جامعة الإسراء
ISRA UNIVERSITY

نطاق الحماية الجزائية للبيانات الشخصية الالكترونية في القانون الأردني

أعدت من قبل

فلاح محمد داود دويكات

أشرف عليها

الدكتور: محمد سالم الشاهين

قدمت هذه الرسالة إلى كلية الحقوق كجزء من مُتطلبات الحصول على درجة الماجستير في القانون العام

كانون الثاني 2024

جامعة الإسراء
ISRA UNIVERSITY

التفويض

أفوض انا الطالب: **فلاح محمد داود دويكات** أفوض جامعة الاسراء بتزويد نُسخ من رسالتي، للمكتبات أو المؤسسات أو الهيئات أو الأشخاص عند طلبها.

التوقيع:

التاريخ: 28 / 1 / 2024

Isra University

I am the student: Falah Mohammad Dawod Dwikat I authorize Al-Isra University to provide copies of my thesis to libraries, institutions, bodies, or individuals upon their request, according to the instructions in force at the university.

Signature: .....

Date:. 28 / 1 / 2024

جامعة الإسراء
ISRA UNIVERSITY

نموذج (4) صفحة لجنة المناقشة

نوقشت هذه الرسالة (نطاق الحماية الجزائية للبيانات الشخصية الالكترونية في القانون الأردني)

وأجيزت بتاريخ 21/ 1 /2024.

أعضاء لجنة المناقشة:

اسم العضو	التوقيع
الدكتـــور: محمد سالم الشاهين / رئيساً ومشرفـــاً	.....
الأستاذ الدكتور: أكرم طراد القايز/ عضواً داخليـــاً	.....
الدكتـــور: منير محمد العفيشات / عضواً خارجيـاً	.....

شكر وتقديـــــــــر

الحمدُ لله الذي وهبني برحمته القوة والعزيمة، والثبات إلى أن أنجزتُ هذه الرسالة، لك الحمدُ يا الله حمداً يليقُ بجلال وجهك وعظيم سلطانك، حمداً دائماً يدوم بدوامك لا يبيد، والصلاة والسلام على رسول الله محمد صلى الله عليه وسلم، وبعد، فلا يسعني، وقد انتهيت من إعداد هذه الرسالة إلا أن أردّ الفضل إلى أهله فإنني أتقدم بجزيل الشكر والعرفان إلى مشرفي، **الدكتور: محمد سالم الشاهين** الذي كان لي المعلم والمرشد، وقدم لي ما يملكهُ من الخبرة والمعرفة التي احتاجها، فأعطاني من وقته الكثير، وسعدت بصحبته، وتشرفت بالعمل معه، واستفدت من علمه، فكان لنصائحه وملاحظاته السديدة أكبر الأثر في إتمام هذا العمل.

كما، وأتقدم بالشكر والتقدير إلى الأساتذة الأفاضل لجنة المناقشة لتفضلهم بقبول مناقشة رسالتي.

وأتقدم بعظيم الشكر لأخي وصديقي والمحامي لؤي زعل الشرايعة، والأستاذ فادي الزيود الذي قدم لي يد العون والمساعدة ووقوفه إلى جانبي طيلة فترة الدراسة.

وختامًا شكري وتقديري العالي إلى جامعتي العزيزة، جامعة الإسراء بمنتسبيها جميعهم، وأساتذتي الأعزاء في كلية الحقوق، وزملائي الطلبة الأعزاء الذين غمروني بفضلهم ومحبتهم، والى الأخوة والأصدقاء جميعهم الذين دعموني معنويًا، وشجعوني على إكمال رسالتي.

الباحث

فلاح محمد داود دويكات

الأهداء

أهدي ثمرة هذا الجهد البسيط إلى ...

إلى أمي نبع الحنان . . التي استمدت قوتي من بركة دعائها

إلى أبي الذي قضى حياته في مساندتي ووصولي إلى هذه المرحلة

إلى سندي . . .إخوتي وأخواتي

إلى زوجتي الغالية

إلى أهل الفضل علي الذين غمروني بالحب والتقدير وقدموا لي النصح والتوجيه والإرشاد

أساتذتي

الباحث

فلاح محمد داود دويكات

فهرس المحتويات

جامعة الإسراء
ISRA UNIVERSITY

نطاق الحماية الجزائية للبيانات الشخصية الإلكترونية في القانون الأردني

أعدت من قبل

فلاح محمد داود دويكات

أشرف عليها

الدكتور: محمد سالم الشاهين

الملخص

هدفت الدراسة الحالية إلى معرفة نطاق الحماية الجزائية للبيانات الشخصية الإلكترونية في القانون الأردني؛ حيث يرتبط المفهوم القانوني للبيانات ذات الطابع الشخصي للضحايا الذين وقعت عليهم جريمة انتهاك بياناتهم الشخصية من خلال التكنولوجيا بالعناصر المحددة الخاصة بهم؛ كالهوية الشخصية (الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية)، بحيث يعد انتهاك البيانات ذات الطابع الشخصي في المفهوم القانوني جريمة إلكترونية يعاقب عليها القانون، لذا بين الباحث في دراسة الحالية في الفصل الأول البيانات الشخصية ومعالجتها ونطاق حمايتها فيما يخص تحديد هوية الضحية، وشروط الحصول على البيانات ذات الطابع الشخصي والآثار المترتبة على معالجتها وأثرها على الخصوصية، كما تناول الباحث في الفصل الثاني نطاق الحماية الجزائية للبيانات الشخصية من خلال بيان صور الجرائم الواقعة على البيانات الشخصية وفقًا لقانون الجرائم الإلكترونية الحالي؛ كالبوصلة التقنية المعروفة بالكوكيز، والتصيد الاحتيالي الإلكتروني، وسرقة هوية الشخص، وتناول الباحث في المقابل العقوبات الجزائية لانتهاك حرمة البيانات الشخصية المنفذة تكنولوجيا والتي شملت عقوبة الدخول قصداً إلى الشبكة المعلوماتية، وعقوبة استخدام وسيلة إلكترونية للضرر بالبيانات وعقوبة الدخول دون تصريح للبيانات وذلك بالرجوع إلى قانون العقوبات الأردني رقم (16) لسنة (1960)، وقانون الجرائم الإلكترونية رقم (17) لسنة (2023)، وقانون الاتصالات رقم (15) لسنة (1995) وتعديلاته حتى عام (2023). وقانون المطبوعات والنشر الأردني وتعديلاته حتى عام (2023)، والاتفاقية الأوروبية لحقوق الإنسان. وتوصل الباحث إلى أن المشرع الأردني أيد في نص المادة (2) من قانون حماية البيانات الشخصية لسنة (2023) على سلامة البيانات، وعلى الدور الرئيس لمجلس الوزراء فيما يخص شروط الإفصاح عن هذه البيانات، ولكنه لم يحدد نطاق الحماية الجزائية فيما يخص المعطيات التي ترتبط بالبيانات الشخصية–كل على حدة–مثل: (رقم الجوال، وعنوان البريد الإلكتروني، ورقم بطاقة الائتمان، والبيانات الشخصية: (الصوت، وبصمات الأصابع، والحمض النووي، والبيانات البيومترية للضحايا). كما لم يحدد المشرع الأردني في قانوني الجرائم الإلكترونية والاتصالات الحاليين نصوصًا تتعلق بجريمة البطاقات، وجريمة الوصول إلى عنوان (IP) للضحية، كما لم يشر هذين القانونين إلى مصطلحيّ البوصلة التقنية المعروفة "بالكوكيز"[1]، والتصيد الاحتيالي الإلكتروني[2].

---

[1] البوصلة التقنيّة (الكوكيز) هي: ملف موجود على الفرص الصلب الخاص بحاسوب الضحية يبين الموقع الإلكتروني الذي أرسل له الضحية رسالة، ويحتفظ بنسخة من هذه الرسائل لديه (عنوان IP).

[2] التصيد الاحتيالي الإلكتروني: التقنيات التي يستخدمها الهاكرز من أجل جمع المعلومات الشخصية عن مستخدمي الإنترنت. *سيوضحهما الباحث في رسالته.

الفصل الأول

الإطار العام للدراسة

المقدمة:

إن حماية حقوق الأفراد داخل المجتمع سواء أكانت هذه الحقوق مادية أم حقوق معنوية، هي من أهم الحقوق التي ضمنها القانون الأردني، والتي لم يتركها للأفراد أنفسهم لأنه وضع قواعد قانونية تنظم العلاقات جميعها؛ حماية لهذه الحقوق، ومنعًا للإعتداء عليها، إذ أنه لم يعد من المقبول الاعتداء على حقوق المواطن الأردني، خاصة أن القواعد القانونية الجزائية اعتبرت هذا الفعل جريمة يعاقب عليها، حيث وضع المشرع الأردني قواعداً قانونية للمسؤولية العقدية لحماية هذه الحقوق، كما وضع قواعداً أخرى لحماية الحقوق الناشئة عن المسؤولية التقصيرية.

