليها.

[2] المادة رقم (1/ ب) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

والأوامر التي يمكن للحواسيب والأجهزة الذكية القائمة على تقنية المعلومات تنفيذها وقد صُممت هذه المجموعة من التعليمات بشكل محدد لتحقيق وظيفة أو مجموعة من الوظائف المعينة بدءًا من العمليات البسيطة وصولًا إلى المهام المعقدة والمتشعبة في مختلف التطبيقات والمجالات[1].

كما كفل المشرع العماني حماية للبرامج المعلوماتية بموجب قانون مكافحة جرائم تقنية المعلومات من خلال تجريم الأفعال التي تمثل اعتداءً عليها؛ فالمادة (9) من قانون مكافحة جرائم تقنية المعلومات تعاقب بالسجن والغرامة كل من أدخل عمدًا ودون وجه حق في نظام معلوماتي أو شبكة معلوماتية أو وسائل تقنية المعلومات ما من شأنه إيقاف أي منها أو تعطيله عن العمل، أو ألغى أو غير أو عدل أو شوه أو أتلف أو دمر البرامج المستخدمة أو المخزنة في أي منها مع علمه بذلك[2].

بالإضافة إلى ذلك فإن المادة (11) من قانون مكافحة جرائم تقنية المعلومات تجرم إنتاج أو بيع أو توزيع أو حيازة برامج مصممة لارتكاب جرائم تقنية المعلومات، مما يشمل البرامج الضارة التي قد تستخدم في إتلاف أو تعطيل البرامج المعلوماتية المشروعة، [3]،وبذلك يوفر القانون حماية جنائية للبرامج المعلوماتية ضد مختلف أشكال الاعتداء التي قد تؤدي إلى الإضرار بها أو تعطيلها أو استخدامها في أغراض غير قانونية[4].

وبالنظر إلى قانون حماية البيانات الشخصية العماني (المرسوم السلطاني رقم 6 / 2022) نجد أن المشرع كفل حماية غير مباشرة للبرامج المعلوماتية من خلال تركيزه الأساسي على حماية البيانات الشخصية

---

(1) المادة رقم (1/ ط) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

(2) المادة رقم (9) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

(3) المادة رقم (13) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

(4) المادة رقم (11) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

التي تتم معالجتها باستخدام هذه البرامج، فعلى سبيل المثال المادة(13) تنص على" أن يلتزم المتحكم بوضع الضوابط والإجراءات الواجب الالتزام بها عند معالجة البيانات الشخصية ويجب أن تشتمل على وجه الخصوص الآتي:أ – تحديد المخاطر التي قد تقع على صاحب البيانات الشخصية جراء المعالجة، ب – إجراءات وضوابط نقل وتحويل البيانات الشخصية، ج – التدابير الفنية والإجرائية لضمان تنفيذ المعالجة وفقا لأحكام هذا القانون، د – أي ضوابط أو إجراءات أخرى تحددها اللائحة"[1]، أيضًا المادة (19) تنص على أن "يلتزم المتحكم عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات الشخصية عن الاختراق وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة"[2]، تنظم المواد (14–22) إطاراً قانونياً متكاملاً لمعالجة البيانات الشخصية يلزم المتحكمين بالإفصاح الشفاف عن عمليات المعالجة وحماية حقوق الأفراد وضمان السرية، والامتثال للضوابط الرقابية والإبلاغ الفوري عن أي اختراقات مع تعيين مسؤول حماية البيانات والحصول على الموافقات المسبقة كل ذلك وفقاً للضوابط والإجراءات التي تحددها اللائحة التنفيذية[3].

ومن وجهة نظر الباحث بالرغم من أن القانون لا يتناول بشكل مباشر حماية البرامج المعلوماتية ككيانات مستقلة، إلا أن حماية البيانات الشخصية التي تعتمد عليها في المعالجة توفر مظلة حماية غير مباشرة لهذه البرامج من خلال إلزام الأطراف المعنية باتخاذ التدابير اللازمة لضمان سلامة وسرية المعالجة، وأيضًا لم يتطرق المشرع إلى مسألة النسخ بالطرق غير الشرعية بدون موافقة المالك أو الوكيل المختص.

---

[1] المادة رقم (13) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (19) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[3] المواد أرقام (14: 22) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

ثانياً– محل الجريمة المعلوماتية:

بناء على ما سبق إيضاحه يتمثل محل الجريمة المعلوماتية هنا في البرامج المعلوماتية التقنية " كما سبق تعريفها قانونيًا" حيث تُعد هذه البرامج (سواء كانت أنظمة تشغيل أو برامج تطبيقية أو نصوصًا برمجية) ذات قيمة مالية معنوية باعتبارها أصولًا غير ملموسة قابلة للتقييم الاقتصادي والقانوني، وقد اعترف المشرع بهذه القيمة المعنوية للبرمجيات وأهليتها لأن تكون محلاً للحماية القانونية فسوّغ لها الحماية الجزائية والمدنية ذاتها التي يُقررها القانون للأموال المادية التقليدية، وذلك انطلاقًا من اعتبارها مالاً مُقوّمًا"بالمعنى الاصطلاحي القانوني " لما تُحققه من منافع اقتصادية ولما تتطلبه من استثمارات في تطويرها وصيانتها.

استنادًا إلى قانون مكافحة جرائم تقنية المعلومات وقانون حماية البيانات يمكن تحديد المواد القانونية التي تتناول محل الجريمة المعلوماتية على النحو التالي:

في قانون مكافحة جرائم تقنية المعلومات تتعدد المواد التي تحدد وتحمي العناصر التي يمكن أن تكون محلًا للجريمة المعلوماتية فالمادة (3) تجرم الدخول غير المصرح به إلى المواقع الإلكترونية والنظم المعلوماتية ووسائل تقنية المعلومات أو تجاوز الدخول المصرح به أو الاستمرار فيه، كما تجرم الأفعال التي تترتب عليها آثار سلبية على البيانات والمعلومات الإلكترونية المخزنة أو على النظام أو الوسائل أو الشبكة المعلوماتية نفسها[1]، وتشدد العقوبة إذا كانت البيانات شخصية أو إذا ارتكبت الجريمة أثناء أو بمناسبة تأدية العمل وذلك وفقا لنص المادة 4 من القانون سالف الذكر، كما تحظر المادة (5) تغيير أو تعديل أو إتلاف البيانات والمعلومات الإلكترونية الطبية عمدًا ودون وجه حق، وتولي المادة (6) اهتمامًا خاصًا بالبيانات والمعلومات

[1] المادة رقم (11) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

الإلكترونية الحكومية والخاصة بالمصارف والمؤسسات المالية مجرمة الدخول إليها بقصد الحصول عليها إذا كانت سرية وتشديد العقوبة في حال العبث بها، وتجرم المادة (7) الدخول غير المصرح به إلى المواقع الإلكترونية بقصد تغيير تصميمها أو إتلافها أو شغل عنوانها، كما تحظر المادة (8) اعتراض خط سير البيانات أو المعلومات الإلكترونية أو قطع بثها أو التنصت عليها، وتعتبر المادة (9) إدخال ما من شأنه إيقاف أو تعطيل النظم أو الشبكات أو الوسائل أو إتلاف البرامج والبيانات جريمة معلوماتية، وتجرم المادة (10) إعاقة أو تعطيل الوصول إلى خدمات مزود الخدمة أو النظم أو الوسائل.

أما في قانون حماية البيانات الشخصية، فإن التركيز ينصب على حماية البيانات الشخصية تحديدًا فالمادة (4)تنص على أن" تعد البيانات الشخصية محمية بموجب أحكام هذا القانون"[1]، و المادة (5) "تحظر معالجة البيانات الشخصية التي تتعلق بالبيانات الجينية أو البيانات الحيوية أو البيانات الصحية أو الأصول العرقية أو الحياة الجنسية أو الآراء السياسية أو الدينية أو المعتقدات أو الإدانة الجزائية أو المتعلقة بتدابير أمنية إلا بعد الحصول على تصريح بذلك من الوزارة، وفقا للضوابط والإجراءات التي تحددها اللائحة"، كما تحظر المادة (6) "يحظر معالجة البيانات الشخصية للطفل إلا بموافقة ولي أمره، ما لم تكن تلك المعالجة لمصلحة الطفل الفضلى، وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة"، وتلزم المواد من (13) إلى (22) المتحكم والمعالج باتخاذ تدابير لحماية البيانات الشخصية وضمان سريتها وعدم نشرها إلا بموافقة أصحابها، كما تلزمهم المادة (19) "يلتزم المتحكم عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات

[1] المادة رقم (4) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

الشخصية عن الاختراق وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة"، وتنص المواد من (25) إلى (29) على عقوبات لمخالفة هذه الأحكام المتعلقة بحماية البيانات الشخصية.

من وجهة نظر الباحث بناء على ماسبق إيضاحه يكفل المشرع العماني حماية لمحل الجريمة المعلوماتية الذي يشمل البيانات والمعلومات الإلكترونية بأنواعها والنظم المعلوماتية ووسائل تقنية المعلومات والشبكات والمواقع والبرامج والبطاقات المالية الإلكترونية وذلك من خلال تجريم مختلف أشكال الاعتداء عليها في قانون مكافحة جرائم تقنية المعلومات بالإضافة إلى توفير حماية خاصة للبيانات الشخصية التي تتم معالجتها عبر هذه الوسائل والأنظمة في قانون حماية البيانات الشخصية.

ثالثاً- أركان الجريمة المعلوماتية:

استنادًا إلى قانون مكافحة جرائم تقنية المعلومات (المرسوم السلطاني رقم 12 / 2011) وقانون حماية البيانات الشخصية (المرسوم السلطاني رقم 6 / 2022)، يمكن تحديد أركان الجريمة المعلوماتية على النحو التالي:

1- الركن المادي:

يتكون الركن المادي للجريمة المعلوماتية من الفعل أو الامتناع الذي ينهى عنه القانون والنتيجة الجرمية المترتبة عليه، وعلاقة السببية بين الفعل والنتيجة، و في الجرائم المعلوماتية تبعًا لطبيعة الجريمة فقد يكون فعلًا إيجابيًا كالدخول غير المصرح به إلى نظام معلوماتي (المادة 3)، أو إدخال برامج ضارة (المادة 9)، أو تغيير بيانات إلكترونية (المادة 5، 12)، أو نشر محتوى غير قانوني عبر الشبكة (المواد 14: 27)، أو استخدام

بطاقة مالية مزورة (المادة 28)، أما النتيجة الجُرمية فهي الأثر الذي يترتب على الفعل أو الامتناع مثل إلغاء أو تغيير أو إتلاف البيانات (المادة 3)، أو تحقيق منفعة غير مشروعة (المادة 12، 13) أو المساس بحرمة الحياة الخاصة (المادة 16)، أو وقوع ضرر على صاحب البيانات الشخصية (المادة 23 من قانون حماية البيانات الشخصية) ويجب أن تكون هناك علاقة سببية مباشرة بين الفعل المرتكب والنتيجة الجرمية المتحققة.

من وجهة نظر الباحث بناء على ما سبق إيضاحه من مواد قانونية توضح الركن المادي للجريمة المعلوماتية في التشريع العُماني يتحقق الركن المادي في جرائم الاعتداء على البرامج المعلوماتية من خلال ثلاثة عناصر أساسية:

أ- السلوك الإجرامي الذي يتمثل في أي فعل غير مشروع كالنسخ غير المرخص أو الإتلاف أو التعديل غير المصرح به للبرامج دون موافقة مالكها الشرعي، مع ضرورة تنفيذ هذا السلوك عبر الوسائل الإلكترونية.

ب- النتيجة الجرمية المتمثلة في الضرر الحاصل سواء كان ذلك بانتقاص قيمة البرنامج أو انتهاك حقوق مالكه وقد يكون هذا الضرر خاصاً يصيب فرداً أو شركة معينة أو عاماً يؤثر على مصالح جماعية أو وطنية.

ج- العلاقة السببية الوثيقة بين السلوك والنتيجة حيث يجب أن تنتج الأفعال غير المشروعة الضرر المباشر للبرنامج أو لحقوق مالكه كأن يؤدي النسخ غير القانوني إلى خسائر مادية أو معنوية للمالك الأصلي، وتجدر الإشارة إلى أن هذه الأفعال قد ترتكب بدوافع مختلفة كالربح الشخصي أو الإضرار بالآخرين أو حتى مجرد العبث مع ضرورة تحقق العناصر الثلاثة معاً لقيام الركن المادي الكامل للجريمة.

2- الركن المعنوي:

يتكون الركن المعنوي للجريمة المعلوماتية من القصد الجنائي أو الخطأ غير العمدي وذلك حسب طبيعة الجريمة المنصوص عليها في القانون في معظم الجرائم المعلوماتية المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات[1]، يتطلب القانون توافر القصد الجنائي أي اتجاه إرادة الجاني الواعية إلى ارتكاب الفعل المجرم مع العلم بالعناصر المكونة للجريمة ويتضح القصد الجنائي في العديد من المواد باستخدام عبارات مثل "عمدًا ودون وجه حق" (المادة 3، 5، 6، 7، 8، 9، 13) أو "بقصد" (المادة 6، 11، 12، 13، 14، 18، 20، 22، 23، 27، 28)، أما في قانون حماية البيانات الشخصية[2]، فقد تتطلب بعض المخالفات مجرد الخطأ غير العمدي أو الإهمال في اتخاذ التدابير اللازمة لحماية البيانات الشخصية وإن كانت معظم العقوبات المنصوص عليها تبدو مرتبطة بفعل متعمد أو إهمال جسيم (المادة 30).

رابعًا-عقوبة جريمة الاعتداء على البرامج المعلوماتية:

تعد جرائم الاعتداء على البرامج المعلوماتية من أبرز التحديات التي تواجه صناعة التكنولوجيا في العصر الرقمي حيث تشير الإحصائيات إلى أن عمليات النسخ غير القانونية للبرامج وتتنوع أشكال هذه الجرائم بين القرصنة المباشرة للبرامج وتحميلها غير المشروع على أجهزة الحاسوب أو وحدات التخزين سواء من خلال النسخ الحرفي الكلي أو الجزئي للبرنامج أو النسخ غير الحرفي الذي يعتمد على استغلال الأفكار الأساسية للبرنامج الأصلي، وتتم هذه الانتهاكات عادة دون الحصول على ترخيص من المالك الشرعي أو الجهة

---

[1] قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

المختصة؛ مما يشكل اعتداءً صارخًا على حقوق الملكية الفكرية ويؤدي إلى أضرار اقتصادية كبيرة لمطوري البرامج وشركات التكنولوجيا[1]، وحرصًا على التصدي لجريمة الاعتداء على البرامج المعلوماتية أولى المشرع العُماني اهتمامًا خاصًا بهذا الأمر وسعى إلى وضع عقوبات رادعة وهو ما يتضح في قانون مكافحة جرائم تقنية المعلومات (المرسوم السلطاني رقم 12 / 2011) حيث يمكن تتبع هذه العقوبات من خلال المواد القانونية التالية.