وتعد حماية البيانات الشخصية الإلكترونية متطلب أساسي لمعالجة كثير من الاختلالات القائمة والمزعجة للأفراد من خلال سهولة الحصول على بياناتهم الشخصية واختراقها من قبل عدة جهات وأفراد، واستخدامها على نحو غير لائق، وإمكانية التلاعب بها لتحقيق مكاسب غير مشروعة أو إيقاع مشكلات اجتماعية متعددة، سهلتها البرامج الإلكترونية التي تناولها قانون الجرائم الإلكترونية رقم (17) لسنة (2023) من حيث كونها: (مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات أو أي وسيلة من وسائل تقنية المعلومات).

خاصة أن قانون الاتصالات الأردني رقم (13) لسنة (1995) وتعديلاته ركز في المادة (65/ب) على احترام حقوق المواطن الأردني: (لا يجوز نشر أو إشاعة مضمون الرسائل التي تم التقاطها في معرض تتبع مصدر الرسالة بموجب الفقرة (أ) من هذه المادة، ويعاقب الموظف الذي يقوم بنشر أو إشاعة مضمون تلك الرسائل بالعقوبات المقررة قانونًا).

وتعد جريمة اختراق البيانات الشخصية من الأفعال الضارة، لإرتباطها بحقوق الأفراد وسلامتهم، وحقهم بالحياة الكريمة داخل المجتمع، ولقد ازدادت أهمية البيانات الشخصية مع التقدم التكنولوجي والذي أدى إلى تنوع أشكال الجريمة، وإلى زيادة أضرارها النفسية والمادية والاجتماعية، وعلى الرغم من أن التعويض المادي للضرر لا يؤدي إلى محو الآلام النفسية والاجتماعية التي حدثت للضحايا بسبب انتهاك بياناتهم الشخصية، إلا أنه يعد وسيلة رادعة للجناة، وتعويضية للضحايا.

حيث أن والأصل أن تكون البيانات الشخصية محمية، والاطلاع عليها واستخدامها من قبل الغير عمل مُجرم في قانون العقوبات وغيره من التشريعات ذات العلاقة، وبالتالي لا يجوز التصرف بها بأي حال من الأحوال.

وعلى الرغم من أن اقتحام خصوصية الآخرين وبياناتهم الشخصية يعد عملاً غير مقبول ومرفوض، إلا أن انتهاك البيانات الشخصية في ارتفاع مستمر، لذا جاءت الدراسة الحالية لمناقشة هذا النوع الجديد من الجرائم الإلكترونية من خلال نطاق الحماية الجزائية لها في القانون الأردني.

مشكلة الدراسة:

إن المشكلة الرئيسة التي سنتناولها ونعالجها في دراستنا هذه تتمحور في مدى كفاية النصوص التشريعيه الواردة في قانون الجرائم الالكترونية الاردني، وقانون الاتصالات، وقانون العقوبات الاردني، في توفير الحماية الجنائية للبيانات الشخصية وهل وفقت التشريعات والنصوص القانونية في إقرار حماية البيانات الشخصية؟ وما هي مظاهر الحماية الجنائية التي رصدها مشرعنا الأردني لحماية البيانات الشخصية في النصوص الخاصة؟ وتتفرع عن المشكلة الرئيسه التساؤلات الفرعية الآتية:

أسئلة الدراسة:

بالرغم من خطورة انتهاك البيانات الشخصية للأفراد كفعل جرمي؛ إلا أنه لم يتم تناوله بالتفصيل من قبل الدراسات السابقة، لذا حرص الباحث على صياغة الأسئلة وفق ما طرحته المشكلة بالشكل الجديد، وذلك على النحو الآتي:

1. ما هو الأساس القانوني لحماية البيانات الشخصية وطبيعتها القانونية؟
2. ما المقصود بالجرائم الواقعة على الأفراد من حيث بياناتهم الشخصية؟
3. ما هي الشروط الواجب توافرها لقيام المسؤوليه الجنائية في حالة الاعتداء على البيانات الشخصية، والجزاء المترتب على ذلك؟
4. كيف يكون دليل الإثبات أو النفي في جريمة انتهاك البيانات الشخصية؟
5. ما هي طرق إثبات الاعتداء على البيانات الشخصية، ودور القاضي الجزائي في ذلك؟
6. ما نطاق الحماية الجزائية لاختراق هذه البيانات في القانون الأردني؟

أهداف الدراسة:

تهدف هذه الدراسة لتحقيق ما يلي:

- بيان مفهوم البيانات الشخصية للانسان وماهيتها.
- بيان النصوص القانونيه التي يطبقها القضاء الأردني في حماية البيانات الشخصية، ومواطن القصور في معالجة هذه المشكلة المتطورة تكنولوجيًا، وتوصيته لما توصلت اليه الدراسة من نتائج وتوصيات، في سبيل تبني نصوص قانونية لحماية هذه البيانات الشخصية، والتي تدخل في أطار حرمة الحياة الخاصة، كما نسعى كذلك لإثراء المكتبة القانونية العربية في مجال حماية البيانات

الشخصية، كونه موضوعاً معاصراً، كما نسعى أيضًا إلى أن تكون هذه الدراسة بمثابة الطريق نحو مزيد من الأبحاث في مجال حماية البيانات الشخصية في ظل التطور العلمي المستمر.

أهمية الدراسة:

تكمن أهمية الدراسة في أنه نتيجةً للتطور التكنولوجي، والتقدم العلمي، وانتشار أجهزة الحواسيب الحديثة والمزودة بتقنيات وبرامج فائقة السرعة والأداء والدقة، ازدادت حالات انتهاك خصوصية الأفراد بشكل عام، وانتهاك حقه ببياناته الشخصيه بشكل خاص، لذلك عملت التشريعات على تسليط الضوء على حماية البيانات الشخصية للانسان، لتعدد وسائل انتهاك هذا الحق من خلال الاعتداء على البيانات أو نشرها بدون رضاه، أو حتى دون علمه، أو استخدامها في عمليات أو نشاطات غير مشروعة، مما قد يجعله محلاً للجريمة التي يعاقب عليها القانون.

الأهمية العملية:

حيث تبحث الدراسة الحالية في كيفية حماية البيانات الشخصية الإلكترونية للأفراد من خلال التشريعات الجزائية في الأردن، بحيث سيتم طرح اقتراحات واقعية بهذا الشأن والتي يجب إدخالها على النصوص الوضعية السارية المفعول لسد النقص والخلل الملاحظ في القانون المطبق على أرض الواقع.

الأهمية النظرية:

ستكون في نوع من المساهمة لغايات تبسيط النصوص القانونية ويكون ذلك من خلال توضيح مظاهر وصور انتهاكات البيانات الشخصية من خلال الوسائل الإلكترونية، وبيان كيف يؤدي انتهاك الحياة الخاصة إلى افشاء سرية الأفراد.

حدود الدراسة:

يتحدد نطاق ومضمون هذه الدراسة بالحدود الآتية:

الحدود المكانية:

تتمثل الحدود المكانية لهذه الدراسة داخل حدود المملكة الأردنية الهاشمية من خلال تحليل النصوص القانونية المتعلقة بحماية البيانات الشخصية الإلكترونية كونها تعتبر من الحقوق المرتبطة بحماية حياتهم الخاصة في قانون العقوبات الأردني رقم (16) لسنة (1960)، قانون الجرائم الإلكترونية رقم (17) لسنة (2023)، وقانون الاتصالات رقم (15) لسنة (1995) حتى (2023). وقانون المطبوعات والنشر الأردني وتعديلاته لعام(2023)، والاتفاقية الأوروبية لحقوق الإنسان.

الحدود الزمانية:

إن حدود الدراسة الزمانية تتمثل في معالجة جريمة الاعتداء على الحياة الخاصة منذ أن وضع قانون العقوبات الأردني رقم (16) لعام (1960)، قانون الجرائم الإلكترونية رقم (17) لسنة (2023)، وقانون الاتصالات رقم (13) لسنة (1995) حتى (2023).

الحدود الموضوعية:

تقتصر هذه الدراسة على بيان المفهوم القانوني للبيانات ذات الطابع الشخصي الإلكتروني للضحايا، العوائق (الإشكاليات) المرتبطة بجريمة انتهاك البيانات الشخصية إلكترونيًا، وصور الجرائم الواقعة على البيانات الشخصية وفقًا لقانون الجرائم الإلكترونية، وبيان الأساس القانوني لقيام المسؤولية الجزائية لجريمة انتهاك البيانات الشخصية، وبيان موقف المشرع الأردني من الوسائل الجرمية لانتهاكات البيانات الشخصية، وموقف المشرع الأردني من جريمة انتهاك الحياة الخاصة، وانتهاكات البيانات الشخصية كفعل ضار في قانون العقوبات الأردني.

التعريفات الاصطلاحية:

وردت في هذه الدراسة الاصطلاحات التالية:

- **البيانات الشخصية:** هي: (البيانات ذات الطابع الشخصي للضحايا المحددة الخاصة بهم؛ كالهوية الشخصية (الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية) التي تتعلق بالضحايا الطبيعيين الذين تم تحديد هويتهم بشكل مباشر، أو تم بشكل غير مباشر مثل عنوان (IP).[1].
- **الحياة الخاصة أو الخصوصية،** تُعرف على أنها: (الحيز المكاني أو الافتراضي الذي يشمل خصوصيات الأسرة وحرمة المساكن وسرية المراسلات والتي يحرص الفرد على حمايته ولا يبيح فيه صاحبه لأي شخص التواجد فيه أو الاطلاع عليه إلا بموافقته)[2].

---

[1] المناعسة، أسامة (2014). جرائم تقنية المعلومات الإلكترونية، دار الثقافة، الأردن، ص20

[2] حموري، شهد والمصري، ريم (2014). قانون حماية البيانات الشخصية الأردني، ما يمكن تعلمه من تجارب الدول الأخرى، مقالة منشورة على مدونة حبر، متاحة عبر الرابط الإلكتروني: www:7iber.com/wp-content/uploads/2016/01/Reem.pdf.، تمت الزيارة بتاريخ: 15-9-2023، الساعة 8:35 صباحًا.

- **التصيد الاحتيالي:** يُعرف على أنه: (التصيد الذي تستخدمة المواقع الإلكترونية التي تبدو بصورة شرعية لغايات الاستيلاء على أموال الضحايا عن طريق الكشف عن البيانات الشخصية الخاصة بهم من خلال بطاقة الائتمان أو معلومات البنك أو كلمات المرور) [1].
- **البوصلة التقنية (الكوكيز)**، تُعرف على أنها: (ملفات تعريفية نصية ارتباطية تحتوي على بيانات يتم إرسالها إلى المتصفح وتخزينها على الحاسب أو المحمول)[2].
- **الإنترنت:** (هي جزء من الانترنتو التي تمثل شبكة طرق واسعة من المواصلات السريعة التي تتكون من عدد كبير من شبكات الحاسب المترابطة والمتناثرة والتي تمل على ترابط المستندات والمعلومات بعضها ببعض، بحيث يستطيع المستخدم لها أن يتصفح هذه المستندات والاطلاع على المعلومات بحرية[3].
- **الشبكة المعلوماتية:** (وسيلة اتصال حديثة يمكن من خلالها نقل المعلومات الخاصة بالأفراد وتبادلها وتخزينها من خلال استخدام تقنيات متطورة أو وسائل كهربائية أو مغناطيسية أو ضوئية أو الكترومغناطيسية أو أي وسائل أخرى مشابهة[4].

---

(1) النوايسة، عبد الأله (2017). جرائم تكنولوجيا المعلومات، (ط1)، الأردن، دار وائل للنشر والتوزيع.

(2) عبد المجيد، محمود (2021). المجرم المعلوماتي وسلوكياته الإجرامية والأساليب المبتكرة في ارتكابه لجرائمه وسبل مواجهته، (ط1)، الإسكندرية، دار المطبوعات الجامعية، ص336.

(3) يوسف، يوسف (2011). الجرائم الدولية للإنترنت، (ط1)، المركز القومي للإصدارات القانونية، مصر، ص61,

(4) أبو عيسى، حمزة (2019). جرائم تقنية المعلومات، (ط2)، دار وائل للنشر، الأردن، ص136.

الدراسات السابقة ذات الصلة

لم يكن هنالك دراسات متخصصة في نطاق الحماية الجزائية للبيانات الشخصية الالكترونية في القانون الاردني، ولكن عمل الباحث من خلال إعداد هذه الدراسة على الإطلاع على العديد من الدراسات والأدبيات السابقة التي تناولت مواضيع مرتبطة بموضوع الدراسة كأمن المعلومات، وأشكال انتهاكها، والقوانين الدولية الخاصة بالمعلومات الشخصية عبر الإنترنت، وما كتب عن الموضوع، والتي عززت قدرة الباحث في التعرف إلى كيفية إعداد هذه الدراسة، وتحديد مشكلتها وأهدافها ومنهجيتها، ومن هذه الدراسات، والتي قام الباحث بترتيبها من الأحدث إلى الأقدم ما يلي:

- **دراسة ظاهر، سفيان (2023). الحماية الجزائية لصورة الانسان عبر الوسائل الالكترونية، دراسة مقارنة، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الزرقاء الخاصة، الزرقاء: الاردن.**

تناولت الدراسة حماية الصورة الشخصية للانسان عبر استخدامها غير المشروع او الالتقاط أو النشر أو الدوبلاج دون موافقة صاحب النشر أو ورثته، بأعتبارها حقاً من الحقوق اللصيقة بالشخصية الانسانية والتي يحرص عليها كل انسان من الاعتداء او انتهاك خصوصيته, وطرق إثبات الاعتداء، والنصوص القانونية الواردة في قانون العقوبات وقانون الاتصالات في حماية هذا الحق.

وتميزت الدراسة الحالية عن الدراسة السابقة في أنها تناولت البيانات الشخصية بشكل عام دون تفصيل أو تحديد هذه البيانات، وانصبت دراسة الباحث الحالية على حماية البيانات الشخصية في ظل قانون الجرائم الالكترونية.

- **دراسة السكر، سلطان فياض (2022). جريمة انتهاك سرية المعلومات عبر الوسائل الالكترونية في التشريع الأردني، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الاوسط، عمان ، الاردن.**

حيث تناولت الدراسة المعلومات الخاصة بالافراد، والاعتداء عليها عبر الوسائل الالكترونية، والحماية المقررة لتلك المعلومات الشخصية في قانون الجرائم الالكترونية الاردني.

وتميزت الدراسة الحالية عن الدراسة السابقة في أنها تناولت موضوع البيانات الشخصية وليست المعلومات، وبيان ماهيتها، وصور الاعتداء عليها، وطرق اثبات الاعتداء، والعقوبات المقررة للاعتداء على هذه البيانات في قانون الجرائم الالكترونية الاردني.

- **دراسة الزيود، فادي (2021)، جريمة الاعتداء على الحياة بالوسائل الإلكترونية في التشريع الأردني ومدى مواءمتها مع الاتفاقيات الدولية، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة عمان العربية، عمان: الاردن.**

حرص الباحث في الدراسة للوصول إلى تحقيق بعض من الأهداف كبيان مفهوم الحياة الخاصة في التشريع الجزائي والنصوص الجزائية الواردة فيه سيما في قانون العقوبات وقانون الجرائم الإلكترونية وقانون الاتصالات وبيان الحماية القانونية لحق الحياة الخاصة، إضافة لبيان مدى توافق التشريعات الجزائية الأردنية مع المواثيق الدولية التي انضمت إليها الأردن حول حماية حق الحياة الخاصة. ولما كانت خصوصية الفرد ترتبط ارتباطًا وثيقًا بالشخصية الإنسانية، والتي تطورت مع تطور العلم خلال العقود الماضية، فمع ظهور شبكة الإنترنت والحواسيب ومواقع التواصل الاجتماعي والعديد من التطبيقات التي تعمل من خلال شبكة الإنترنت وتطور أساليب الاتصالات

التي تشتمل على مكالمات الفرد وصوره وتسجيلاته ومحادثاته، أصبح من اللازم التصدي لمثل ما ينتج عنها من مشاكل وقضايا، لذلك جاءت هذه الدراسة للوصول إلى فائدتين علميتين، عملية ونظرية، الفائدة العملية والتي تبحث في كيفية معالجة ومحاربة موضوع انتهاك خصوصية الأفراد من خلال التشريعات الجزائية في الأردن، من خلال اقتراحات واقعية بهذا الشأن وبعض المقترحات التي يجب إدخالها على النصوص الوضعية السارية المفعول.

وتميز الدراسة الحالية عن الدراسة السابقة بتناولها عقوبات انتهاك حرمة البيانات الشخصية المنفذة تكنولوجيا من خلال عقوبة الدخول قصداً إلى الشبكة المعلوماتية، وعقوبة استخدام وسيلة إلكترونية للضرر بالبيانات، وموقف المشرع الأردني من جريمة الوصول إلى عنوان (IP) للضحية، والوسائل الجرمية المرتبطة بالهندسة الاجتماعية وكلمات المرور الضعيفة.

- **دراسة "ثوماس" (Thomas, 200). بعنوان: Insufficient computer security theatens doing business, University of Washington Press.**

تطرقت هذه الدراسة إلى الحديث عن ماهية حق الحياة الخاصة، وصور انتهاكها وبيان مخاطر تكنولوجيا المعلومات والكمبيوتر في ظل التطور الهائل في مجال الانترنت ووسائل الاتصال.