المادة (3) تعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمدًا ودون وجه حق موقعًا إلكترونيًا أو نظامًا معلوماتيًا أو وسائل تقنية المعلومات أو جزءًا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك وتشدد الفقرة الثانية من نفس المادة العقوبة إلى السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين إذا ترتب على هذا الدخول إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير البرامج المستخدمة أو المخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات.

كما أن المادة (9) تعتبر أكثر تحديدًا في تجريم الاعتداء المباشر على البرامج المعلوماتية حيث تعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني أو بإحدى هاتين العقوبتين كل من أدخل عمدًا ودون وجه حق في نظام معلوماتي أو شبكة معلوماتية أو وسائل تقنية المعلومات ما من شأنه إيقاف أي منها أو تعطيله عن العمل أو ألغى أو

---

[1] عايد رجاء الخلايله، المسؤلية التقصيرية الإلكترونية "المسؤلية الناشئة عن إساءة استخدام اجهزة الحاسوب والانترنت"، دراسة مقارنة، دار الثقافة للنشر والتوزيع، 2011، ص 101.

غير أو عدل أو شوه أو أتلف أو دمر البرامج المستخدمة أو المخزنة في أي منها مع علمه بأن ذلك من شأنه إيقافها أو تعطيلها عن العمل وذلك باستخدام وسائل تقنية المعلومات، و هذه المادة تجرم بشكل واضح العبث بالبرامج سواء بالإيقاف أو التعطيل أو الإلغاء أو التغيير أو التشويه أو الإتلاف أو التدمير المتعمد.

بالإضافة إلى ذلك فإن المادة (13) المتعلقة بالاحتيال المعلوماتي قد تنطبق على بعض صور الاعتداء على البرامج المعلوماتية إذا كان الهدف من التلاعب بها هو التحايل والتسبب في إلحاق الضرر بالمستفيدين أو المستخدمين لتحقيق مصلحة غير مشروعة، حيث تعاقب بالسجن والغرامة على إدخال أو تعديل أو تغيير أو إتلاف أو تشويه أو إلغاء بيانات أو معلومات إلكترونية في نظام معلوماتي أو التدخل في وظائفه أو أنظمة تشغيله أو تعطيل البرامج عمدًا ودون وجه حق لهذا الغرض.

من وجهة نظر الباحث بناء على ماسبق إيضاحه فإن قانون مكافحة جرائم تقنية المعلومات يوفر حماية جنائية للبرامج المعلوماتية من خلال تجريم أفعال الدخول غير المصرح به الذي يؤدي إلى العبث بها، وكذلك تجريم التدمير أو الإتلاف أو التعطيل المتعمد لها بالإضافة إلى تجريم التلاعب بها لغرض الاحتيال وإلحاق الضرر بالآخرين، مع اختلاف العقوبات المقررة تبعًا لخطورة الفعل والضرر الناتج عنه والقصد الجنائي للمرتكب.

المطلب الثاني: جرائم انتهاك البيانات الشخصية الواقعة بواسطة استغلال الاتصالات المعلوماتية

أدت التطورات الهائلة في وسائل الاتصال الحديثة القائمة على الاتصالات البعدية، وإمكانية التواصل اللامحدود بين أطراف متعددة، بالإضافة إلى القدرة على التخفي خلف هويات مصطنعة؛ إلى توفير بيئة خصبة للجناة للانخراط في عالم الإجرام والشر، وقد عززت هذه الإمكانيات التقنية العالية قدرتهم على تنفيذ الأفعال الإجرامية وإخفاء هوياتهم الحقيقية إلى حد كبير، و لقد فتحت شبكة الاتصالات العالمية (الإنترنت) آفاقًا جديدة لأنماط إجرامية قد تتفق في غاياتها مع الجرائم التقليدية لكنها تتميز بأسلوب تنفيذ أكثر سهولة وتأثيرًا أوسع، مع صعوبة متزايدة في اكتشاف الفعل وتحديد هوية مرتكبه وقد امتد نطاق الإجرام باستغلال الاتصالات المعلوماتية ليشمل الاعتداء على الآخرين نظرًا لسهولة ارتكاب هذا النوع المستحدث من الجرائم باستخدام الوسائل التقنية المتاحة؛ لذلك سنتناول في هذا المطلب فرعين:

الفرع الأول– الأبعاد القانونية للتهديد في الفضاء الرقمي.

الفرع الثاني– الأبعاد القانونية للتجسس في الفضاء الرقمي.

الفرع الأول- الأبعاد القانونية للتهديد في الفضاء الرقمي:

يمكن تناول الأبعاد القانونية للتهديد في الفضاء الرقمي من زاوية حماية البيانات الشخصية والحقوق المتعلقة بها على الرغم من أن هذا القانون لا يتناول جريمة التهديد بشكل مباشر كجريمة قائمة بذاتها، إلا أنه يضع إطارًا قانونيًا يحمي الأفراد من التهديدات التي قد تستغل بياناتهم الشخصية أو تنتهك حقوقهم في هذا الفضاء.

وأحد الأبعاد القانونية الهامة يتمثل في حماية سرية البيانات الشخصية فالمادة (21) من قانون حماية البيانات الشخصية تنص على أن " يلتزم المتحكم بضمان سرية البيانات الشخصية، وعدم نشرها إلا بموافقة مسبقة من صاحب البيانات الشخصية، وذلك على النحو الذي تحدده اللائحة"[1]، وبُعد آخر يتمثل في الحق في إلغاء الموافقة وسحبها فالمادة (11/أ) تنص على "يكون لصاحب البيانات الشخصية الحق في الآتي: أ – إلغاء موافقته على معالجة بياناته الشخصية، وذلك مع عدم الإخلال بالمعالجات التي تمت قبل الإلغاء..."[2].

كما أن الحق في الإخطار بالاختراق والانتهاك المادة (11/و) والمادة (19) يمثل بعدًا قانونيًا هامًا؛ فأي تهديد بشن هجوم إلكتروني يؤدي إلى اختراق البيانات الشخصية أو انتهاكها يستوجب على المتحكم إبلاغ الوزارة وصاحب البيانات وعدم القيام بذلك يعرضه للمساءلة، هذا البعد يهدف إلى تمكين الأفراد من اتخاذ الاحتياطات اللازمة عند وجود تهديد لبياناتهم[3].

---

[1] المادة رقم (21) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (11/أ) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[3] المادتين رقم (11، 19) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

بالإضافة إلى ذلك فإن مبدأ الشفافية والأمانة في المعالجة (المادة 10) "لا يجوز معالجة البيانات الشخصية إلا في إطار الشفافية والأمانة، واحترام كرامة الإنسان، وبعد الموافقة الصريحة لصاحب البيانات الشخصية على ذلك، ويجب أن يكون طلب معالجة البيانات الشخصية مكتوبا وبصورة واضحة وصريحة ومفهومة، ويلتزم المتحكم بإثبات الموافقة الكتابية لصاحب البيانات الشخصية لمعالجة بياناته"[1].

من وجهة نظر الباحث على الرغم من أن قانون حماية البيانات الشخصية لا يعرف جريمة التهديد بشكل مباشر؛ إلا أنه يوفر إطارًا قانونيًا لحماية الأفراد من التهديدات التي تستغل بياناتهم الشخصية أو تنتهك حقوقهم الرقمية، ويفرض التزامات على المتحكمين والمعالجين تهدف إلى منع وقوع مثل هذه التهديدات والتصدي لآثارها حال وقوعها.

كما يُجرم المشرع العُماني جرائم التهديد والابتزاز الإلكتروني عبر مختلف وسائل الاتصال، حيث نص قانون الجزاء العماني على عقوبات رادعة لهذه الجرائم ففي المادة (266) من القانون الجزائي العُماني يُعاقب بالحبس من سنة إلى ثلاث سنوات وغرامة تصل إلى خمسمائة ريال لكل من يمارس التهديد أو الابتزاز عبر الوسائل الإلكترونية[2]، بينما تناولت المادة (267) حالات التهديد البسيط بعقوبة تتراوح بين عشرة أيام وستة أشهر حبساً[3]، وأما المادة (268) فقد جرمت نشر الفيروسات أو البرمجيات الضارة وعاقبت عليها بغرامات مالية كما حظرت المادة (287) الحصول على أموال أو منافع بطريقة غير مشروعة عبر هذه الوسائل وفرضت

---

[1] المادة رقم (10) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (266) من القانون الجزائي العُماني الصادر بالمرسوم السلطاني رقم 7 / 1974.

[3] المادة رقم (267) من القانون الجزائي العُماني الصادر بالمرسوم السلطاني رقم 7 / 1974.

عقوبة تصل إلى ثلاث سنوات سجن وغرامة خمسمائة ريال، مما يعكس حرص المشرع على مواكبة التحديات الأمنية الناشئة عن التطور التقني[1].

كما وسع المشرع العُماني نطاق التجريم ليشمل أفعال التهديد والابتزاز عبر الإنترنت والتي يمكن ارتكابها باستخدام أي وسيلة من وسائل الاتصال التقنية، حيث نصت المادة (18) من قانون مكافحة جرائم تقنية المعلومات على عقوبة السجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين لكل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في تهديد شخص أو ابتزازه لحمله على فعل أو امتناع ولو كان هذا الفعل أو الامتناع مشروعًا، وتشدد العقوبة لتصل إلى السجن المؤقت مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني إذا كان التهديد بارتكاب جناية أو بإسناد أمور مخلة بالشرف أو الاعتبار[2].

على الرغم من عدم وجود تعريف تشريعي محدد للتهديد أو الابتزاز في القانون العماني إلا أنه يمكن فهمهما بأنهما بث الخوف أو الوعيد بإلحاق ضرر بشخص ما أو بمن يرتبط بهم أو بممتلكاتهم مما يشكل ضغطًا على إرادتهم، ويتضمن ذلك إنذار شخص بوقوع خطر عليه أو على ماله أو على شخص أو مال يخص غيره سواء كان هذا الإنذار شفويًا أو كتابيًا أو بأي وسيلة تهدف إلى إلقاء الرعب أو الإزعاج أو التخويف في نفس المجني عليه من خطر يهدده أو يهدد ما يهمه أمره، أما بالنسبة لمحل جريمة التهديد عبر وسائل الاتصال الحديثة فإن التهديد بأي صورة أو وسيلة يصلح أن يكون محلًا للجريمة كما أكدت عليه النصوص

---

[1] المادة رقم (287) من القانون الجزائي العُماني الصادر بالمرسوم السلطاني رقم 7 / 1974.

[2] المادة رقم (18) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم 12 / 2011.

القانونية العمانية سالفة الذكر سواء كان موجهًا مباشرة إلى المجني عليه أو إلى أسرته أو ممتلكاته أو إلى أي شخص أو شيء له به مصلحة ويمكن أن يقع التهديد عبر وسائل الاتصال الحديثة بأشكال متنوعة سواء كانت رسائل نصية أو منشورات على وسائل التواصل الاجتماعي أو رسائل بريد إلكتروني أو غيرها من الوسائل الرقمية[1].

ومن أبرز التطبيقات العملية لهذا النوع من الجرائم في السلطنة قضية مواطن قام بإرسال رسائل عبر تطبيق الواتساب تتضمن سباً وتهديداً لزوجين عمانيين حيث قضت المحكمة حضورياً بإدانته بجريمتين: الأولى جنحة التعدي بالسب والقذف المنصوص عليها في المادة (16) من قانون مكافحة جرائم تقنية المعلومات، والثانية جنحة الإضرار بالغير وفقاً للمادة (18) من ذات القانون وقد أصدرت المحكمة حكماً يقضي بعقوبة سجن سنة عن الجريمة الأولى وشهر سجن عن الجريمة الثانية، بالإضافة إلى غرامة ألف ريال عماني مع دمج العقوبتين وتنفيذهما معاً، كما ألزمت المحكمة المتهم بدفع تعويض مدني للمجني عليهما قدره مائتا ريال عماني مما يعكس توازن القانون بين العقوبة الجزائية والتعويض المدني لضمان حقوق الضحايا[2].

الفرع الثاني– الأبعاد القانونية للتجسس في الفضاء الرقمي:

يشكل التجسس في الفضاء الرقمي تحديًا قانونيًا معقدًا نظرًا لطبيعته العابرة للحدود وتطوره المستمر لذلك سنوضح في هذا الفرع تفصيلًا للأبعاد القانونية المتعلقة بالتجسس في الفضاء الرقمي وذلك من خلال

---

[1] محمد عبيد الكعبي، المرجع السابق، ص 102.

[2] القضية رقم (392/ق/ 2014 / المحكمة الجزائية بالمحكمة الجماعية السيب)، تاريخ جلسة الحكم 2014/01/15 كذلك هناك قضايا تزوير عبر وسائل التواصل التقنية المختلفة في العالم، أيمن عبد الله فكري، جرائم نظم المعلومات "دراسة مقارنة"، دار الجامعة الجديدة للنشر والتوزيع، 2007، ص 82

أولًا: تجريم الوصول غير المصرح به للبيانات والمعلومات، ثانيًا تجريم اعتراض الاتصالات والمراقبة غير المشروعة، ثالثًا تجريم استخدام أدوات وبرامج التجسس، رابعًا حماية حرمة الحياة الخاصة في الفضاء الرقمي، خامسًا الالتزامات بحماية البيانات والإبلاغ عن الاختراقات، سادسًا المسؤولية الجنائية العامة في قانون الجزاء ودورها في مكافحة التجسس الرقمي.

أولًا: تجريم الوصول غير المصرح به للبيانات والمعلومات:

قانون مكافحة جرائم تقنية المعلومات المادة رقم (6): يجرم بشكل صريح الدخول العمدي وغير المصرح به إلى المواقع الإلكترونية أو النظم المعلوماتية بهدف الحصول على بيانات أو معلومات إلكترونية حكومية سرية أو سرية بموجب تعليمات وتشدد العقوبة في حال تم نسخ أو نشر أو إتلاف هذه البيانات[1].

قانون مكافحة جرائم تقنية المعلومات المادة (3): يجرم الدخول العمدي وغير المصرح به إلى المواقع الإلكترونية أو النظم المعلوماتية أو وسائل تقنية المعلومات وتشدد العقوبة إذا ترتب على ذلك إلغاء أو تغيير أو إتلاف أو نسخ أو نشر بيانات أو معلومات إلكترونية وتزداد العقوبة إذا كانت البيانات شخصية[2].