كما بينت الدراسة بعضًا من صور الحماية الجزائية لحق الحياة الخاصة في عدد من التشريعات.

وتتميز الدراسة الحالية عن الدراسة السابقة بتناولها الوسائل الجرمية المرتكزة على الثغرات الآمنة في النظام والتهديدات الداخلية، والوسائل الجرمية المستندة على الخطأ البشري والتنزيلات المخترقة والأفعال الحقيقية، وانتهاكات البيانات الشخصية كفعل ضار في قانون العقوبات الأردني.

- **دراسة شقير ، يحيى، (2012)، مدى توافق قانون ضمان حق الحصول على المعلومات في الاردن مع المعايير الدولية، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الاوسط، عمان: الاردن.**

تناولت الدراسة السابقة الحديث عن قانون ضمان حق الحصول على المعلومات، ومقارنتها مع المعايير الدولية.

وتميزت الدراسة الحالية عن الدراسة السابقة في انها ستتناول حماية البيانات الشخصية في ظل وجود قانون الجرائم الالكترونية، وبيان النصوص القانون في هذا القانون التي تكرس الحماية للبيانات الشخصية، والحماية الجنائية لهذه البيانات والجزاء المترتب على مرتكبيها.

منهجية الدراسة:

تعتمد الدراسة الحالية على:

أولاً: المنهج الوصفي، حيث سيتم استقراء المواد القانونية ذات العلاقة بالبيانات الشخصية الإلكترونية، ونطاق الحماية الجزائية لها في القانون الاردني كما هي في الواقع، ووصفها وصفًا دقيقًا، وببيان خصائصها.

ثانيًا: المنهج التحليلي، اعتمد الباحث على المنهج الوصفي، والمنهج التحليلي، حيث سيتم وصف المفاهيم، والحالات المرتبطة بالموضوع، إضافة إلى تحليل النصوص القانونية الواردة في التشريع

الأردني والخاصة بنطاق الحماية الجزائية للبيانات الشخصية الالكترونية، والخروج بالاستنتاجات المناسبة.

خطة الدراسة:

الفصل التمهيدي (الإطار العام للدراسة) ويشمل المقدمة، والمشكلة، والأسئلة، والأهداف، والأهمية، والمصطلحات، والحدود، والمنهجية، والدراسات السابقة ذات الصلة)

الفصل الأول
ماهية البيانات الشخصية ومعالجتها

المبحث الأول: مفهوم البيانات الشخصية ونطاق حمايتها

المطلب الأول: ماهية البيانات الشخصية

الفصل الثاني

الحماية الجزائية للبيانات الشخصية

المبحث الأول: صور الجرائم الواقعة على البيانات الشخصية وفقًا لقانون الجرائم الإلكترونية

المبحث الثاني : الأساس القانوني لقيام المسؤولية الجزائية وموقف المشرع الأردني من جريمة انتهاك الحياة الخاصة

الخاتمة والنتائج والتوصيات

الفصل الثاني
الحماية الجزائية للبيانات الشخصية

تمتد حالات اختراق البيانات الشخصية للأفراد على مدار العام، وبإمكان أي جهة أو فرد الحصول عليها بسهولة دون وجود مسوغات قانونية رادعة تجعل استخدام البيانات، والاطلاع عليها حكراً على أصحابها والجهات الرسمية التي تتطلب طبيعة عملها، ذلك ولأغراض محددة[1]. ويندرج ضمن البيانات الشخصية الوضع المالي للفرد، والأسرة، وتاريخ الميلاد، ومكانه، وجهة العمل، وعدد الأطفال ومستوياتهم الدراسية واهتماماتهم وأرقام هواتفهم وغير ذلك[2].

المبحث الأول

مفهوم البيانات الشخصية ونطاق حمايتها

ولم ينص صراحة قانون الجرائم الإلكترونية رقم (17) لسنة (2023) على مفهوم محدد وواضح للبيانات الشخصية، وإنما أشار إليها بتعريف عام على أنها: (البيانات التي تمت معالجتها إلكترونيًا وأصبح لها دلالة)، وحدد قانون الجرائم الإلكترونية رقم (17) لسنة (2023) تعريف البيانات من خلال ربطها بخدمات الحاسب الآلي –فقط–، والمعنية بالمعالجة والتخزين والنقل (كل ما يمكن معالجته أو تخزينه أو توريده أو نقله باستخدام تكنولوجيا وتقنية المعلومات بما في ذلك الكتابة أو الصور أو الأرقام أو الفيديوهات أو الحروف أو الرموز أو الإشارات وغيرها). ولغايات توضيح مفهوم البيانات الشخصية ونطاق حمايتها تطرق الباحث إلى الحديث عن ماهية البيانات الشخصية (المطلب الأول):

---

(1) الجمعية الأردنية للمصدر المفتوح (2022). مشروع قانون حماية البيانات الشخصية لسنة (2022)، التقرير السنوي لعام 2022.

(2) وزارة الاقتصاد الرقمي والريادة (2021). قانون حماية البيانات الشخصية لسنة (2021)، التقرير السنوي لعام 2021.

المطلب الأول

ماهية البيانات الشخصية

ارتبطت البيانات الشخصية بالتطور التكنولوجي؛ بحيث لم تعد تقتصر على البيانات التقليدية (الاسم واللقب والعنوان البريدي)؛ بل اتسعت وتنوعت لتشمل صورة الضحية وصوتها، وقدرتها المالية وسلوكياتها وعاداتها وميولها وأذواقها؛ والأكثر من ذلك كله البيانات الشخصية المرتبطة بجسم الضحية، أو ما يعرف بالبيانات البيومترية[1].

وعرفتها المادة (2) من قانون حماية البيانات الشخصية في الأردن لسنة (2022) على أنها: (أي بيانات أو معلومات تتعلق بشخص طبيعي تدل بصورة مباشرة أو غير مباشرة عن أصله أو عرفه أو تدل على آرائه أو انتماءاته السياسية أو معتقداته الدينية أو أي بيانات تتعلق بوضعه المالي أو بحالته الصحية أو الجسدية أو العقلية أو الجينية. أو بصمته الحيوية (البيومترية) أو بسجل السوابق الجنائية الخاص به، أو أي معبومات أو أي بيانات يقرر المجلس اعتبارها حساسة، إذا كان إفشائها أو سوء استخدامها يلحق ضرراً بالشخص المعني بها).

ولغايات توضيح البيانات الشخصية كان من الضروري تناولها من خلال المنحى التكنولوجي–موضوع دراستنا الحالية–، وذلك بصفتها بيانات شخصية تكنولوجية، من خلال التعريف القانوني لها (الفرع الأول)، والتعريف الدولي لها (الفرع الثاني)؛ كونها قضية عالمية.

---

[1] الزيود، فادي (2022). جريمة الاعتداء على الحياة الخاصة بالوسائل الإلكترونية في التشريع الأردني ومدى مواءمتها مع الاتفاقيات الدولية، مرجع سابق، ص44. الشوابكة، محمد (2011). جرائم الحاسوب والغ نترنت– الجريمة المعلوماتية، (ط4)، مرجع سابق، ص6.

الفرع الأول

المفهوم القانوني للبيانات ذات الطابع الشخصي الإلكتروني للضحايا

يرتبط المفهوم القانوني للبيانات ذات الطابع الشخصي للضحايا بالعناصر المحددة الخاصة بهم؛ كالهوية الشخصية (الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية)، بحيث تعتبر البيانات ذات الطابع الشخصي للضحايا في المفهوم القانوني جريمة إلكترونية يعاقب عليها القانون الأردني[1] تتطلب من الضحايا تقديم شكوى، ويحق بالتالي للضابطة العدلية حق الدخول إلى مسرح الجريمة الإلكترونية[2].

وتعد البيانات الشخصية (شخصية) طالما أنها تتعلق بالضحايا الطبيعيين الذين تم تحديد هويتهم بشكل مباشر، أو غير مباشر من خلال (IP)[3] الذي أشار إليه الباحث-سابقًا. والذي يشمل الاسم أو رقم التسجيل أو رقم الهاتف أو الصورة الفوتوغافية أو بيانات الشخصية للضحايا المرتبطة ببصمة الأصابع أو الحمض النـــووي،

---

[1] حموري، شهد والمصري، ريم (2014). قانون حماية البيانات الشخصية الأردني، ما يمكن تعلمه من تجارب الدول الأخرى، مقالة منشورة على مدونة حبر، متاحة عبر الرابط الإلكتروني: www:7iber.com/wp-content/uploads/2016/01/Reem.pdf.، تمت الزيارة بتاريخ: 15-9-2023، الساعة 8:35 صباحًا.

[2] الأكلبي، علي (2019).البيانات الضخمة واتخاذ القرار، بحث منشور في **مجلة الدراسات التكنولوجية**، الرياض، 15(2)، 12-34.

[2]الزيود، فادي (2022). جريمة الاعتداء على الحياة الخاصة بالوسائل الإلكترونية في التشريع الأردني ومدى مواءمتها مع الاتفاقيات الدولية، مرجع سابق، ص44. الشوابكة، محمد (2011). جرائم الحاسوب والغ نترنت- الجريمة المعلوماتية، (ط4)، مرجع سابق، ص6.

وكذلك البيانات الشخصية الإلكترونية التي يكون من شأنها تمييز الضحايا عن غيرهم مثل مكان الإقامة، والمهنة، النوع، والسن[1].

وتشير البيانات الشخصية الناشئة عن معالجة تقنية أو فنية خاصة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية للشخص الطبيعي والتي تمكن من تحديد هوية الضحية من خلال صوره الوجه أو البيانات الخاصة ببصمات الإصبع[2].

ويلزم توافر مجموعة من الشروط حتى يمكن الاستعانة بهذه البيانات واستخدامها؛ فيجب أن تكون هذه البيانات فريدة ودائمة وقابلة للقياس؛ حيث يمكن من خلال الأجهزة التقنية الحديثة تحديد هوية الشخص من خلال الرجوع إلى خصائص أو صفات الجسم مثل بصمة الأصابع أو الخطوط العريضة لكف اليد وتحليل الشبكية، وقزحية العين، والشبكة الوريدية للأصبع، واليد أو شكل الوجه وكذلك الحمض النووي، فكل هذه البيانات البيومترية المستخرجة من هذه الخصائص أثناء التسجيل هي بيانات شخصية[3].

---

(1) الأهواني، حسام الدين (1978). الحق في احترام الخصوصية، دار النهضة العربية، القاهرة، ص12.

(2) فضيلة، تومي (2017). أيديولوجيات الشبكات بالاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، مجلة العلوم الإنسانية والاجتماعية، جامعة قصدي مرباح، الجزائر، المجلد الثاني، العدد الثلاثون، ص14.

(3) كامل، جبالي (2016). حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق، جامعة أسيوط في الفترة من (12–13) إبريل، ص22.

ولم يكتف المشرع الأردني بتناول البيانات الشخصية للمواطنين من حيث التعريف، بل شدد على كل من ينتهك حرمة هذه البيانات في نص المادة (64) من قانون الاتصالات الأردني حتى عام (2023) من خلال ما يلي:

أولاً: لموظفي الهيئة ضبط أي أجهزة أو معدات اتصال غير مرخصة أو مخالفة للقانون أو تستعمل في نشاط غير مرخص له قبل إيصل خطي يبين نوع الأجهزة ومواصفاتها وتسليم هذه الأجهزة إلى الهيئة).

ثانيًا: تصادر المضبوطات غير القابلة للترخيص، أما الأجهزة المسموح بترخيصها فيتم الاحتفاظ بها إلى حين ترخيصها.

الفرع الثاني

موقف التوجيهات الأوروبية من البيانات ذات الطابع الشخصي الإلكتروني

يندرج ضمن حماية البيانات الشخصية بعض المصطلحات أو المفاهيم ذات الصلة مثل البيانات الشخصية، ومعالجة البيانات الشخصية، وبطاقات البيانات الشخصية، حيث يجب أن تفهم كل هذه المفاهيم والمصطلحات وفقًا لما جاء في نص قانون الجمعية الأوروبية على أساس التعريفات الدقيقة التي نص عليها التوجيه الأوروبي (EC-95-46)[1].

وينظر التوجه الأوروبي من البيانات الشخصية الإلكترونية على أنها وسيلة لا مفر منه، فرضتها الثورة المعرفية؛ حيث أصبح استخدام الإنترنت يُعرّض مستخدميه إلى الكثير من المخاطر، لما يتطلبه من الإدلاء ببعض البيانات والمعلومات الشخصية (الاسم، والعنوان، وتفاصيل الحساب، المصرفي، وعادات المستخدم اليومية، وأسماء أصدقائه)، بل وأكثر من ذلك[2].

ومع ذلك، فإن تدفق البيانات الشخصية للمستخدمين يمثل خطراً على خصوصية هؤلاء الأشخاص من خلال استخدام البيانات الخاصة بالبطاقات المصرفية، أو سرقة الهوية للشخص من أجل التشهير بسمعة الشخص أو تدمير مستقبله المهني بعد نشر المعلومات على الإنترنت [3].

---

(1) فضيلة، تومي (2017). أيديولوجيات الشبكات بالاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، مرجع سابق، ص20..

(2) عثمان، بكر (2016). المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي، أطروحة دكتوراه (مرجع سابق، ص14.

(3) سيد، أشرف جابر والشافي، خالد (2013). حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع فيس بوك، مرجع سابق، ص23..

ويسعى التوجه الأوروبي إلى تحذير متصفحي الإنترنت أن يراعو الحيطة والحذر في الكشف عن معلوماتهم، وبياناتهم الشخصية على مواقع الويب؛ بالنظر إلى المخاطر التي يمكن أن تهددهم بسبب قيام الشركات بإنشاء ملف تعريفي لهم عن طريق البيانات والمعلومات التي تم جميعها عنهم؛ حيث تحصل هذه الشركات على البيانات الشخصية من خلال العديد من المصادر[1].

ويبدو أن القبول الواسع لكل من هذه المفاهيم من شأنه أن يؤدي إلى مستوى عالي من حماية البيانات الشخصية، مما يسمح – بلا شك– باتساع مجال التطبيق.

يرى الباحث–أيضًا– أن المشرع الأردني في نص المادة (2) من قانون حماية البيانات الشخصية لسنة (2022) يؤيد التوجه السابق عندما ركز حديثه عن خطورة الإخلال بالأمن، وسلامة البيانات موضحًا أنها: (وصول غير مشروع أو أي عملية أو نقل أو إجراء غير مصرح به على البيانات).

إلا أن المادة (71) من قانون الاتصالات الأردني حتى عام (2023) تناولت هذا الموضوع بشكل عام من خلال تركيزها على الانتهاك لهذه البيانات وعلى الغرامة المالية، والحبس بدون تحديد طبيعته وضرره لكل حالة حين قالت: (كل من نشر أو أشاع مضمون أي اتصال بواسطة شبكة اتصالات عامة أو خاصة أو رسالة هاتفية اطلع عليها بحكم وظيفته أو قام بتسجيلها دون سند

---

(1) Belharet, A. (2020). A Study on the Impact of Artificial Intelligence on Project Management of Technology Information Systems. P 16. والعنزي، زياد (2018). المسؤولية القانونية عن طرد عضو من المجموعة في مواقع التواصل الاجتماعي في التشريع الأردني، مجلة علوم الشريعة والقانون، المجلد الرابع والخمسون، العدد الثاني، ص11 وما بعدها.

قانوني يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (100) دينار ولا تزيد على (300) دينار أو بكلتا العقوبيتين.

وبالمثل اكتفت المادة (76) منه– أيضًا– على تناول العقوبة بشكل عام دون تفصيل عقوبة كل صورة من صور جريمة الانتهاك بقولها: (كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على 200 دينار أو بكلتا العقوبيتين). مما حذا بالباحث بضرورة ربط هذا المفهوم الخطير البيانات الشخصية الإلكترونية بمعطيات عدة تتعلق بما يتم الاستيلاء عليه من بيانات الضحايا وذلك في الأبواب التالية من دراسته الحالية:

المطلب الثاني

معطيات البيانات الشخصية الإلكترونية

يبدو أن استعمال البيانات الشخصية الإلكترونية يرتبط بمعطيات في القوانين والتشريعات–بشكل عام– تبرز من خلال إمكانية الشخص تحديد هويته بشكل مباشر أو غير مباشر يؤكد على ضرورة تحقيق أعلى مستوى من الحماية لبياناته الشخصية داخل مجتمع قد تسوده الكثير من الجرائم المبتكرة والحديثة(1). وتنطبق معطيات البيانات الشخصية على حماية المعلومات التي تحدد هوية الشخص بشكل مباشر مثل الاسم أو موطنه وتتعداها إلى المعلومات التي تحدد العناصر التي تحدده شخصيًا بشكل غير مباشر، وتبرز هذه المعطيات والتي ترتبط –على الأغلب–بالتقنيات الحديثة من خلال[2]:

أولاً: رقم الجوال.

ثانيًا: عنوان البريد الإلكتروني.

ثالثًا: رقم بطاقة الائتمان.

رابعًا: البيانات الشخصية (الصوت، وبصمات الأصابع، والحمض النووي).

خامسًا: البيانات البيومترية (السمات البيولوجية والسلوكية، وقد تشمل بصمات الأصابع، ومسح قزحية العين وطريقة الضحية في فعل شيء كاالطريقة التي يسير أو يكتب بها).