قانون حماية البيانات الشخصية المادة (21) تنص على "يلتزم المتحكم بضمان سرية البيانات الشخصية، وعدم نشرها إلا بموافقة مسبقة من صاحب البيانات الشخصية، وذلك على النحو الذي تحدده اللائحة"[3].

---

[1] المادة رقم (6) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] المادة رقم (3) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[3] المادة رقم (21) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

ثانيًا: تجريم اعتراض الاتصالات والمراقبة غير المشروعة:

قانون مكافحة جرائم تقنية المعلومات المادة (8): يجرم اعتراض خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو التنصت عليها عمدًا ودون وجه حق[1] ، وكذلك المادة (332) من القانون الجزائي العماني.

ثالثًا: تجريم استخدام أدوات وبرامج التجسس:

قانون مكافحة جرائم تقنية المعلومات المادة (11): يعاقب على إنتاج أو بيع أو شراء أو حيازة برامج أو أدوات أو أجهزة مصممة أو مكيفة لارتكاب جرائم تقنية المعلومات، بما في ذلك تلك التي تستخدم في التجسس، وذلك بقصد استخدامها في هذه الجرائم[2].

رابعًا: حماية حرمة الحياة الخاصة في الفضاء الرقمي:

قانون مكافحة جرائم تقنية المعلومات المادة (16): يجرم استخدام وسائل تقنية المعلومات في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد بالتقاط صور أو نشر أخبار أو تسجيلات صوتية أو مرئية تتصل بها ولو كانت صحيحة، وذلك دون رضا أصحابها[3]، وكذلك المادة (332) من القانون الجزائي العماني.

---

[1] المادة رقم (8) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] المادة رقم (11) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[3] المادة رقم (16) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

خامسًا: الالتزامات بحماية البيانات والإبلاغ عن الاختراقات:

قانون حماية البيانات الشخصية المادة (19)[1]، ولائحته التنفيذية المادتان (30 و32): يلزم المتحكم بالإبلاغ عن أي اختراق للبيانات الشخصية يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية سواء للوزارة أو لصاحب البيانات، خلال مدة محددة. وأي فعل تجسس ناجح يستتبع هذا الالتزام بالإبلاغ[2].

قانون حماية البيانات الشخصية المادة (13) ولائحته التنفيذية المادة (26) يلزم المتحكم بوضع الضوابط والإجراءات والتدابير الفنية والإجرائية لضمان حماية البيانات الشخصية من الوصول غير المصرح به، وأي ضعف في هذه التدابير يستغله طرف ثالث للتجسس قد يعرض المتحكم للمساءلة.

سادسًا: المسؤولية الجنائية العامة في قانون الجزاء ودورها في مكافحة التجسس الرقمي:

على الرغم من أن قانون مكافحة جرائم تقنية المعلومات يتناول بشكل مباشر العديد من الأفعال التي تشكل جوهر التجسس الرقمي يظل قانون الجزاء (المرسوم السلطاني رقم 7/ 2018) يمثل الإطار القانوني العام الذي يمكن أن يمتد تأثيره ليشمل بعض جوانب هذه الجرائم وذلك من خلال مبادئه وأحكامه العامة في التجريم والعقاب وسريان القانون.

---

[1] المادة رقم (19) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادتين رقم (30، 32) من اللائحة التنفيذية لقانون حماية البيانات الشخصية وزارة النقل والاتصالات وتقنية المعلومات" قرار وزاري رقم 34 / 2024.

1- مبدأ الإقليمية وتجاوز الحدود الرقمية:

تنص المادة (15) من قانون الجزاء على سريان أحكامه على أي جريمة ترتكب في إقليم سلطنة عمان ويشمل ذلك الأراضي والمياه الإقليمية وما يعلوهما من فضاء جوي بالإضافة إلى الجرائم التي تقع على متن السفن والطائرات العمانية والأهم في سياق الجرائم الرقمية تعتبر الجريمة مرتكبة في الدولة إذا وقع فيها أي فعل من الأفعال المكونة لها أو إذا تحققت نتيجتها فيها، أو حتى إذا كان يُراد لها أن تتحقق داخل الإقليم و هذا المبدأ ذو أهمية بالغة في ملاحقة أفعال التجسس الرقمي التي قد تبدأ خارج حدود السلطنة ولكن تستهدف أنظمة أو بيانات موجودة داخلها أو تلك التي تنطلق من داخل السلطنة وتؤثر على أهداف خارجية[1].

2- مفهوم العلانية في الفضاء الرقمي:

تُعرّف المادة (9) من قانون الجزاء مفهوم العلانية بشكل موسع ليشمل ليس فقط الأقوال والأفعال التي تتم في الأماكن المادية العامة بل أيضًا تلك التي يتم نقلها أو عرضها بأي وسيلة في جمع أو مكان عام أو مكان متاح للجمهور ويشمل هذا التعريف بوضوح النشر عبر الإنترنت ووسائل التواصل الاجتماعي المختلفة؛ وبالتالي فإن أي فعل تجسس رقمي يتضمن نشر معلومات تم الحصول عليها بطريقة غير مشروعة عبر هذه الوسائل يعتبر فعلاً علنيًا ويخضع لأحكام قانون الجزاء المتعلقة بالجرائم التي ترتكب علانية مثل التشهير أو نشر الأسرار[2].

---

[1] المادة رقم (15) من القانون الجزائي العُماني الصادر بالمرسوم السلطاني رقم 7 / 2018.

[2] المادة رقم (9) من القانون الجزائي العُماني الصادر بالمرسوم السلطاني رقم 7 / 2018.

3- المسؤولية عن التحريض والاتفاق والمساعدة في الجرائم الرقمية:

تحدد المواد (38) و (39) من قانون الجزاء مسؤولية الشركاء في الجريمة بمن فيهم المحرضون والمتفقون والمساعدون ويمكن تطبيق هذه الأحكام على جرائم التجسس الرقمي، حيث قد يتم التحريض على ارتكابها أو الاتفاق على تنفيذها أو تقديم المساعدة التقنية أو المعلوماتية لتسهيلها عبر وسائل الاتصال الرقمي؛ وبالتالي فإن الأشخاص الذين يلعبون دورًا في التخطيط أو التنفيذ غير المباشر لعمليات التجسس الرقمي قد يخضعون للمساءلة الجنائية بموجب هذه المواد[1].

من وجهة نظر الباحث بناء على ما سبق إيضاحه يتضح أن الأبعاد القانونية لمكافحة التجسس في الفضاء الرقمي في سلطنة عمان لا تقتصر على قانون مكافحة جرائم تقنية المعلومات وقانون حماية البيانات الشخصية ولائحته التنفيذية فحسب؛ بل تمتد لتشمل المبادئ العامة والقواعد المنصوص عليها في قانون الجزاء فقانون مكافحة جرائم تقنية المعلومات يستهدف بشكل خاص الأفعال التي تستغل طبيعة التقنيات الرقمية في التجسس والاعتداء على البيانات والنظم، بينما يركز قانون حماية البيانات الشخصية على حماية البيانات وتنظيم معالجتها والإبلاغ عن اختراقاتها في هذا السياق، و يكمل قانون الجزاء هذا الإطار بتوفير قواعد عامة تتعلق بسريان القانون ومفهوم العلانية والمسؤولية الجنائية عن المساهمة في الجريمة مما يوسع نطاق التجريم ليشمل جوانب أخرى من أفعال التجسس الرقمي التي قد لا يغطيها القانون الخاص بشكل مباشر و هذا التكامل

[1] المادتين رقم (38، 39) من القانون الجزائي العُماني الصادر بالمرسوم السلطاني رقم 7 / 2018.

بين الأطر القانونية المختلفة يعزز قدرة سلطنة عمان على مواجهة التحديات المتزايدة التي تفرضها جرائم الفضاء الرقمي بما فيها التجسس.

المبحث الثاني: المسؤولية الجزائية عن انتهاك البيانات الشخصية

تؤسس المادة (24) من قانون حماية البيانات الشخصية العُماني لركيزة أساسية في تحديد نطاق المسؤولية الجنائية وتوقيع الجزاءات المستحقة على الأفعال التي يجرمها حيث تنص صراحة على أنه " مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون الجزاء أو أي قانون آخر، يعاقب على الجرائم المبينة في هذا القانون بالعقوبات المنصوص عليها فيه"[1].

بيد أن هذه القاعدة العامة تخضع لاستثناء ذي أهمية بالغة و يتمثل في أنه إذا وجد قانون آخر نافذ وساري المفعول في الدولة سواء أكان ذلك القانون هو قانون الجزاء العام الذي يشتمل على الإطار الشامل والمتكامل للعقوبات المقررة لمختلف أنواع الجرائم أو أي قانون خاص آخر يتضمن تجريمًا لذات الفعل موضوع التجريم في هذا القانون، وينص في الوقت نفسه على عقوبة أشد وأكثر صرامة وقسوة من العقوبة التي تم تحديدها في هذا القانون فإن الأولوية المطلقة في التطبيق ستكون للعقوبة الأشد والأكثر ردعًا المنصوص عليها في ذلك القانون الآخر، ويستهدف هذا الاستثناء الجوهري تحقيق الانسجام والتكامل بين مختلف التشريعات والقوانين المعمول بها في الدولة، وتفادي نشوء أي تعارض أو تباين غير مبرر في العقوبات المقررة لذات السلوك الإجرامي، مع التأكيد بشكل قاطع على مبدأ تحقيق الردع العام والخاص بأكثر فعالية من خلال تطبيق

[1] المادة رقم (24) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

العقوبة الأشد والأكثر تأثيرًا متى ما كانت موجودة ومنصوصًا عليها في أي قانون آخر ساري المفعول في النظام القانوني للدولة؛ لذلك سنتناول في هذا المبحث مطلبين:

المطلب الأول: الصفة الخاصة للمسؤولين عن جرائم انتهاك البيانات الشخصية وعقوبتهم.

المطلب الثاني: التحديات التشريعية والقضائية في إثبات المسؤولية الجزائية عن انتهاك البيانات الشخصية.

المطلب الأول: الصفة الخاصة للمسؤولين عن جرائم انتهاك البيانات الشخصية وعقوبتهم

يُعد قانون حماية البيانات الشخصية في سلطنة عمان الإطار القانوني الأساسي الذي يُحدد مسؤوليات الأطراف المختلفة في التعامل مع البيانات الشخصية، ووفقًا لهذا القانون تتوزع مسؤولية انتهاك البيانات الشخصية على عدة أطراف سواء كانوا أشخاصًا طبيعيين أو اعتباريين وذلك تبعًا لأدوارهم والتزاماتهم المحددة فيه؛ لذلك سنتناول في هذا الفرع أولا المسؤولون عن جرائم انتهاك البيانات الشخصية وفقا لقانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم 6 / 2022، ثانيًا المسؤولون عن جرائم انتهاك البيانات الشخصية وفقا قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم 12 /2012، ثالثًا الجهة المختصة بالإشراف والتطبيق.

الفرع الأول– قانون حماية البيانات الشخصية العُماني الصادر بالمرسوم السلطاني رقم 6 / 2022:

تتحدد مسؤولية انتهاك البيانات الشخصية على عدة أطراف سواء كانوا أشخاصًا طبيعيين أو اعتباريين وذلك وفقًا للأدوار والالتزامات المنصوص عليها في القانون كالآتي:

أولًا- الأشخاص الطبيعيون:

يمكن أن يكون الأشخاص الطبيعيون مسؤولين عن جرائم انتهاك البيانات الشخصية إذا قاموا بأفعال مخالفة لأحكام القانون على سبيل المثال إذا قام موظف في شركة ما بالكشف عن بيانات شخصية لعملاء الشركة دون وجه حق أو موافقة، فإنه قد يكون مسؤولًا بشكل شخصي عن هذا الانتهاك وبشكل عام فإن أي شخص طبيعي يقوم بمعالجة البيانات الشخصية بشكل يخالف القانون كجمعها أو تخزينها أو نشرها دون سند قانوني أو موافقة صاحب البيانات، يمكن أن يقع تحت طائلة المسؤولية.

ولقد نصت المادة (25) من قانون حماية البيانات على أن " يعاقب بغرامة لا تقل عن (500) خمسمائة ريال عماني، ولا تزيد على (2000) ألفي ريال عماني، كل من يخالف أحكام المادة (14) من هذا القانون" والمادة 14 نصت على أن " يلتزم المتحكم بوضع الضوابط والإجراءات الواجب الالتزام بها عند معالجة البيانات الشخصية، ويجب أن تشتمل على وجه الخصوص الآتي: أ – تحديد المخاطر التي قد تقع على صاحب البيانات الشخصية جراء المعالجة، ب – إجراءات وضوابط نقل وتحويل البيانات الشخصية، ج – التدابير الفنية والإجرائية لضمان تنفيذ المعالجة وفقا لأحكام هذا القانون، د – أي ضوابط أو إجراءات أخرى تحددها اللائحة.

وبناء على المادة (25) سالفة الذكر نجد أن أي شخص طبيعي أو اعتباري يثبت ارتكابه لفعل أو الامتناع عن فعل يُعد مخالفة صريحة لما نصت عليه المادة (14)، فإنه سيُعاقب بعقوبة مالية تتمثل في دفع غرامة.

وقد حددت المادة (25) بدقة الحد الأدنى لقيمة هذه الغرامة المالية بحيث لا يجوز أن تقل عن مبلغ خمسمائة (500) ريال عماني، كما وضعت حدًا أقصى لقيمتها بحيث لا يمكن أن تتجاوز مبلغ ألفي (2000) ريال عماني. ومن خلال هذا التحديد للنطاق المالي للعقوبة، فإن المشرع يمنح الجهة القضائية أو الإدارية المختصة بنظر واقعة المخالفة وتقدير العقوبة المناسبة، سلطة تقديرية في تحديد المبلغ النهائي للغرامة الذي سيتم توقيعه على المخالف، وذلك ضمن الإطار الذي رسمه القانون. وعند ممارسة هذه السلطة التقديرية، يتعين على الجهة المختصة أن تأخذ في الحسبان مجموعة من العوامل والمعايير ذات الصلة، مثل طبيعة المخالفة المرتكبة ومدى جسامتها وتأثيرها، والظروف والملابسات التي صاحبت ارتكاب الفعل المخالف، وما إذا كان المخالف قد سبق له ارتكاب مخالفات مماثلة، بالإضافة إلى أي اعتبارات أخرى قد تكون ذات أهمية في تحقيق العدالة والتناسب بين الفعل المخالف والعقوبة المقررة. ولذلك، فإن الفهم الشامل والدقيق للعقوبة المنصوص عليها في المادة (25) يستلزم بالضرورة الرجوع إلى النص الكامل للمادة (14) من هذا القانون، وذلك لتحديد ماهية الأفعال أو الالتزامات التي يُرتب القانون على مخالفتها هذا الجزاء المالي المحدد.

ثانيًا- الشركات (الأشخاص الاعتبارية):

تتحمل الشركات والجهات الاعتبارية المسؤولية عن انتهاكات البيانات الشخصية التي ترتكب باسمها أو لحسابها تنص المادة (30) من القانون على أنه "مع عدم الإخلال بالمسؤولية الجزائية للأشخاص الطبيعيين، يعاقب الشخص الاعتباري بغرامة لا تقل عن (5000) خمسة آلاف ريال عماني، ولا تزيد على (100000)

مائة ألف ريال عماني، إذا كانت الجريمة قد ارتكبت باسمه، أو لحسابه من قبل رئيس، أو أحد أعضاء مجلس إدارته، أو مديره، أو أي مسؤول آخر، بموافقته، أو بتستر، أو إهمال جسيم منه[1].

من وجهة نظر هذا الباحث هذه المادة تحدد مسؤولية الشخص الاعتباري في حال ارتكاب جريمة انتهاك البيانات من قبل أحد مسؤوليه أو العاملين لديه، سواء كان ذلك بموافقته أو بتستره أو نتيجة إهمال جسيم منه؛ وبالتالي فإن الشركات ملزمة باتخاذ كافة التدابير اللازمة لضمان حماية البيانات الشخصية التي تقوم بمعالجتها، وتتحمل مسؤولية أي إخفاق في ذلك يؤدي إلى انتهاك هذه البيانات.

لذلك نصت المادة (26) من هذا القانون على أنه " يعاقب بغرامة لا تقل عن (1000) ألف ريال عماني، ولا تزيد على (5000) خمسة آلاف ريال عماني، كل من يخالف أحكام المواد (15)، (16)، (17)، (18)، (20)، (22) من هذا القانون".

بناء على المادة سالفة الذكر نجد أن أي شخص طبيعي أو اعتباري يثبت ارتكابه لفعل أو الامتناع عن فعل يُعد مخالفة صريحة لما نصت عليه أي من هذه المواد المذكورة، فإنه سيُعاقب بعقوبة مالية تتمثل في دفع غرامة. وقد حددت المادة (26) بدقة الحد الأدنى لقيمة هذه الغرامة المالية بحيث لا يجوز أن تقل عن مبلغ ألف (1000) ريال عماني، كما وضعت حدًا أقصى لقيمتها بحيث لا يمكن أن تتجاوز مبلغ خمسة آلاف (5000) ريال عماني. ومن خلال هذا التحديد للنطاق المالي للعقوبة، فإن المشرع يمنح الجهة القضائية أو الإدارية المختصة بنظر واقعة المخالفة وتقدير العقوبة المناسبة، سلطة تقديرية في تحديد المبلغ النهائي للغرامة الذي سيتم توقيعه على المخالف، وذلك ضمن الإطار الذي رسمه القانون.

---

[1] المادة رقم (30) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

وعند ممارسة هذه السلطة التقديرية، يتعين على الجهة المختصة أن تأخذ في الحسبان مجموعة من العوامل والمعايير ذات الصلة، مثل طبيعة المخالفة المرتكبة في إطار أي من المواد المذكورة ومدى جسامتها وتأثيرها، والظروف والملابسات التي صاحبت ارتكاب الفعل المخالف، وما إذا كان المخالف قد سبق له ارتكاب مخالفات مماثلة، بالإضافة إلى أي اعتبارات أخرى قد تكون ذات أهمية في تحقيق العدالة والتناسب بين الفعل المخالف والعقوبة المقررة. ولذلك، فإن الفهم الشامل والدقيق للعقوبة المنصوص عليها في المادة (26)، يستلزم بالضرورة الرجوع إلى النصوص الكاملة للمواد (15)، (16)، (17)، (18)، (20)، و (22) من هذا القانون، وذلك لتحديد ماهية الأفعال أو الالتزامات التي يُرتب القانون على مخالفتها هذا الجزاء المالي المحدد.

وذلك لأن المادة (15) نصت على أن" يلتزم المتحكم والمعالج بالضوابط والإجراءات التي تقررها الوزارة، لضمان أن معالجة البيانات الشخصية تمت وفقا لأحكام هذا القانون"، كذلك المادة (16) " يلتزم المتحكم والمعالج – بناء على طلب الوزارة – بتعيين مدقق خارجي للتأكد من أن إجراءات معالجة البيانات الشخصية قد تمت وفقا لأحكام هذا القانون، ووفقا لإجراءات وضوابط المتحكم .." ، المادة (17)" يلتزم المتحكم والمعالج بالاحتفاظ بمستندات عمليات المعالجة، وذلك وفقا للمدد والإجراءات التي تحددها اللائحة، المادة (18)نصت على " يلتزم المتحكم والمعالج بالتعاون مع الوزارة، وتقديم ما تطلبه من بيانات ومستندات تراها لازمة لممارسة اختصاصها طبقا لأحكام هذا القانون، وذلك خلال المدة التي تحددها اللائحة، المادة (20)" يلتزم المتحكم بتحديد مسؤول حماية البيانات الشخصية، وتحدد اللائحة ضوابط اختيار هذا المسؤول ومهامه،المادة(22)نصت على " يلتزم المتحكم بالحصول على الموافقة الكتابية لصاحب البيانات الشخصية قبل إرسال أي مادة إعلانية أو تسويقية وذات أغراض تجارية إليه، وذلك على النحو الذي تحدده اللائحة".

من وجهة نظر الباحث بناءً على المادة (24) التي تضع الإطار العام للعقوبات مع إمكانية تطبيق عقوبات أشد من قوانين أخرى، فإن المادة (26) تحدد بشكل دقيق الغرامة المالية التي تتراوح بين ألف وخمسة آلاف ريال عماني كجزاء على مخالفة الالتزامات الواردة في المواد (15)، (16)، (17)، (18)، (20)، و (22). هذه المواد بدورها تُلقي بمسؤوليات واضحة على عاتق المتحكم والمعالج في البيانات الشخصية، بدءاً بالالتزام بالضوابط والإجراءات التي تحددها الوزارة لضمان المعالجة القانونية (المادة 15)، مروراً بتعيين مدقق خارجي بناءً على طلب الوزارة (المادة 16)، والاحتفاظ بمستندات المعالجة (المادة 17)، والتعاون مع الوزارة وتقديم البيانات المطلوبة (المادة 18)، وتحديد مسؤول لحماية البيانات (المادة 20)، وصولاً إلى الحصول على موافقة كتابية قبل إرسال مواد إعلانية (المادة 22)؛ وعليه فإن الغرامة المحددة في المادة (26) تمثل عقوبة مالية على الإخلال بأي من هذه الالتزامات التنظيمية والإجرائية الهامة التي تهدف في مجملها إلى ضمان حماية البيانات الشخصية وشفافية عمليات معالجتها.

ثالثًا– مزودو الخدمة:

يشير القانون في المادة (7) الفقرة (و) إلى" إصدار وإلغاء تراخيص مزودي الخدمة الذين يعهد إليهم دراسة وتقييم التزام المتحكم والمعالج بأحكام هذا القانون، وفقا للضوابط والإجراءات التي تحددها اللائحة"[1]، بناء على هذه المادة هؤلاء المزودون مرخصون من قبل الوزارة لتقييم مدى التزام المتحكمين والمعالجين بأحكام القانون إذا قصر هؤلاء المزودون في أداء مهامهم بشكل صحيح أو تواطأوا في إخفاء مخالفات فمن الممكن تصور مسؤوليتهم عن المساهمة في انتهاكات البيانات الشخصية ومع ذلك لم تتطرق مواد العقوبات بشكل

[1] المادة رقم (7/ و) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022.

مباشر إلى مسؤولية مزودي الخدمة المرخصين بشكل منفصل، مما يعني أن مسؤوليتهم قد تندرج تحت المسؤولية العامة عن المخالفات أو قد يتم تنظيمها بشكل تفصيلي في اللائحة التنفيذية أو القرارات اللاحقة.

رابعًا–المتحكم والمعالج:

يُعد "المتحكم" و"المعالج" الطرفين الرئيسيين اللذين تقع عليهما مسؤولية حماية البيانات الشخصية بموجب القانون. المتحكم هو من يحدد أهداف ووسائل معالجة البيانات، بينما المعالج يقوم بالمعالجة نيابة عن المتحكم. العديد من المواد في القانون تحدد التزامات كل من المتحكم والمعالج، وبالتالي فإن أي إخلال بهذه الالتزامات يمكن أن يؤدي إلى مسؤوليتهم عن انتهاكات البيانات الشخصية وذلك وفقا لما ورد بالمادة (19)" يلتزم المتحكم، عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات الشخصية عن الاختراق وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة.

بناءً على ما تم تفصيله من مواد قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022 يتضح أن القانون العُماني يولي أهمية خاصة لصفة الجاني في بعض جرائم معالجة البيانات الشخصية حيث يشترط القانون في حالات معينة أن يكون مرتكب الفعل المؤثم هو "المتحكم" أو "المعالج" للبيانات، وتُعرف هذه الصفة بأنها للشخص المسؤول عن تحديد أغراض ووسائل معالجة البيانات أو من يقوم بالمعالجة لحساب المتحكم كما أن اشتراط هذه الصفة الخاصة للجاني يترتب عليه تحميله مسؤوليات قانونية إضافية و قد يؤدي إلى تشديد العقوبات المقررة في حال ثبوت إخلاله بهذه المسؤوليات.

خامسًا– صفة المتحكم والمعالج كعامل في المسؤولية والعقوبة:

يُعرّف القانون "المتحكم" بأنه الشخص الذي يحدد أهداف ووسائل معالجة البيانات الشخصية سواء قام بالمعالجة بنفسه أو عهد بها إلى طرف آخر، أما "المعالج" فهو الشخص الذي يقوم بمعالجة البيانات الشخصية نيابة عن المتحكم[1].

و هذه التفرقة بين المتحكم والمعالج ليست مجرد تصنيف إجرائي بل تحمل تبعات قانونية هامة خاصة فيما يتعلق بالمسؤولية والعقوبات في حال مخالفة أحكام القانون، و عند وقوع مخالفة لأحكام قانون حماية البيانات الشخصية فإن صفة الجاني كونه متحكمًا أو معالجًا للبيانات قد تكون ذات تأثير مباشر على تحديد المسؤولية وتغليظ العقوبة فالمتحكم بحكم سلطته في تحديد أهداف ووسائل المعالجة يتحمل مسؤولية أساسية عن ضمان الالتزام بأحكام القانون وبالمثل فإن المعالج الذي يقوم بتنفيذ عمليات المعالجة بناءً على تعليمات المتحكم، يقع عليه واجب الالتزام بهذه التعليمات وبالقانون ذاته.

يلاحظ من استعراض الفصل الخامس من القانون المتعلق بالعقوبات أن هناك مواد تفرض عقوبات على المخالفات بشكل عام في حين أن مواد أخرى قد تتضمن إشارات ضمنية أو فعلية إلى مسؤولية المتحكم أو المعالج بشكل خاص نظرًا لطبيعة الالتزامات المفروضة عليهم في الفصول الأخرى من القانون على سبيل المثال الالتزام بإخطار صاحب البيانات الشخصية ببيانات المتحكم والمعالج (المادة 14)، أو الالتزام بتعيين مدقق خارجي بناءً على طلب الوزارة (المادة 16)، هي التزامات تقع بشكل أساسي على عاتق المتحكم و/أو المعالج.

---

[1] المادة رقم (1) قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022

سادسًا– تشديد العقوبات بناءً على صفة المسؤولين عن جرائم انتهاك البيانات الشخصية وسلطة المحكمة في توقيع الجزاء:

يُنشئ قانون حماية البيانات الشخصية في سلطنة عُمان إطاراً متدرجاً من العقوبات المالية للردع، حيث يمنح الجهات المختصة (القضائية أو الإدارية) سلطة تقديرية واسعة في توقيع الغرامات. تنص المادة (27) على غرامة تتراوح بين (5,000) وخمسة آلاف ريال إلى (10,000) عشرة آلاف ريال عُماني لمخالفة التزامات المتحكم المتعلقة بوضع الضوابط والإجراءات (م 13)، بينما تتصاعد العقوبة في المادة (28) لتصبح بين (15,000) وخمسة عشر ألف ريال إلى (20,000) عشرين ألف ريال عُماني عند مخالفة مواد أكثر جسامة مثل المواد (5) و(6) و(19) و(21) وفي أقصى درجات المخالفة، تنص المادة (29) على غرامات رادعة تتراوح بين (100,000) مائة ألف ريال و(500,000) خمسمائة ألف ريال عُماني مما يعكس مدى خطورة الأفعال التي ترتبط بها و عند تقدير قيمة الغرامة النهائية في كل حالة، يجب على الجهة المختصة الأخذ في الحسبان جسامة المخالفة الأضرار المترتبة عليها والسوابق المماثلة للمخالف وذلك لتحقيق العدالة والتناسب وإضافة إلى ذلك تمنح المادة (31) المحكمة المختصة صلاحية الحكم بمصادرة الأدوات التي استُعملت في ارتكاب الجريمة كما تتيح المادة (32) للوزارة المختصة فرض جزاءات إدارية سريعة ومرنة لا تزيد قيمتها على (2,000) ألفي ريال عُماني للمخالفات الأقل جسامة، دون إخلال بالعقوبات الجنائية الأخرى.

بناء على ما سبق إيضاحه يرى الباحث أن قانون حماية البيانات الشخصية في سلطنة عمان يضع مسؤولية حماية البيانات على عاتق جميع الأطراف المشاركة في معالجتها سواء كانوا أشخاصًا طبيعيين يقومون بأفعال مخالفة بشكل مباشر، أو شركات وجهات اعتبارية تتحمل مسؤولية أفعال موظفيها، أو المتحكمين والمعالجين الذين يقع عليهم العبء الأكبر في تطبيق أحكام القانون وضمان سلامة البيانات.