---

(1) التهامي، سامح (2011). الحماية القانونية للبيانات الشخصية، مرجع سابق، ص22.

(2) كامل، جبالي (2016). حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق، جامعة أسيوط في الفترة من (12–13) إبريل، ص20.

لذا سيتناول الباحث هذه المعطيات التي تضمنها التعريف الخاص بالبيانات الشخصية المتفق عليها في القوانين والتشريعات العالمية –بشكل عام– في الفرعين التاليين:

الفرع الأول

البيانات أو المعلومات التي تحدد هوية الشخص

إن التعبير عن أية بيانات أو معلومات في أي تشريع يدل على رغبة المشرع–بشكل عام– في الأخذ بمفهوم واسع للبيانات ذات الطابع الشخصي[1].

وتتضمن البيانات التي تحدد هوية الشخص جميع أنواع المعلومات المرتبطة به؛ كما هو عليه الحال بالنسبة للمعلومات الشخصية أو الذاتية مثل فصيلة الدم الخاصة بشخص معين[2].

وفيما يتعلق بمضمون أو محتوى هذه المعلومات؛ تندرج المعلومات الأكثر خصوصية ضمن البيانات ذات الطابع الشخصي بالنظر إلى المخاطر المحتملة الناشئة عن الاعتداء عليها[3].

ويقصد بالبيانات التي تحدد هوية الشخص، أي البيانات الأكثر خصوصية التي يدلى بها مستخدم شبكة الإنترنت عند دخوله موقع معين من أجل إتمام إجراءات الدخول على هذا الموقع؛ حيث يلزم على مستخدم الشبكة أن يسجل بعض المعلومات شديدة الحساسية مثل الميل الجنسي والآراء السياسية وديانته(4)، وفي ذلك تناولت المادة (2) من قانون حماية البيانات الشخصية في الأردن لسنة (2022) التشخيص على أنه: (المعالجة الآلية للبيانات للتعرف على اتجاهات الشخص المعني أو ميوله أو خياراته أو سلوكياته).

---

(1) الغويري، ضيف الله (2014). ضمانات الحق في الحماية الخاصة في النظام السعودي، مجلة المدير الناجح، المجلد الثامن، العدد الثاني عش، ص11,

(2) المؤيد، محمد (2009). صور المسؤولية التقصيرية الناشئة عن الاعتداء على بيانات الكمبيوتر والتعامل عبر الإنترنت وتسوية منازعاتها، مجلة الدراسات الاجتماعية، المجلد الثاني، العدد الثامن والعشرون.

(3) الديحاني، فهيد (2014). الطبيعة القانونية للحق في الصورة الشخصية وحمايته المدنية في القانون الكويتي، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد (56).

(4) الديحاني، فهيد (2014). الطبيعة القانونية للحق في الصورة الشخصية وحمايته المدنية في القانون الكويتي، مرجع سابق، ص11.

يرى الباحث بالتالي ضرورة تحديد هوية الشخص أو الضحية والتي تتعلق بآلية إدلائه للبيانات.

ويرى الباحث من خلال ما سبق أنه مما لاشك فيه، أن مثل هذه المعلومات هي بيانات أكثر خصوصية تندرج ضمن قانون حماية البيانات الشخصية التي يحظر معالجتها في حالات معينة.

ومما لاشك فيه أن هذه البيانات الشخصية الإلكترونية التي تدلي بها الضحية المستهدفة ترتبط بالحياة الخاصة لها، والتي إرتأى الباحث مناقشتها في الفرع الثاني:

الفرع الثاني

المعلومات المرتبطة بالحياة الخاصة

وفقًا للتفسير الضيق، يشمل مصطلح البيانات الشخصية؛ المعلومات المرتبطة بالحياة الخاصة والعائلية للشخص الطبيعي (الضحية المستهدفة)، وكذلك المعلومات المرتبطة بأعماله أو أنشطته أيًا كانت مثل المعلومات المتعلقة بعلاقات العمل، وكذلك المرتبطة بسلوكياته الاجتماعية[1].

فالأمر يتعلق بالأشخاص الطبيعيين دون النظر إلى وظيفتهم أو صفاتهم (مثل المستهلكين، والمرضى والموظفين، والعملاء، وما إلى ذلك)[2].

حيث عرفت المادة (2) من قانون حماية البيانات الشخصية الأردني لسنة (2022) الشخص المعني، على أنه: (الشخص الطبيعي الذي تتم معالجة بياناته الخاصة به).

---

(1) سدي، عمر (2020). المسؤولية الجنائية على إفشاء السر، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد التاسع، العدد الثالث، ص11,

(2) سليم، بوزيدي (2016). الاعتداء على الحق في الصورة في ظل التطورات التكنولوجية الحديثة، رسالة ماجستير (غير منشورة)، جامعة عبد الرحمن، ميرة: الجزائر، ص20

فعلى سبيل المثال يندرج ضمن البيانات الشخصية جميع المعلومات المرتبطة بوصفات العلاج التي يكتبها الطبيب من أجل شراء الدواء مثل رقم تعريف الدواء؛ وجرعة الدواء؛ واسم الدواء؛ وسعر الدواء، وأسباب الاستخدام، واسم الطبيب وعائلته، ورقم الهاتف، وما إلى ذلك؛ إما في شكل وصفات طبية فردية أو في شكل مجموعة من الوصفات الطبية التي يمكن اعتبارها بانات ذات طابع شخصي بالنسبة للطبيب الذي يقدم لمريضه الوصفة الطبية؛ حتى ولو كانت البيانات الشخصية المتعلقة بالمريض تبقى مجهولة[1].

وهذا يتطلب وجود شخص مراقب يشرف على هذه البيانات، وفي ذلك نصت المادة (2) من قانون حماية البيانات الشخصية الأردني لسنة (2022) على أن المراقب هو: (الشخص الطبيعي المعين للإشراف على قواعد البيانات والمعالجة وفقًا لأحكام هذا القانون).

غير أن المادة السابقة لم تحدد بشكل مفصل آلية هذه المراقبة، وبالتالي يرى الباحث أن تصنيفات الجرائم التي سترتكب قد تفوق التقسيمات في الفقرة السابقة إلى صور جديدة لم يعهدها مستخدم البيانات (الصور الناجمة عن الجرائم الإلكترونية، كجريمة هتك العرض الإلكتروني، وجريمة اغتيال الشخصية إلكترونيًا من حيث تشوية سمعته، وتصوير جسد الضخية).

وبالتالي، فإن تقديم المعلومات المتعلقة بالوصفات الطبية المكتوبة من قبل أطباء محدودون أو إمكانية أو قابلية تحديدها إلى الصيدليات ينطبق عليه مصطلح البيانات ذات الطابع الشخصي الوارد –من وجهة نظر الباحث–، والذي يشكل خطورة على أمن المعلومة.

---

(1) لامي، بارق (2017). جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير (غير منشورة)، جامعة الشرق الأوسط، عمان: الأردن، ص20.

لذا قام الباحث بتفصيل العلاقة السابقة برؤية أخرى، وذلك من خلال مناقشة وتحليل معالجة هذه البيانات وبيان مدى آثارها، وذلك من خلال المبحث الثاني (البيانات الشخصية والآثار المترتبة على معالجتها).

---

(1) الخلايلة، عايد (2011. المسؤولية التقصيرية الالكترونية، دراسة مقارنة، (ط2)، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص20.

(2) الزعبي، علي احمد (2006). حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، طرابلس: بيروت، ص22.

(3) المادة (7) والمادة (8) من الدستور الأردني *سيتم تناولهما في الأبواب القادمة

المبحث الثاني

مفهوم معالجة البيانات الشخصية والآثار المترتبة على معالجتها

يشتق مصطلح معالجة البيانات من كلمة معالج أو الشخص الطبيعي أو الشخص الاعتباري الذي يكون مختصًا بمعالجة البيانات التي تتطلب تكاتف أكثر من شخص، وتتطلب وجود برامج أشار إليها قانون الجرائم الإلكترونية رقم (17) لسنة (2023) على أنها: (مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات أو أي وسيلة من وسائل تقنية المعلومات). وبالتالي قام الباحث بتناول **معالجة البيانات** في المطلب الأول:

---

[1] الشوابكة، محمد امين (2011). جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص20.