الفرع الثاني– قانون مكافحة جرائم تقنية المعلومات العماني الصادر بالمرسوم السلطاني رقم 12 / 2011:

في قانون مكافحة جرائم تقنية المعلومات لا يوجد فصل أو مواد تحدد بشكل مباشر المسؤولية عن "انتهاك البيانات الشخصية" كمصطلح قانوني محدد، ومع ذلك يتضمن القانون عدة مواد تجرّم أفعالًا قد تؤدي إلى المساس بسلامة وسرية وتوافر البيانات والمعلومات الإلكترونية؛ والتي قد تشمل البيانات الشخصية وبناءً على ذلك يمكن تحديد الأطراف التي قد تقع عليها المسؤولية عن هذه الأفعال التي قد تشكل انتهاكًا للبيانات الشخصية:

أولًا– الأشخاص الطبيعيون:

يمكن أن يكون الأشخاص الطبيعيون مسؤولين عن ارتكاب جرائم تقنية المعلومات التي قد تؤدي إلى انتهاك البيانات الشخصية كما ورد بالمادة (3)" يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك، فإذا ترتب على ما ذكر في الفقرة الأولى إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية أو إلحاق ضرر بالمستخدمين أو المستفيدين، تكون العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين، فإذا كانت البيانات أو المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة

السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين"[1]،بناء على المادة سالفة الذكر يستنتج الباحث أن أي فرد يقوم بهذه الأفعال المتعلقة بالبيانات الشخصية بشكل غير قانوني قد يقع تحت طائلة المساءلة القانونية، بالاضافة للمادة االسالفة الذكر نجد المادة (16) تنص على " يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على خمسة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات كالهواتف النقالة المزودة بآلة تصوير في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بالتقاط صور أو نشر أخبار أو تسجيلات صوتية أو مرئية تتصل بها ولو كانت صحيحة، أو في التعدي على الغير بالسب أو القذف"[2].

بناء على ما سبق إيضاحه يرى الباحث أن تؤسس المادة (3) من قانون مكافحة جرائم تقنية المعلومات العماني مسؤولية الأشخاص الطبيعيين عن الدخول غير المصرح به إلى الأنظمة والمعلومات الرقمية، مع تشديد العقوبة بشكل ملحوظ عندما يكون الهدف أو الناتج عن هذا الدخول غير القانوني هو بيانات شخصية. تجرم هذه المادة الدخول العمدي أو تجاوز حدود الدخول المصرح به أو الاستمرار فيه بشكل غير قانوني، بالإضافة إلى أي أفعال مصاحبة تؤدي إلى إلغاء أو تغيير أو إتلاف أو نشر البيانات الشخصية. وتتدرج العقوبات من السجن والغرامة في الحالات العامة إلى عقوبات أشد تصل إلى السجن لمدة ثلاث سنوات والغرامة عند استهداف البيانات الشخصية، مما يعكس الأهمية التي يوليها المشرع لحماية خصوصية الأفراد في الفضاء الرقمي وتجريم أي محاولة للوصول أو العبث ببياناتهم الشخصية دون وجه حق.

---

[1] المادة رقم (3) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] المادة رقم (16) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

ومن جانب آخر تتناول المادة (16) من نفس القانون مسؤولية الأشخاص الطبيعيين عن استخدام وسائل تقنية المعلومات، وتحديدًا الهواتف المزودة بآلات تصوير والشبكة المعلوماتية، في الاعتداء على حرمة الحياة الخاصة والعائلية للأفراد.

تجرم هذه المادة التقاط الصور أو نشر الأخبار أو التسجيلات الصوتية أو المرئية المتعلقة بالحياة الخاصة دون رضا المعنيين، بالإضافة إلى التعدي على الغير بالسب أو القذف عبر الإنترنت. وقد حددت المادة عقوبة موحدة لهذه الأفعال تتمثل في السجن والغرامة أو إحداهما، مما يؤكد على أن القانون لا يتسامح مع استغلال التقنية في انتهاك خصوصية الأفراد أو الإساءة إليهم عبر نشر بياناتهم الشخصية أو المعلومات المتعلقة بحياتهم الخاصة أو سمعتهم بشكل غير قانوني.

ثانيًا- الشركات (الأشخاص الاعتبارية):

تنص المادة (29)" دون إخلال بالمسؤولية الجزائية للأشخاص الطبيعيين، يعاقب الشخص الاعتباري بغرامة تعادل ضعف الحد الأعلى لعقوبة الغرامة المقررة قانونا للجريمة، إذا كانت الجريمة قد ارتكبت باسمه أو لحسابه من قبل رئيس أو أحد أعضاء مجلس إدارته أو مديره أو أي مسؤول آخر يتصرف بتلك الصفة أو بموافقته أو بتستر أو بإهمال جسيم منه"[1].

يرى الباحث بناء على المادة السابقة أن الشخص الاعتباري مسؤول عن جرائم تقنية المعلومات التي تُرتكب باسمه أو لحسابه حيث يُعاقب بغرامة تعادل ضعف الحد الأعلى للغرامة المقررة قانونًا إذا ارتُكبت الجريمة من قبل رئيس أو عضو مجلس إدارة أو مدير أو أي مسؤول آخر بتصريح منه أو بتغطية منه أو

[1] المادة رقم (19) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

نتيجة إهمال بالغ من جانبه، مما يعني إمكانية تحميل الشركات المسؤولية الجنائية عن أفعال مسؤوليها أو إهمالهم الجسيم الذي يسفر عن جرائم تقنية معلومات مثل حالة سماح شركة بإهمال فادح يؤدي إلى اختراق أنظمتها وسرقة بيانات العملاء.

ثالثًا- مزودو الخدمة:

تُعرّف المادة (1) الفقرة (ك) مزود الخدمة بأنه " كل شخص طبيعي أو اعتباري عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات أو يقوم بمعالجة أو تخزين البيانات والمعلومات الإلكترونية نيابة عن خدمة الاتصالات أو مستخدميها"[1].

بناء على هذه المادة يمكن أن يكون مزودو الخدمة مسؤولين عن جرائم تقنية المعلومات إذا ارتكبوا أفعالًا مجرّمة بموجب القانون وتتعلق بالبيانات الشخصية التي يقومون بمعالجتها أو تخزينها فإذا قام مزود خدمة بالولوج غير المصرح به إلى بيانات شخصية مخزنة لديه أو قام بنشرها بشكل غير قانوني فإنه قد يكون مسؤولًا بموجب المادة سالفة الذكر، بالإضافة إلى ذلك قد يكون مزود الخدمة مسؤولًا إذا فشل في اتخاذ التدابير الأمنية اللازمة لحماية البيانات الشخصية التي يعالجها أو يخزنها مما أدى إلى اختراقها أو الوصول إليها بشكل غير قانوني، خاصة إذا كان هذا الفشل ناتجًا عن إهمال جسيم.

[1] المادة رقم (1/ ك) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

وبالنظر إلى مواد قانون مكافحة جرائم تقنية المعلومات العماني رقم 12 / 2011 نجد أن القانون قد أخذ في الاعتبار الصفة الخاصة للجاني في عدة مواضع حيث تترتب على هذه الصفة مسؤوليات إضافية وتؤدي إلى تشديد العقوبات في بعض الحالات ويمكن تلخيص هذه الحالات كما يلي:

- **الموظف العام أو من في حكمه أثناء أو بمناسبة تأدية عمله (المادة 4):**

تنص المادة (4) على أنه " يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من ارتكب إحدى الجرائم المنصوص عليها في المادة (3) من هذا القانون أثناء أو بمناسبة تأدية عمله"[1].

هنا صفة الجاني كموظف مسؤول عن الأنظمة أو البيانات تجعله في موقع استغلال سلطته أو صلاحياته، مما يستدعي تشديد العقوبة.

- **تغيير أو إتلاف البيانات الطبية (المادة 5):**

تنص المادة (5) على " يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على عشرة آلاف ريال عماني، كل من غير أو عدل أو أتلف عمدا ودون وجه حق باستخدام وسائل تقنية المعلومات بيانات أو معلومات إلكترونية عبارة عن تقرير فحص أو تشخيص أو علاج أو رعاية طبية مخزن في نظام معلوماتي أو وسائل تقنية المعلومات"[2].

---

[1] المادة رقم (4) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] المادة رقم (5) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

على الرغم من أن المادة لا تشترط صفة محددة للجاني، إلا أن طبيعة البيانات المستهدفة (طبية) قد تشير ضمنيًا إلى أن الجاني قد يكون له وصول خاص بحكم وظيفته أو تخصصه، مما يجعله مسؤولًا بشكل أكبر عن سلامة هذه البيانات.

- **الدخول للحصول على بيانات حكومية أو مصرفية سرية (المادة 6):**

تُشدد العقوبة في المادة (6) "..... كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا بقصد الحصول على بيانات أو معلومات إلكترونية حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك،.. "[1].

بناء على المادة 6 سالفة الذكر في هذه الحالة قد يكون الجاني موظفًا في جهة حكومية أو مصرف أو مؤسسة مالية ولديه صلاحية وصول بحكم عمله، ولكنه استغل هذه الصلاحية بطريقة غير مشروعة.

- **إساءة استخدام وسائل تقنية المعلومات (المادة 11):**

تعاقب المادة (11) ".. كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج أو بيع أو شراء أو استيراد أو توزيع أو عرض أو إتاحة برامج أو أدوات أو أجهزة مصممة أو مكيفة لأغراض ارتكاب جرائم تقنية المعلومات أو كلمات سر أو رموز تستخدم لدخول نظام معلوماتي، أو حاز أدوات أو برامج مما ذكر، وذلك بقصد استخدامها في ارتكاب جرائم تقنية المعلومات"[2].

---

[1] المادة رقم (6) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

[2] المادة رقم (11) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

هنا الصفة الخاصة تكمن في نية الجاني واستعداده لارتكاب جرائم تقنية المعلومات من خلال الأدوات التي يمتلكها أو يتعامل بها.

- التزوير والاحتيال المعلوماتي (المادتان 12 و13):

في جرائم التزوير والاحتيال المعلوماتي، قد لا تكون هناك صفة محددة للجاني بالمعنى الوظيفي، لكن قدرة الجاني على الوصول إلى الأنظمة والمعلومات والتلاعب بها هي التي تمكنه من ارتكاب الجريمة، إذا كان النظام المعلوماتي خاصًا بجهة حكومية أو مصرف أو مؤسسة مالية، فإن العقوبة تُشدد، مما يعكس أهمية حماية هذه الأنظمة وحقيقة أن من لديهم وصول إليها قد يكونون في موقع مسؤولية أكبر.

- المسؤولية الجزائية للشخص الاعتباري (المادة 29):

تنص المادة (29) ".. يعاقب الشخص الاعتباري بغرامة تعادل ضعف الحد الأعلى لعقوبة الغرامة المقررة قانونا للجريمة، إذا كانت الجريمة قد ارتكبت باسمه أو لحسابه من قبل رئيس أو أحد أعضاء مجلس إدارته أو مديره أو أي مسؤول آخر يتصرف بتلك الصفة أو بموافقته أو بتستر أو بإهمال جسيم منه[1]، وهنا صفة المسؤول في الكيان الاعتباري هي التي تجعل الكيان مسؤولًا جنائيًا ويُعاقب بغرامة مضاعفة.

من وجهة نظر الباحث بوجه عام على الرغم من أن القانون لا يحدد دائمًا صفة معينة للجاني في كل جريمة إلا أنه يولي اهتمامًا خاصًا للحالات التي يكون فيها الجاني في موقع مسؤولية أو سلطة تسمح له بارتكاب الجريمة بسهولة أكبر أو يكون تأثير فعله أشد ضررًا (مثل الموظف العام، المتعامل مع البيانات الطبية

[1] المادة رقم (29) قانون مكافحة جرائم تقنية المعلومات الصادر بالمررسوم السلطاني رقم 12 / 2011.

أو الحكومية أو المصرفية) كما أن القانون يركز على نية الجاني في بعض الجرائم المتعلقة بإساءة استخدام الأدوات والبرامج. بالإضافة إلى ذلك، يُحمّل القانون المسؤولية للأشخاص الاعتباريين بناءً على صفة المسؤولين الذين ارتكبوا الجريمة باسمهم أو لحسابهم، وبالتالي يمكن القول إن قانون مكافحة جرائم تقنية المعلومات العماني يأخذ في الاعتبار الصفة الخاصة للجاني كعنصر مؤثر في تحديد المسؤولية وتغليظ العقوبة عند الاقتضاء خاصة عندما يكون الجاني في موقع ائتمان أو سلطة أو عندما تكون طبيعة البيانات أو الأنظمة المستهدفة حساسة أو ذات أهمية خاصة.

بناء على ما سبق إيضاحه يود الباحث أن يؤكد على أن قانون مكافحة جرائم تقنية المعلومات يركز على الأفعال التي تمثل جرائم تقنية المعلومات بشكل عام والتي قد تشمل أفعالًا تؤدي إلى انتهاك البيانات الشخصية، بينما قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم 6 / 2022 يركز بشكل خاص على تنظيم معالجة البيانات الشخصية وحماية حقوق أصحابها ويحدد التزامات واضحة للمتحكمين والمعالجين في هذا الشأن، وفي حالات انتهاك البيانات الشخصية، يمكن أن تطبق أحكام كلا القانونين حسب طبيعة الفعل المرتكب والضرر الناتج.

الفرع الثالث– الجهة المختصة بالإشراف والتطبيق:

بناءً على مواد اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادر بالقرار الوزاري رقم 34 / 2024 تتضح مسؤولية وزارة النقل والاتصالات وتقنية المعلومات كجهة مختصة بالإشراف والتطبيق على النحو التالي:

تُلزم المادة الثانية المتحكم أو المعالج بموافاة الإدارة المختصة (التقسيم الإداري المختص في الوزارة لإدارة حماية البيانات الشخصية) بأي مستندات أو بيانات أو معلومات تطلبها خلال (30) يومًا من تاريخ الطلب؛ وهذا ما يُظهر دور الإدارة المختصة كجهة تتلقى المعلومات اللازمة لمراقبة الامتثال للقانون واللائحة[1].

كما تُحدد المواد (5: 10) دور الوزارة (ممثلة في الإدارة المختصة والوزير) في عملية إصدار التصاريح الضرورية لمعالجة البيانات الشخصية كالآتي[2]:

المادة (5) تُلزم المتحكم بالحصول على تصريح من الوزارة قبل البدء في معالجة البيانات وتقديم نموذج مُحدد يتضمن معلومات أساسية حول عملية المعالجة ، كما أن المادة (6) تُلزم المتحكم عند تقديم طلب التصريح إرفاق سياسة حماية البيانات الخاصة به وتفاصيل التدابير الاحترازية المُعتمدة لمواجهة اختراق البيانات وذلك لتقييمها من قبل الوزارة، كما تتولى الإدارة المختصة مسؤولية دراسة طلب التصريح والبت فيه خلال مدة لا تتجاوز (45) يومًا، وفي حال الرفض يجب أن يكون القرار مُسببًا، مع إتاحة حق التظلم إلى الوزير ذلك وفقا للمادة (7)، كما يصدر التصريح رسميًا من الوزير لمدة أقصاها خمس سنوات بعد استيفاء الشروط وسداد الرسوم، مع إمكانية التجديد بنفس الإجراءات وذلك وفقا للمادة (8)، كما تُلزم المادة (9) المتحكم بإبلاغ الإدارة المختصة بأي تغييرات تطرأ على البيانات المُضمنة في التصريح خلال (15) يومًا من تاريخ التعديل، و تحدد

(1) المادة (2) وزارة النقل والاتصالات وتقنية المعلومات قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية.

(2) المواد من (5: 10) وزارة النقل والاتصالات وتقنية المعلومات قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية.

المادة(10) حالات إلغاء التصريح من قبل الوزارة، مثل مخالفة القانون أو اللائحة، أو عدم الإبلاغ عن التعديلات، أو الحصول على التصريح بطرق احتيالية.

وتوضح المواد من (41: 45) اجراءات الشكاوى والتحقيق فيها وتوقيع الجزاءات من قبل الإدارة المختصة والوزير كالآتي[1]:

فبناء على المادة (41) يحق لأصحاب البيانات أو أي شخص ذي مصلحة تقديم شكوى أو بلاغ إلى الإدارة المختصة بشأن أي مخالفة للقانون أو اللائحة خلال (30) يومًا من العلم بالمخالفة، وتتولى الإدارة إخطار المتحكم بالشكوى، كما تتولى الإدارة المختصة مسؤولية البت في الشكوى أو البلاغ خلال (60) يومًا وذلك بناء على المادة (43)، ووفقًا لما ورد بالمادة (44) يُمنح الوزير صلاحية توقيع جزاءات إدارية على المخالفين، تشمل الإنذار، ووقف التصريح، والغرامة المالية، وإلغاء التصريح ، و يُتاح لمن وقع عليه الجزاء حق التظلم إلى الوزير خلال (60) يومًا من تاريخ الإخطار بالقرار وذلك بناء على المادة (45).

المطلب الثاني:
التحديات التشريعية والقضائية في إثبات المسؤولية الجزائية عن انتهاك البيانات الشخصية

تواجه منظومة العدالة في سلطنة عمان تحديات كبيرة في تطبيق أحكام قانون حماية البيانات الشخصية لا سيما عند محاولة إثبات المسؤولية الجزائية عن انتهاك هذه البيانات، كما تبرز هذه التحديات في أكثر من جانب سواء على المستوى التشريعي الذي يواجه صعوبات في تحديد أركان الجريمة وتوزيع المسؤولية أو على

[1] المواد من (41:45) وزارة النقل والاتصالات وتقنية المعلومات قرار وزاري رقم 34 / 2024 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية.

المستوى القضائي والإجرائي في التعامل مع طبيعة الجرائم الإلكترونية العابرة للحدود، و هذه الصعوبات مجتمعة تُعقد مسار التقاضي وتتطلب جهودًا مضاعفة من كافة الجهات المعنية لضمان تحقيق العدالة؛ و بناءً على ذلك سنتناول في هذا المطلب فرعين:

الفرع الأول: التحديات التشريعية في تحديد الجريمة وتوزيع المسؤولية.

الفرع الثاني: التحديات القضائية والإجرائية في الإثبات والتحقيق في جريمة انتهاك البيانات الشخصية.

الفرع الأول– التحديات التشريعية في تحديد جريمة انتهاك البيانات الشخصية وتوزيع المسؤولية:

أولًا– صعوبة تحديد أركان الجريمة الجزائية وإثبات القصد الجنائي:

بالرغم من أن قانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم 6 لسنة 2022 يحدد في مواده من المادة الخامسة إلى المادة الثالثة والعشرين الأفعال المخالفة التي تستوجب العقوبة[1]، فإن القضاء يواجه تحديًا كبيرًا في إثبات المسؤولية الجزائية عن انتهاك البيانات الشخصية حيث تكمن الصعوبة الأولى في تحديد أركان الجريمة بشكل دقيق لا سيما في سياق الجرائم الإلكترونية المعقدة[2]، وهذا ما أكده حكم المحكمة العمانية العليا في حكمها الصارد في 2006 حيث أن الصعوبة الأساسية تكمن في الطبيعة

[1] المواد من رقم (5) الى رقم (23) من قانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] محمد علي مقراش، حجية أدلة الاثبات أمام القاضي الجزائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2019، ص63.

غير المادية للجرائم الإلكترونية؛ فخلافًا للجرائم التقليدية التي تعتمد على أدلة ملموسة تتطلب هذه الجرائم إثبات وقائع يصعب تحديدها بدقة وتعتمد على أدلة رقمية مثل البيانات والنبضات[1].

ولمواجهة هذا التحدي يجب على القضاء أن يؤدي دورًا إيجابيًا وفعالًا في تحري الحقيقة؛ فبخلاف القاضي المدني يتوجب على القاضي الجزائي البحث عن الحقيقة الموضوعية بنفسه، وذلك من خلال الاستعانة بالوسائل التقنية الحديثة ويشمل ذلك تفتيش نظم الحاسوب وطلب مساعدة الخبراء المتخصصين لجمع الأدلة الرقمية ولكن يجب أن يتم قبول هذه الأدلة فقط بعد التأكد من مشروعيتها وأن تكون مستندة إلى اكتشاف علمي أو تقني حديث، مما يضمن أن يواجه القضاء الصعوبات المتعلقة بالبيانات الشخصية عبر التكنولوجيا والضوابط القانونية المناسبة[2].

ومن وجهة نظر الباحث يرى أن الإثبات في هذه الجرائم يشكل تحديًا كبيرًا لعدة أسباب أولًا صعوبة تتبع مسار الجريمة، حيث تُرتكب غالبًا عبر شبكات إلكترونية معقدة قد يستخدم فيها الفاعلون تقنيات متطورة لإخفاء هوياتهم، و ثانيًا صعوبة إثبات الركن المادي للجريمة أي الفعل الإجرامي نفسه، و ثالثًا وأهمًا التحدي الأكبر هو إثبات الركن المعنوي أو القصد الجنائي وذلك لأنه يصعب تحديد ما إذا كان الفاعل (المتحكم أو المعالج) ارتكب الفعل المخالف بقصد الإضرار أم أنه كان نتيجة إهمال جسيم فقط؟؛ وذلك لأنه المادة (30) من قانون حماية البيانات الشخصية تعاقب الشخص الاعتباري إذا ارتكبت الجريمة "بموافقته، أو بتستر، أو

---

[1] الطعن رقم (392/2006)، جزائي عليا جلسة الثلاثاء 7/ 2006/11.

[2] الحماية الجنائية لخصوصية البيانات الشخصية الرقمية، على الرابط الالكتروني التالي:
https://jordan-lawyer.com/2022/10/23/criminal-protection-of-the-privacy-of-digital-personal-data/ تاريخ الزيارة 23 أغسطس 2025.

إهمال جسيم منه" وهو ما يفرض على جهات التحقيق عبئًا إضافيًا لإثبات هذا القصد؛ لأن الاختراق قد يحدث بسبب ثغرة أمنية غير مكتشفة أو خطأ بشري غير متعمد وفي هذه الحالات يصبح التمييز بين الإهمال الجزائي والجريمة العمدية أمرًا بالغ الصعوبة مما يؤدي إلى تعقيد مسار التقاضي، لذلك فإن الحاجه إلى وجود خبراء فنيين متخصصين في الأدلة الرقمية لفك شفرات الجرائم الإلكترونية وتحليلها تصبح أمرًا حتميًا وهو ما قد لا يكون متاحًا بسهولة في جميع الحالات[1].

ثانيًا– صعوبة إثبات الضرر المترتب على انتهاك البيانات الشخصية:

لا تقتصر التحديات على إثبات الفعل الإجرامي والقصد الجنائي بل تتعداه إلى إثبات الضرر المترتب على انتهاك البيانات الشخصية[2]، فقانون حماية البيانات الشخصية العماني يربط بعض الالتزامات بالإضرار أو المخاطر المحتملة كما هو الحال في المادة (19) التي تلزم المتحكم بالإبلاغ عن الاختراق الذي "يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية"[3]، وفي المادة (32) من اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بالقرار الوزاري رقم 34 لسنة 2024 التي تحدد واجب الإخطار لصاحب البيانات الشخصية إذا كان الاختراق "يسبب ضررًا جسيمًا أو مخاطر عالية"[4]، حيث يبرز التحدي القضائي في تحديد ماهية هذا "الضرر الجسيم" أو "المخاطر العالية" وإثباته بصورة ملموسة

---

[1] إيمان أحمد على طه، الحماية التشريعية للحق في خصوصية البيانات في العصر الرقمي، جامعة الأزهر، الجزء الثالث، العدد السادس والثلاثون، 2021، ص 48.

[2] رشيدة بوبكر، الحماية الجزائية للتعاملات الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص493.

[3] المادة رقم (19) من قانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم 6 / 2022.

[4] المادة رقم (32) من اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بالقرار الوزاري رقم 34 / 2024.

وقاطعة؛ ففي كثير من الأحيان لا يكون الضرر ماديًا مباشرًا بل قد يكون ضررًا معنويًا أو ضررًا محتملًا قد يترتب عليه عواقب سلبية في المستقبل مثل استخدام البيانات المسربة في عمليات احتيال أو انتحال شخصية[1].

ويتطلب حل التحدي القضائي المتمثل في إثبات "الضرر الجسيم" أو "المخاطر العالية" في انتهاكات البيانات الشخصية تبني نهجاً يجمع بين الخبرة القانونية والتقنية يمكن تحقيق ذلك من خلال الاعتماد على تقارير خبرة متخصصة حيث يقوم خبراء الأدلة الرقمية والأمن السيبراني بتقييم طبيعة وحجم البيانات المخترقة وتحليل كيفية استخدامها المحتمل في أنشطة ضارة مثل الاحتيال أو انتحال الشخصية في المستقبل[2]، كما يمكن للمشرع أن يحدد معايير واضحة لما يشكل "ضررًا جسيمًا" سواء كان ذلك بالنظر إلى حساسية البيانات المخترقة (مثل البيانات الصحية أو المالية) أو عدد الأشخاص المتضررين أو الأثر المحتمل على خصوصيتهم وسلامتهم بالإضافة إلى ذلك يجب أن تتجه الأحكام القضائية نحو تقدير الضرر المعنوي والمحتمل وعدم قصره على الضرر المادي المباشر بما يعكس خطورة انتهاكات البيانات الشخصية على الفرد والمجتمع ويتطلب هذا النهج أيضاً نقل عبء الإثبات على الجهة التي حدث لديها الاختراق (المتحكم بالبيانات) لتقديم الدليل على اتخاذها كافة الإجراءات اللازمة لمنع الضرر أو تخفيفه وإثبات أن الاختراق لم ينتج عنه ضرر جسيم أو مخاطر عالية[3].

---

[1] عبد القادر كمال، محمد نور الدين، أثر مبدأ المشروعية في حجية الدليل الجزائي في القانون الجزائري، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، العدد الأول، المجلد الرابع عشر، جامعة معسكر، الجزائر، 2017، ص266.

[2] رشيدة بوبكر، المرجع السابق، ص493.

[3] عبد القادر كمال، محمد نور الدين، المرجع السابق، ص266.

بناء على ما سبق إيضاحه من وجهة نظر الباجث إن إقناع المحكمة بوجود هذا النوع من الأضرار يمثل تحديًا كبيرًا خاصة إذا لم يتم استخدام البيانات المخترقة على الفور كما أن اللائحة لم تحدد معايير واضحة لتقييم "الضرر الجسيم" أو "المخاطر العالية" مما يترك الأمر لاجتهاد كل حالة على حدة، وهو ما قد يؤدي إلى تباين في الأحكام القضائية وهذا الغموض في تحديد معايير الضرر قد يشكل ثغرة قانونية يصعب من خلالها إثبات المسؤولية الجزائية وتحقيق العدالة الكاملة لأصحاب البيانات المتضررة.

ثالثًا– صعوبة تحديد الجهة المسؤولة عن انتهاك البيانات الشخصية:

إن تحديد الجهة المسؤولة عن انتهاك البيانات الشخصية يشكل تحديًا قضائيًا بارزًا نظرًا لتعدد الأطراف المشاركة في عملية المعالجة[1]، وبالرجوع للمادة الأولى من لقانون حماية البيانات الشخصية العماني نجد القانون يفرق بين "المتحكم" الذي يحدد أهداف المعالجة، و"المعالج" الذي ينفذها نيابة عن المتحكم وفي كثير من الحالات يعهد المتحكم بالمعالجة إلى معالج خارجي، مما يخلق تداخلاً في المسؤوليات[2]، بناء على هذه المادة هل يتحمل المتحكم المسؤولية الكاملة في حال إهمال المعالج؟ أم أن المسؤولية تقع على عاتق المعالج فقط؟ كما أن المادة رقم (30) من قانون حماية البيانات الشخصية تعاقب الشخص الاعتباري ولكنها لا تعفي الأفراد من المسؤولية الجزائية[3].

---

[1] عائشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث، المجلد الثاني، العدد الخامس، يونيو 2016، ص 52.

[2] المادة رقم (1) من اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بالقرار الوزاري رقم 34 لسنة 2024.

[3] المادة رقم (30) من قانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم 6 لسنة 2022.

من وجهة نظر الباحث بناء ما سبق إيضاحه هنا يُطرح سؤالاً قضائياً معقدًا حول كيفية تحديد المسؤولية الفردية لرئيس مجلس الإدارة، أو المدير، أو أي مسؤول آخر، خاصة وأن القانون سالف الذكر ينص على أن المسؤولية تقع إذا كان الانتهاك "بموافقته، أو بتستر، أو إهمال جسيم منه" و إثبات هذه الأفعال يتطلب تحقيقات داخلية معقدة ودقيقة وقد يواجه القضاء صعوبة في الحصول على الأدلة الكافية لإدانة فرد معين داخل المؤسسة ، و بالإضافة إلى ذلك قد يتم إسناد المسؤولية إلى شخص اعتباري أجنبي مما يثير تحديات أخرى تتعلق بالاختصاص القضائي وتنفيذ الأحكام وذلك لأن عدم وجود نصوص واضحة تحدد المسؤولية المشتركة أو التفصيلية بين المتحكم والمعالج يجعل من الصعب على القضاء الفصل في هذه القضايا بشكل حاسم وقد يؤدي إلى إفلات بعض الأطراف من العقاب.