المطلب الأول

مفهوم معالجة البيانات الشخصية الإلكترونية

يتميز مفهوم معالجة البيانات الشخصية الإلكترونية بالاتساع؛ بهدف تحقيق الحماية الكافية والشاملة(1)، وقد ورد تعريف معالجة البيانات الشخصية في كافة القوانين الدولية كما بين الباحث في مستهل رسالته–؛ إلا أن المشرع الأردني لم يتناولها بالتفصيل من حيث كونها عملية تتعلق بالبيانات الشخصية؛ أي أنها عملية أو مجموعة من العمليات المبرمة أو التي تسخدم الوسائل الآلية لكي تطبقها على البيانات الشخصية مثل الجمع أو التسجيل، أو التنظيم أو الحفظ، او التعديل أو التصميم أو الاستخراج أو الاسترجاع أو الاستخدام أو الإحالة عن طريق الإرسال أو النشر أو أي شكل آخر من الأشكال مثل التقريب لشكل الضحية[1]. في حين لم ينص قانون حماية البيانات الشخصية الأردني على تفصيل معالجة البيانات الشخصية الإلكترونية إلا من تعريف فقط المنظمين لهذه المعالجة من مسؤولين، ومتلقين، وذلك على النحو الآتي:

أولاً: عرفت المادة (2) من قانون حماية البيانات الشخصية الأردني لسنة (2022) المسؤول على أنه: (أي شخص طبيعي أو اعتباري سواء أكان داخل المملكة أم خارجها تكون البيانات في عهدته).

ثانيًا: عرفت المادة ذاتها من القانون ذاته المتلقي على أنه: (أي شخص طبيعي أو اعتباري سواء كان داخل المملكة أو خارجها يتم نقل البيانات إليه أو تبادلها معه من المسؤول)

ولغايات تفصيل هذا الموضوع قام الباحث بتناول معالجة البيانات الشخصي من خلال الشخص المعني بالأمر (الفرع الأول):

---

[1] الغويري، ضيف الله (2014). ضمانات الحق في الحماية الخاصة في النظام السعودي، مجلة المدير الناجح، المجلد الثامن، العدد الثاني عشر، ص22.

الفرع الأول

معالجة البيانات المرتبطة بالشخص المعني بالأمر

يشير مصطلح الشخص المعني بالأمر –في موضوع دراستنا الحالية– إلى الشخص الطبيعي الذي تكون معطياته الشخصية موضوعًا للمعالجة، فعلى سبيل المثال، البيانات أو المعلومات المدرجة في الملف الشخصي للموظف بقسم شؤون الموظفين؛ فهذه البيانات تعبر بصورة واضحة عن المعني بالأمر من حيث حالته الشخصية بصفته موظفًا[1].

كما ينطبق ذلك أيضًا على النتائج الخاصة بالفحص الطبي للمريض في ملفه الطبي الموجودة بالمستشفى أو صوره أو فيديو لشخص أثناء إجراء مقابلة معه[2].

ولم ينص المشرع الأردني على الشخص المعني إلا في نص المادة (2) من قانون حماية البيانات الشخصية الأردني لسنة (2022) عند تناوله فقط موضوع الموافقة المسبقة، حيث نصت على أنه: (موافقة الشخص المعني المسبقة على المعالجة).

يرى الباحث أن هناك حاجة لتفسير موقف الشخص المعني من موضوع البيانات الشخصية في النصوص الحالية تفاديًا لمزيد من الجرائم، حيث يعتبر هو الضحية الأولى في جرائم الاحتيال في موضوع البيانات الشخصية الإلكترونية.

---

[1] العنزي، زياد (2018). المسؤولية القانونية عن طرد عضو من المجموعة في مواقع التواصل الاجتماعي في التشريع الأردني، مرجع سابق، ص20.

[2] الغويري، ضيف الله (2014). ضمانات الحق في الحماية الخاصة في النظام السعودي، مرجع سابق، ص22.

يرى الباحث أن موضوع معالجة البيانات –على خطورتها– تم التطرق إليها من زاويتين:

أولاً: حصرها في موضوع الحماية فقط.

حيث نصت المادة (6/ 3) من قانون حماية البيانات الشخصية الأردني لسنة (2022) على موضوع المعالجة من خلال: (3– إذا كانت ضرورية لحماية حياة الشخص المعني أو لحماية مصالحة الحيوية).

ثانيًا: ربطها بالضرورة لمنع الجريمة أو ملاحقتها

حيث نصت المادة (4/6) من قانون حماية البيانات الشخصية الأردني لسنة (2022): (4– إذا كانت ضرورية لمنع جريمة أو لكشفها من قبل جهة مختصة، أو لملاحقة الجرائم المرتكبة خلافًا لأحكام القانون).

ولم يتناول قانون الاتصالات الأردني وتعديلاته (2023) في المادة (6/ي) معالجة البيانات إنما تناول الحديث عن تنظيم الدخول إلى الشبكات لاغيًا دور المعالج قائلاً: (تنظيم الدخول إلى شبكات الاتصالات وشروط الربط بينها وفق تعليمات تصدرها الهيئة لهذه الغاية، والموافقة على اتفاقيات الربط المشار إليها في الفقرة (5) من المادة (29) من هذا القانون والتأكد من عدم مخالفة الاتفاقيات لتلك التعليمات).

فهناك جانب يعاني من ضبابية وهو الحاجة إلى إجراء وقائي مستند إلى التكنولوجيا يحذر تداول هذه البيانات التي قد تكون عاملاً رئيسًا في حدوث الجريمة.

الفرع الثاني

مفهوم بطاقة أو ملف البيانات الشخصية

لم يحدد المشرع الأردني نصوصًا تتعلق بتناول البطاقات، فهو ينظر لمفهوم البطاقات بشكل منفصل حتى لا يتم الخلط بينه وبين معالجة البيانات الشخصية[1]، فارتكزت أغلب التشريعات التي تناولت هذا الموضوع، ومنها التشريعات الخاصة بالتوجه الأوروبي.

[1] الهميم، عبد اللطيف (2003). احترام الحياة الخاصة، دار عمان للنشر والتوزيع، عمان، ص33.

ولم يتناول قانون الجرائم الإلكترونية رقم (17) لسنة (2023) مفهوم بطاقة أو ملف البيانات الشخصية، وإنما بينت المادة (3/ج) منه فقط غرامة منتهك البيانات الشخصية، حيث نصت على أنه:

(يعاقب كل من دخل أو وصل قصداً إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو تشفيره أو إيقافه أو تعطيله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (600) ستمائة دينار ولا تزيد على (3000) ثلاثة آلاف دينار).

ولم يشر كذلك قانون الاتصالات الأردني حتى عام (2023) إلى مفهوم بطاقة أو ملف البيانات الشخصية، وإنما اكتفى في نص المادة (6/د) على حماية حقوق المستخدمين قائلاً:

(حماية مصالح المستفيدين ومراقبة الأشخاص والجهات المرخص لها للتأكد من الالتزام بشروط الرخصة بما في ذلك مواصفات الخدمات المقدمة وجودتها وأسعارها واتخاذ الإجراءات القانونية اللازمة بحث من يخالف هذه الشروط).

الفرع الثالث

شروط الحصول على البيانات ذات الطابع الشخصي

أصدر قانون الجرائم الإلكترونية رقم (17) لسنة (2023) التصريح (الإذن الممنوح من صاحب العلاقة إلى الشخص أو أكثر وللجمهور للدخول أو الوصول إلى نظام المعلومات أو تقنية المعلومات أو الشبكة المعلوماتية أو استخدامها).

وبين قانون الجرائم الإلكترونية رقم (17) لسنة (2023) على أن التصريح يكون:

أولاً: الإذن الممنوح من صاحب العلاقة.

ثانيًا: حيث يكون صاحب العلاقة شخصًا أو أكثر وللجمهور للدخول أو الوصول إلى نظام المعلومات أو تقنية المعلومات أو الشبكة المعلوماتية أو استخدامها).

يرى الباحث أن الحصول على البيانات الشخصية أو الإفصاح عنها أو توفيرها أو معالجتها يكون مشروعًا في الحالات الآتية:

- إذا كانت ضرورية لغرض منع أو كشف جريمة بناء على طلب رسمي من جهات التحقيق.
- إذاكانت مطلوبة أو مصرحًا بها بموجب قانون أو كان ذلك بقرار من المحكمة.
- إذا كانت البيانات ضرورية لتقدير أو تحصيل أية ضريبة أو رسوم.
- إذا كانت المعالجة ضرورية لحماية مصلحة حيوية للضحية التي تم جمع البيانات حولها.

والأمر على خلاف ذلك بالنسبة للدستور الأردني؛ حيث حظيت البيانات الشخصية للأفراد الطبيعيين في البيئة الرقمية بحماية الدستور الأردني الذي يعدها حقًا أساسيًا من حقوق الإنسان طالما أنها ترتبط بحرمة الحياة الخاصة للمواطن الأردني؛ حيث تكفل الدولة حرية الرأي، ولكل أردني

أن يعرب بحرية عن رأيه بالقول والكتابة والتصوير وسائر وسائل التعبير بشرط أن لا يتجاوز حدود القانون.

كما أن تداول هذه البيانات الشخصية الإلكترونية يتطلب مزيداً من الاحتياطات والإجراءات الخاصة اللازم اتباعها من خلال تدفقها بين دول العالم من أجل الحفاظ على خصوصية هذه البيانات[1].