ولمواجهة تحدي تحديد المسؤولية بين "المتحكم" و"المعالج" يتطلب تبني نهج المسؤولية المشتركة والمترابطة بدلاً من إلقاء المسؤولية الكاملة على طرف واحد، ففي حين أن المتحكم هو الجهة التي تحدد أهداف المعالجة وطريقتها ويتحمل المسؤولية الأساسية عن البيانات؛ فإن ذلك لا يعفيه من المسؤولية في حال إهمال المعالج كما تقع على عاتق المتحكم مسؤولية قانونية وعقدية أساسية تتمثل في اختيار المعالج المناسب والتحقق من التزامه بالضمانات الأمنية والفنية الكافية لحماية البيانات، و يجب على المتحكم أن يضمن وجود عقد مفصل يوضح بوضوح التزامات كل طرف في حالة خرق البيانات أو التقصير في تطبيق الإجراءات الأمنية[1].

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 53.

الفرع الثاني– التحديات القضائية والإجرائية في الإثبات والتحقيق في جريمة انتهاك البيانات الشخصية:

أولًا– تحديات التحقيق في الجرائم العابرة للحدود:

تعتبر الجرائم العابرة للحدود من أكبر التحديات التي تواجه القضاء في قضايا انتهاك البيانات الشخصية[1]، فالمادة (23) من قانون حماية البيانات الشخصية العماني تسمح للمتحكم بنقل البيانات الشخصية خارج حدود سلطنة عمان شريطة الالتزام بالضوابط والإجراءات التي تحددها اللائحة[2]، والمادة (38) من اللائحة التنفيذية للقانون سالف الذكر تلزم المتحكم بضمان مستوى حماية كافٍ لدى جهة المعالجة الخارجية .[3]

بناء على المواد سابقة الذكر يعتقد الباحث أنه يصعب على السلطات القضائية العمانية بسط ولايتها الكاملة على الأطراف الأجنبية فعملية التحقيق وجمع الأدلة مثل تفتيش الخوادم أو الحصول على سجلات الدخول كما ان عملية التحقق في هذه الحالة تتطلب تعاونًا قضائيًا ودوليًا قد يستغرق وقتًا طويلاً أو يواجه عوائق قانونية وسيادية قد ترفض بعض الدول تقديم المساعدة القضائية لأسباب تتعلق بسيادتها أو لاختلاف قوانينها، كما أن إثبات أن المتحكم العماني كان يعلم بأن جهة المعالجة الخارجية لا توفر حماية كافية يصبح أمرًا معقدًا، خاصة أن المادة (39) من اللائحة التنفيذية لقانون حماية البيانات الشخصية العماني تطلب من

---

[1] سامح عبد الواحد التهامي، المسؤولية المدنية عن فيرسة النظم المعلوماتية عبر الانترنت، مجلة الحقوق، جامعة الكويت، المجلد 40، العدد الثالث، 2016، ص 31.

[2] المادة رقم (23) من قانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم 6 / 2022.

[3] المادة رقم (38) من اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بالقرار الوزاري رقم 34 / 2024.

المتحكم إجراء تقييم لمستوى الحماية ولكنها لا تفرض عقوبة جزائية على عدم كفاية هذا التقييم[1]، و هذا الغموض التشريعي إلى جانب الصعوبات الإجرائية في تتبع الجريمة عبر الشبكات العالمية يضع القضاء أمام مأزق حقيقي في تطبيق أحكام القانون وإنفاذ العقوبات الجزائية؛ مما قد يؤدي إلى إفلات المجرمين من العقاب.

و يتطلب حل تحدي الجرائم العابرة للحدود في قضايا انتهاك البيانات الشخصية تبني استراتيجيات تعاون دولي فعّال وتطوير أطر قانونية و على الرغم من أن المادة (23) من قانون حماية البيانات الشخصية العماني والمادة (38) من لائحته التنفيذية تلزمان المتحكم بضمان مستوى حماية كافٍ لدى جهة المعالجة الخارجية، إلا أن الواقع العملي للتحقيق في حال وقوع اختراق في دولة أخرى يظل معقداً للتعامل مع هذا التحدي يمكن الاعتماد على آليات التعاون القضائي الدولي المتمثلة في الاتفاقيات والمعاهدات الثنائية والمتعددة الأطراف، مثل اتفاقية بودابست بشأن الجرائم الإلكترونية والتي تسهل تبادل المعلومات والأدلة الرقمية بين الدول، و علاوة على ذلك يجب على المشرع تعزيز آليات المساعدة القانونية المتبادلة وتفعيل دور الإنتربول والمنظمات الدولية الأخرى في تتبع الأدلة الرقمية عبر الحدود؛ مما يضمن عدم إفلات مرتكبي الجرائم السيبرانية من العقاب وأخيرًا يجب أن تكون هناك رقابة صارمة على العقود المبرمة مع المعالجين الخارجيين للتأكد من أنها تتضمن بنوداً صريحة حول المسؤولية والإجراءات الواجب اتباعها في حال وقوع خرق للبيانات، مع تحديد الاختصاص القضائي المناسب لحل النزاعات[2].

---

[1] المادة رقم (39) من اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بالقرار الوزاري رقم 34 / 2024.

[2] سامح عبد الواحد التهامي، المرجع السابق، ص 32.

ثانيًا– تحديات إثبات الجرائم المتعلقة ببيانات الأطفال:

يولي قانون حماية البيانات الشخصية العماني ولائحته التنفيذية أهمية خاصة لحماية بيانات الأطفال لكن تطبيق هذه الحماية قضائيًا يواجه تحديات كبيرة فالمادة (6) من قانون حماية البيانات الشخصية والتي تنص على " يحظر معالجة البيانات الشخصية للطفل إلا بموافقة ولي أمره، ما لم تكن تلك المعالجة لمصلحة الطفل الفضلى، وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة"[1]، والمادة (11) من اللائحة التنفيذية والتي تنص على "... ويجوز للمتحكم أو المعالج – بحسب الأحوال – أن يطلب من الطفل الحد الأدنى من بيانات ولي أمره، وذلك بغرض التحقق من هويته والحصول على موافقته"[2].

بناء على ما سبق إيضاحه "المادة 11 من قانون البيانات الشخصية، المادة 6 من لائحة التنفيذية" يرى الباحث أن المادتين تحظران معالجة بيانات الطفل إلا بعد الحصول على الموافقة الصريحة من ولي أمره ما لم تكن المعالجة لمصلحته الفضلى وهنا يبرز التحدي القضائي في كيفية التحقق من سن صاحب البيانات الشخصية ففي بيئة الإنترنت قد يقوم الأطفال أو المراهقون بتقديم بيانات غير صحيحة عن أعمارهم لتجاوز القيود المفروضة وفي هذه الحالة هل يمكن تحميل المتحكم المسؤولية الجزائية؟ لذلك يتطلب الأمر إثبات أن المتحكم كان يعلم أن صاحب البيانات طفل ولكنه قام بمعالجتها دون موافقة ولي أمره وهو ما يمثل تحديًا إجرائيًا كبيرًا فكيف يمكن إثبات هذا العلم اليقيني؟ كما أن اللائحة التنفيذية للقانون لم تحدد آلية واضحة للتحقق من العمر أو لتوثيق موافقة ولي الأمر مما يترك الباب مفتوحًا للجدل القانوني بالإضافة إلى ذلك قد يكون من الصعب على القضاء تحديد ما إذا كانت المعالجة لمصلحة الطفل "الفضلى" أم لا حيث أن هذا المفهوم قد

---

[1] المادة رقم (6) من قانون حماية البيانات الشخصية العماني الصادر بالمرسوم السلطاني رقم 6 / 2022.

[2] المادة رقم (11) من اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بالقرار الوزاري رقم 34 / 2024.

يكون فضفاضًا ويخضع لتفسيرات مختلفة وهذه العوامل مجتمعة تجعل من قضايا انتهاك بيانات الأطفال معقدة قضائيًا وتتطلب أدلة قوية لا تتوفر دائمًا.

و لمواجهة تحديات حماية بيانات الأطفال يجب على المشرع والقضاء إيجاد حلول عملية لثغرات التحقق من العمر وإثبات "العلم اليقيني" لدى المتحكم كما يمكن للمشرع أن يحدد آليات التحقق من العمر بشكل أكثر دقة في اللائحة التنفيذية مثل إلزام المتحكم باستخدام تقنيات التحقق الموثوقة التي لا تعتمد فقط على إقرار الطفل بعمره وتقديم قائمة بالوثائق المقبولة أو استخدام تقنيات التحقق الإلكتروني المتاحة التي تضمن حماية خصوصية الطفل كما يمكن للقضاء أن يطور تفسيرًا لمفهوم "العلم اليقيني" بما يتجاوز مجرد المعرفة المباشرة؛ ليشمل "العلم المفترض" في الحالات التي لا يتخذ فيها المتحكم الإجراءات المعقولة للتحقق من عمر المستخدم خاصةً عندما يكون محتوى الموقع أو التطبيق موجهاً للأطفال أو يجذبهم بالإضافة إلى ذلك يجب أن يوضح القانون بشكل أكبر مفهوم "مصلحة الطفل الفضلى" من خلال وضع معايير واضحة وقابلة للقياس مثل أن تكون المعالجة ضرورية لتقديم خدمة تعليمية أو صحية أساسية للطفل وأن لا تنطوي على أي مخاطر قد تضر به، مما يقلل من الجدل القضائي ويساعد على تحقيق الحماية الفعّالة لبيانات الأطفال[1].

ثالثًا– تكامل الدليل الرقمي مع الدليل التقليدي في إثبات جرائم البيانات الشخصية:

أحد أبرز التحديات التي يواجهها المشرع والقضاء هو مواكبة التطور التقني السريع في عالم جرائم البيانات الشخصية مما يجعل القوانين عرضة للتقادم بسرعة[2]، و هذا الواقع يضع القاضي في موقف يتطلب

---

[1] سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم على الرابط الإلكتروني التالي:
https://ju.edu.sa/ar/personal-data-protection-policy-children-and-those-similar-conditions تاريخ الزيارة 22أغسطس 2025.

[2] عبد القادر كمال، محمد نور الدين، المرجع السابق، ص267.

منه المواءمة بين الدليل التقليدي والدليل الرقمي وفي حال وجود تعارض جوهري بين الدليلين وكان الدليل الرقمي مخالفًا للواقع فإن للمحكمة أن تستبعد الدليل المخالف[1]، وقد سارت على هذا المبدأ محكمة التمييز الأردنية في أحد أحكامها التي أكدت على أن المحكمة قد تستبعد الدليل الرقمي إذا كان مخالفًا للوقائع الثابتة[2]، كما أن المحكمة غالبًا ما تهتدي بما يؤكده الخبير باعتبار ذلك دليلًا علميًا وفنيًا[3]، وفي هذا السياق أكدت المحكمة العليا العمانية في أحد مبادئها على أن لمحكمة الموضوع كامل السلطة في تقدير القوة التدليلية لعناصر الدعوى، وهي الخبير الأعلى في كل ما تستطيع أن تفصل فيه بنفسها ولكن متى تعرضت لرأي الخبير الفني في مسألة فنية بحتة فإنه يتعين عليها أن تستند في تفنيده إلى أسباب فنية تحملها لا أن تحل محل الخبير فيها[4]، من وجهة نظر الباحث أن هذا التكامل بين الدليلين يعزز من حجية الدليل الرقمي ويؤثر على قناعة القاضي لتحقيق العدالة.

و لمواجهة تحديات التحقيق في الجرائم السيبرانية يتعين على المشرع والقضاء أن يتبنى نهجاً متكاملاً يمزج بين الدليل الرقمي والدليل التقليدي مع إعطاء الأولوية للدليل الرقمي باعتباره العنصر الأقوى في إثبات هذه الجرائم و يجب أن يتم توفير التدريب المستمر للقضاة والمدعين العامين للتعرف على طبيعة الأدلة الرقمية وكيفية التعامل معها وتأسيس وحدات متخصصة للتحقيق في الجرائم المعلوماتية[5]، كما أن على المحكمة أن

---

[1] فريد ناشف، بحث بعنوان مدى قبول الدليل غير المشروع في المحاكمة الجزائية، دراسة مقارنة، عدد الخامس عشر، دورية دراسات قانونية الصادرة عن مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، دار الخلدونية للنشر والتوزيع، 2012، الجزائر، ص 145.

[2] قرار محكمة التمييز الأردنية بصفتها الجزائية رقم (2764) / 2020.

[3] عبد القادر كمال، محمد نور الدين، المرجع السابق، ص268.

[4] طعن رقم 41 لسنة 2017، الدائرة الجزائية (أ) جلسة يوم الثلاثاء الموافق: 17/10/2017م.

[5] عبد القادر كمال، محمد نور الدين، المرجع السابق، ص269.

تولي أهمية قصوى لآراء الخبراء الفنيين وأن لا تستبعد الدليل الرقمي إلا في حال وجود تعارض جوهري مع وقائع الدعوى الثابتة بأدلة أخرى لا تقبل الشك مع ضرورة تبرير قرارها بأسباب فنية مقنعة[1]، هذا النهج يضمن أن الدليل الرقمي لن يتم استبعاده بشكل تعسفي ويعزز من قوته الإثباتية مما يؤدي إلى تحقيق العدالة في قضايا البيانات الشخصية[2].

في ختام هذا الفصل نجد أن التطور الهائل في الإنترنت وتكنولوجيا المعلومات قد فرض تحديات جذرية على المنظومات القانونية التقليدية مما استدعى من المشرعين إعادة صياغة مفاهيم الجريمة وأركانها لمواكبة الأفعال الإجرامية المستحدثة، وقد بيّنّا كيف أن المشرع العُماني قد استجاب لهذه التحديات من خلال إصدار تشريعات متخصصة، مثل قانون مكافحة جرائم تقنية المعلومات وقانون حماية البيانات الشخصية، كما تناولنا مظاهر هذه الجرائم بدءًا من تلك التي تستهدف النظم المعلوماتية بشكل مباشر وصولاً إلى تلك التي تُرتكب عبر استغلال الاتصالات الرقمية مع التركيز على جرائم مثل السرقة التقنية والاعتداء على البرامج المعلوماتية والتهديد في الفضاء الرقمي، وتوضح هذه الجهود التشريعية الحاجة المستمرة لوضع أطر قانونية مرنة وفعالة قادرة على حماية الأفراد والمجتمع من الأضرار المتزايدة لهذه الجرائم في العصر الرقمي.

---

[1] قرار محكمة التمييز الأردنية بصفتها الجزائية رقم (2764) / 2020.

[2] فريد ناشف، المرجع السابق، ص 147.

الخاتمة

تناولت هذه الدراسة بشكل عميق ومفصل الحماية الجزائية للبيانات الشخصية في الفضاء الرقمي مع التركيز بشكل خاص على الأطر التشريعية في كل من سلطنة عمان والمملكة الأردنية الهاشمية، و لقد كشفت الدراسة عن حقيقة لا يمكن تجاهلها وهي أن التطور التكنولوجي السريع وغير المسبوق والذي أدى إلى تحول مجتمعاتنا إلى مجتمعات رقمية، تعتمد بشكل كلي على المعلومات والبيانات قد خلق بيئة جديدة تبرز فيها الحاجة الملحة لوضع تشريعات صارمة وواضحة تضمن حماية خصوصية الأفراد؛ حيث أن البيانات الشخصية لم تعد مجرد معلومات عابرة، بل أصبحت ثروة حقيقية ووقودًا للاقتصاد الرقمي مما جعلها هدفًا رئيسيًا للعديد من الجهات سواء كانت أفرادًا يسعون للاستغلال غير المشروع أو مؤسسات تسعى لتحقيق مكاسب تجارية، وفي ظل هذا الواقع الجديد أظهرت الدراسة أن التهديدات التي تواجه هذه البيانات تتطور باستمرار وتتخذ أشكالاً معقدة بدءًا من الاختراق وسرقة البيانات وصولاً إلى بيعها في السوق السوداء والاستخدام غير المصرح به، و هذه التحديات المتجددة تتطلب استجابة قانونية مرنة وديناميكية مما يؤكد على ضرورة التحديث المستمر للإطار القانوني لمواكبة هذه التحديات وعدم ترك أي ثغرات يمكن استغلالها.

بالإضافة إلى ذلك سلطت الدراسة الضوء على الجانب الأخلاقي والمسؤولية الاجتماعية للمشرعين والجهات الحكومية في حماية هذا الحق الأساسي، و إن الحق في الخصوصية وحماية البيانات الشخصية ليس مجرد بند قانوني بل هو حجر الزاوية في بناء مجتمع آمن وموثوق في العصر الرقمي عندما يثق الأفراد بأن بياناتهم في مأمن فإنهم يشاركون بشكل أكبر في الاقتصاد الرقمي، مما يدعم النمو الاقتصادي والابتكار لذلك فإن المسار الذي تسلكه الدول العربية مثل سلطنة عمان والأردن في إقرار قوانين الجرائم المعلوماتية هو خطوة في الاتجاه الصحيح، ومع ذلك فإن هذه الخطوة تتطلب المزيد من التعميق والتفصيل لضمان أن تكون هذه

القوانين شاملة وقابلة للتطبيق العملي على أرض الواقع، وأن تكون قادرة على فرض عقوبات رادعة بحق مرتكبي هذه الجرائم، وإن الحماية الفعالة للبيانات الشخصية تتطلب تضافر الجهود بين الجهات التشريعية والتنفيذية والأفراد أنفسهم من خلال التوعية وبناء القدرات والتعاون الدولي.

النتائج:

بناءً على التحليل القانوني للتشريعات والممارسات القضائية في كل من سلطنة عمان والأردن توصل الباحث إلى النتائج القانونية التالية:

1- توصَّل الباحث إلى أنَّ قانون حماية البيانات الشخصية العُماني وتحديداً المادة 11 الفقرة (هـ) يُقرُّ بحق الأفراد في طلب حذف بياناتهم؛ مما يؤكد على مبدأ التحكم الفردي بالبيانات ومع ذلك يوازن القانون بين هذا الحق والمصلحة العامة من خلال وجود استثناءات تسمح بالاحتفاظ بالبيانات لأغراض التوثيق الوطنية أو لأسباب قانونية أخرى، وهذا التوازن يعكس توجه المشرع العُماني نحو حماية حقوق الأفراد مع الحفاظ على الأرشيفات والسجلات ذات الأهمية الوطنية.

2- أظهرت الدراسة أن هناك اتفاقًا بين المشرّعين العُماني والأردني في إرساء إطار قانوني واضح لحماية البيانات الشخصية ويتجلّى هذا الاتفاق في توحيد تعريفات المفاهيم الأساسية مثل "المُعالِج" و "المعالجة"؛ مما يعكس التزامًا مشتركًا بضبط عمليات معالجة البيانات.

3- تواجه الأجهزة الأمنية والقضائية تحديات كبيرة في إثبات الجرائم المتعلقة بالبيانات الشخصية وطبيعة الأدلة الرقمية (سرعة زوالها، سهولة تزويرها، وصعوبة تتبعها) تتطلب آليات إجرائية متطورة ووجود خبراء متخصصين في الأدلة الجنائية الرقمية، وهو ما لا يتوفر دائمًا بشكل كافٍ.

4- على الرغم من وجود عقوبات جزائية إلا أنها في بعض الأحيان قد لا تكون رادعة بما يكفي لجرائم البيانات الشخصية كما أن عدم وعي الضحايا بحقوقهم القانونية أو الإجراءات اللازمة لتقديم الشكوى يقلل من عدد القضايا المرفوعة؛ مما يساهم في إفلات الجناة من العقاب.

5- إن القوانين المحلية غير كافية لمكافحة الجرائم المعلوماتية التي تمتد عبر الحدود الوطنية وهناك نقص في آليات التعاون القضائي الدولي واتفاقيات تسليم المجرمين وتبادل المعلومات؛ مما يجعل من الصعوبة بمكان ملاحقة مرتكبي هذه الجرائم الذين يعملون من خارج الحدود الإقليمية للدولة.

التوصيات:

بناءً على النتائج التي توصل إليها الباحث يوصي بما يلي:

1- نناشد المشرع العُماني بالاستفادة من النموذج الأردني الرائد في تنظيم حماية البيانات الشخصية الذي يقدم إطاراً تشريعياً متكاملاً يتميز بكونه إطاراً متقدماً يوفر حماية قوية تستند إلى مبادئ أساسية؛ حيث يشدد على ضرورة الحصول على الموافقة المستنيرة، ويضمن بشكل كامل حقوق أصحاب البيانات، ويطبقها عبر آليات رقابية ذات كفاءة.

2- نوصي بضرورة إطلاق حملات توعية وطنية مستمرة تهدف إلى زيادة وعي الأفراد بأهمية حماية بياناتهم الشخصية، وتقديم إرشادات حول كيفية تأمينها على الإنترنت.

3- نوصي بضرورة تدريب وتأهيل القضاة وأعضاء الإدعاء العام والمحققين الجنائيين على الجوانب الفنية والقانونية للجرائم المعلوماتية، ويشمل ذلك فهم طبيعة الأدلة الرقمية وكيفية جمعها وتحليلها بشكل صحيح ومقبول أمام القضاء.

4- نوصي بضرورة انضمام عُمان إلى الاتفاقيات والمعاهدات الدولية لمكافحة الجرائم الإلكترونية مثل اتفاقية بودابست، كما ندعو إلى تعزيز آليات التعاون القضائي وتبادل المعلومات مع الدول الأخرى مما يسهل ملاحقة مرتكبي الجرائم العابرة للحدود.

5- نوصي بضرورة تشريعات تلزم المؤسسات والشركات سواء كانت خاصة أو عامة بتبني سياسات فعالة لحماية البيانات الشخصية، ومن المهم أن تتضمن هذه السياسات مبادئ "الخصوصية حسب التصميم" و"الخصوصية بشكل افتراضي" مع إجراء تقييمات دورية للمخاطر الأمنية.

المراجع

أولًا- المراجع العامة:

1. أحمد بدر، علم المكتبات والمعلومات دراسات في النظرية والارتباطات الموضوعية، الطبعة الأولى، دار الغريب، القاهرة، مصر، 1996.
2. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الاسكندرية، مصر، 2006.
3. أيمن عبد الله فكري، جرائم نظم المعلومات "دراسة مقارنة"، دار الجامعة الجديدة للنشر والتوزيع، 2007.
4. حنان ريحان مبارك المضحكى، الجرائم المعلوماتية" دراسة مقارنة"، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014.
5. رجاء عايد الخلايلة، المسؤولية التقصيرية الالكترونية "دراسة مقارنة"، درا الثقافة لنشر والتوزيع، 2011.
6. رشيدة بوبكر، الحماية الجزائية للتعاملات الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012.
7. عايد رجاء الخلايله، المسؤلية التقصيرية الإلكترونية "المسؤلية الناشئة عن إساءة استخدام اجهزة الحاسوب والانترنت"، دراسة مقارنة، دار الثقافة للنشر والتوزيع، 2011.
8. عبد الرزاق السنهوري، الوجيز في شرح القانون المدني الجزء الأول" نظرية الالتزام بوجة عام"، الطبعة الثانية، دار النهضة العربية، القاهرة، 1997.
9. عبد القادر الفار، مصادر الالتزام" مصادر الحق الشخصي في القانون المدني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006.
10. عدنان السرحان، نوري خاطر، شرح القانون المدني" مصادر الحقوق الشخصية " دار الثقافة، عمان، الأردن، 2005.

11. لينا ابراهيم يوسف حسان، التوثيق الألكتروني ومسؤولية الجهات المختصة به " دراسة مقارنة "، الطبعة الأولى، دار الراية للنشر والتوزيع، الجيزة، مصر، 2009.

12. محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي، مطبوعات جامعة الكويت، إبريل 1992.

13. محمد عبيد الكعبي، الجرائم الناشئة عن استخدام غير المشروع لشبكة الإنترنت "دراسه مقارنة"، الطبعة الثانية، دار النهضة العربية للنشر، القاهرة، مصر، 2009.

14. محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، القاهرة، مصر، 2018.

15. محمد فهمي طلبه وآخرون، فيروسات الحاسب وأمن البيانات، المكتب المصري الحديث، القاهرة، مصر.

16. محمود حسن إسماعيل، مبادئ علم الاتصال ونظريات التأثير، الطبعة الرابعة، الدار العالمية للنشر والتوزيع، القاهرة، مصر،2004.

17. نعيم مغبغب، مخاطر المعلوماتية والإنترنت المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن، بيروت، لبنان، 2000.

18. نهلا عبد القادر المؤمني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008.

19. وليد رمضان عبد الرازق محمود، ضوابط جمع ومعالجة البيانات الشخصية في ظل الإدارة الإلكترونية، كلية الحقوق جامعة بنى سويف، مصر

20. يونس عرب، المخاطر التي تهدد الخصوصية وخصوية المعلومات في العصر الرقمي اتحاد المصارف العربية، الطبعة الأولى، 2002.

ثانيًا– المراجع المتخصصة:

1. باسل فايز حمد القطاطشة، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية: دراسة مقارنة، جامعة العلوم الإسلامية العالمية، عمان، 2022.

2. جمال موراي، حق الأفراد في حماية بياناتهم الشخصية وفقاً لقانون حماية البيانات الشخصية، موسوعة حماة الحق، الأردن 19 ديسمبر، 2023

3. حبيبة سيف سالم راشد الشامسي، حماية البيانات الشخصية في ضوء القانون الاتحادي رقم 45 لسنة 2021: بحث، مجلة الأمن والقانون، المجلد 31، العدد 1، 2023.

4. سيد أحمد محمود أحمد، حماية البيانات الشخصية الرقمية وفقا لأحكام القانون المصري رقم 151 لسنة 2020: حماية البيانات الشخصية المعالجة الكترونيا بين الواقع والمأمول، مجلة العلوم القانونية والاقتصادية، المجلد 66، العدد 1، 2024.

5. ضرغام عبد الله فاضل، حماية بيانات الأفراد الشخصية عبر الإنترنت "دراسة مقارنة"، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، 2021.

6. عثمان بكر عثمان، المسؤلية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2013.

ثالثاً–المقالات والأبحاث المنشورة:

1. إبراهيم الدسوقي أبو الليل، التعاقد عبر الوسائل الاتصال الحديثة، الطبعة الثالثة، الملجلد الثالث، بحث منشور ضمن أعمال مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المنعقد في الفترة من 1–3 مايو 2000.
2. إيمان أحمد على طه، الحماية التشريعية للحق في خصوصية البيانات في العصر الرقمي، جامعة الأزهر، الجزء الثالث، العدد السادس والثلاثون، 2021.
3. سامح عبد الواحد التهامى، الحماية القانونية للبيانات الشخصية " دراسة القانون الفرنسي"، القسم الأول، مجلة الحقوق، جامعة الكويت، مج35، ع 11، 2011.
4. سامح عبد الواحد التهامي، المسؤولية المدنية عن فيرسة النظم المعلوماتية عبر الانترنت، مجلة الحقوق، جامعة الكويت، المجلد 40، العدد الثالث، 2016.
5. عائشة بن قارة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث، المجلد الثاني، العدد الخامس، يونيو 2016.
6. عبد الفتاح بيومي حجازي، التوقيع الألكتروني في النظام القانوني المقارن، دار الفكر الجامعي، الإسكندرية، مصر.
7. عبد القادر كمال، محمد نور الدين، أثر مبدأ المشروعية في حجية الدليل الجزائي في القانون الجزائري، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، العدد الأول، المجلد الرابع عشر، جامعة معسكر، الجزائر، 2017.

8. علاء عيد طه، الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية، مجلة كلية الحقوق والعلوم السياسية، جامعة الملك سعود، مجلد 32، 2016.

9. فريد ناشف، بحث بعنوان مدى قبول الدليل غير المشروع في المحاكمة الجزائية، دراسة مقارنة، عدد الخامس عشر، دورية دراسات قانونية الصادرة عن مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، دار الخلدونية للنشر والتوزيع، 2012، الجزائر.

10. محمد عرفان الخطيب، ضمانات الحق في العصر الرقمي من تبدل المفهوم لتبدل الحماية، قراءة في الموقف التشريعي الأوروبي والفرنسي وإسقاط على الموقف التشريعي الكويتي، بحث منشور على مجلة كلية القانون العالمية، أبحاث المؤتمر السنوي الدولي الخامس من 9 – 10 مايو 2018، الكويت، ملحق خاص العدد 3، الجزء الأول، 2018.

11. محمد علي مقراش، حجية أدلة الاثبات أمام القاضي الجزائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2019.

رابعاً– الرسائل والأطروحات:

1. عبد السلام أحمد خلف العرمان، الحماية الجزائية للبيانات الشخصية في التشريع الأردني دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، عمان.
2. كنده الشماط، الحق في الحياة الخاصة، رسالة لنيل درجة الدكتوراه في الحقوق، جامعة دمشق، سوريا،2004–2005.
3. محمد رشيد حامد، الحماية الجزائية للمعلومات الشخصية في مواجهة أخطار البنوك، رسالة ماجستير، كلية الحقوق، جامعة آل البيت، عمان، الأدرن.

الفهرس