ولأن تداول البيانات الشخصية قد يكون مدخلاً لجرائم من نوع جديد يشهدها المجتمع الأردني بسبب هذا الفضاء الرقمي الواسع؛ قام الباحث بتناولها في المطلب الثاني (تداول البيانات الشخصية الإلكترونية وأثرها على الخصوصية)

---

[1] الجبوري، بيرك فارس (2009). حقوق الشخصية وحمايتها المدنية، دراسة مقارنة، أطروحة دكتوراه (غير منشورة)، جامعة القاهرة، القاهرة: مصر، ص12.

المطلب الثاني

تداول البيانات الشخصية الإلكترونية وأثرها على الخصوصية

يؤثر تداول البيانات الشخصية الإلكترونية على خصوصية الأفراد، وعلى الرغم من أن المادة (17/ب) من قانون حماية البيانات الشخصية الأردني لسنة (2022) بينت أن مجلس حماية البيانات الشخصية يتولى: (اعتماد المعايير والتدابير الخاصة بحماية البيانات)؛ إلا أن المسؤول الأول عن تداول هذه المعلومات، هو صاحبها.

ويبدو ذلك واضحًا من خلال إدلاء الشخص الذي يرغب في التسجيل على موقع معين على الشبكة العنكبوتية ببعض المعلومات الخاصة به مثل اسمه الأول واسم العائلة وعنوان البريد الإلكتروني وكلمة المرور والجنس وتاريخ الميلاد[1].

كما يمكن أن يطلب الموقع الإلكتروني منه بعض المعلومات الأخرى مثل مؤهلاته وخبرته المهنية التي يدلي بها في ملفه الشخصي عند التسجيل، حيث تشمل المعلومات المتعلقة بشخص طبيعي محدد، ويمكن وصفها بأنها بيانات شخصية [2].

كما يتولد عن تكنولوجيا المعلومات والاتصالات الكثير من البيانات الشخصية التي يمكن التوصل إليها من خلال مكالمة سابقة على هاتف محمول، أو عن طريق الاتصال التكنولوجي[3].

---

[1] حجازي، مصطفى أحمد عبد الجواد (2004). المسؤولية المدنية للصحفي عن انتهاك حرمة الحياة الخاصة، دار النهضة العربية، القاهرة، ص22.

[2] صادق، طارق (2015). الجرائم الإلكترونية جرائم الهاتف المحمول– دراسة مقارنة، أطروحة دكتوراه (غير منشورة)، (ط1)، جامعة حلوان، حلوان: مصر، ص22.

وتشترط الموافقة المسبقة في تداول البيانات الشخصية الإلكترونية، وذلك ما وضحته المادة (5/أ) من قانون حماية البيانات الشخصية الأردني لسنة (2022)؛ حيث بينت أنه: (يشترط في الموافقة المسبقة:

1- أن تكون صريحة وموثقة خطيًا أو إلكترونيًا.

2- أن تكون محددة من حيث المدة والغرض.

3- أن يكون الطلب بلغة واضحة وبسيطة وغير مضللة ويمكن الوصول إليه بسهولة.

4- موافقة أحد والديَ أو ولي الشخص الذي لا يتمتع بالهلية القانونية أو موافقة القاضي بناء على طلب الوحدة إذا اقتضت المصلحة الفضلى لمن لا يتمتع بالأهلية القانونية ذلك.

يرى الباحث أن المادة السابقة جعلت موضوع التداول للبيانات الشخصية مشروطًا فقط بالشخص المعني، وبما لا يتوافق مع الموافقة المسبقة لطبيعة المجتمع الذي يتم تداول البيانات الشخصية داخله؛ مما يترتب عليهه جرائم من نوع حدبث لم يألفها هذا المجتمع.

وفي المقابل بينت المادة (5/ب) من القانون ذاته أنه لا يعتد بالموافقة المسبقة في الحالتين التاليتين:

1- إذا صدرت استناداً إلى معلومات غير صحيحة أو ممارسات خادعة أو مضللة، وكانت هي السبب في قرار الشخص المعني بمنحها.

2- إذا تم تغيير طبيعة المعالجة أو نوعها أو أهدافها دون الحصول على الموافقة بذلك.

وهذا لا يعني -من وجهة نظر الباحث- أن تداول البيانات الشخصية بشكل إلكتروني لا يعني عدم الحاجة إلى نطاق حماية لها؛ لذا قام الباحث بمناقشة هذه الجزئية في الفرع الأول:

وهكذا، فإن وضع نظام البيانات الشخصية في بيئة الإنترنت عليه أن يراعي طبيعة المخاطر التي يمكن أن تواجه مستخدم الإنترنت عند قيامه بتصفح الشبكة، حيث تخلق الإنترنت سلسلة من التحديات الجديدة في مواجهة حماية الخصوصية.

وفي ذلك فصلت المادة (3/ب) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023) هذا الموضوع بقولها: (إذا كان الدخول أو الوصول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو نشر او إعادة نشر أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو خسترة سريتها أو تشفير أو إيقاف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات أو تقنية معلومات أو أي جزء منها فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (600) ستمائة دينار ولا تزيد على (300) ثلاثة آلاف دينار، وتكون العقوبة الحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن (3000) ثلاثة الآف دينار ولا تزيد على (1500) خمسة عشر ألف دينار إذا تمكن من تحقيق النتيجة).

الفرع الأول
نطاق حماية خصوصية البيانات الشخصية

يعكس نطاق حماية خصوصية البيانات الشخصية لمستخدمي التكنولوجيا الأشخاص المعنيين بحماية خصوصية هذه البيانات مثل المسؤول عن معالجة البيانات الشخصية، والمناول، ومستلم البيانات أو المتلقي للبيانات، حيث يلزم موافقة الشخص المعني بالأمر من أجل توفير حماية واسعة النطاق للبيانات الشخصية، وهذا ما بينه الباحث في المطلب السابق.

ولقد نصت المادة (14) من قانون حماية البيانات الشخصية الأردني لسنة (2022) على أنه: (لا يجوز نقل البيانات وتبادلها بين المسؤول أو أي شخص آخر بمن فيهم المتلقي إلا بموافقة الشخص المعني ووفقًا للشروط التالية:

1- أن يحقق النقل مصالح مشروعة للمسؤول والمتلقي.

2- أن يتوفر العلم الكافي لدى الشخص المعني بالمتلقي ووالأغراض التي ستستخدم البيانات من أجلها.

3- أن لا يكون الغرض من النقل التسويق للمنتجات أو الخدمات ما لم يوافق الشخص المعني بذلك.

ولقد شدد المشرع الأردني في نطاق حماية خصوصية البيانات الشخصية في المادة (23/ ج)، حين وضح الدور الرئيس لمجلس الوزراء فيما يخص شروط الإفصاح عن هذه البيانات: (يصدر مجلس الوزراء الأنظمة اللازمة لتنفيذ أحكام هذا القانون، بما في ذلك شروط الإفصاح عن البيانات والأشخاص الذين يجوز الإفصاح لهم والبيانات المسموح بالإفصاح عنها).

وأن التعريف الوحيد المتعلق مباشرة بالشخص المعني من خلال معالجة البيانات الشخصية يتعلق بموافقته أو رضائه؛ ويشير كذلك إلى كل تعبير عن الإرادة الحرة يمكن من خلالها التوصل إلى أن الشخص المعني قد وافق على المعالجة على أن تكون بياناته الشخصية محلاً للمعالجة[1].

يرى الباحث أن الفضل الكبير للتوجه في الأخذ بموافقة الشخص المعني هنا، وذلك على خلاف المشرع الأردني الذي يبدو أنه متردد في بيان نص محدد فيما يخص موافقة الشخص المعني.

وهكذا، يصبح من المستحيل من الناحية النظرية أن يخضع شخص معين إلى معالجة للبيانات الشخصية المتعلقة به دون تمكينه من التعبير عن موافقته.

---

[1] السكر، سلطان فياض (2022). جريمة انتهاك سرية المعلومات عبر الوسائل الالكترونية في التشريع الاردني، رسالة ماجستير (غير منشورة)، كلية الحقوق، جامعة الشرق الاوسط، عمان: الأردن، ص12 .

الفرع الثاني

مسؤول معالجة البيانات الشخصية الإلكترونية

إن وضع تعريف للمسؤول عن معالجة البيانات أمراً ضروريًا من أجل معرفة الشخص الذي يجب أن يمتثل للقواعد والالتزامات الناشئة عن القواعد على حماية البيانات الشخصية الإلكترونية؛ طالما كانت هناك موافقة على معالجة هذه البيانات[1].

حيث إنه ووفقًا لنص المادة (2) من قانون الجرائم الإلكتروني سابق الذكر– بشأن حماية الأشخاص الطبيعيين فيما يتعلق بالبيانات الشخصية وحرية تداول هذه البيانات؛ فالمسؤول عن معالجة البيانات هو شخص طبيعي أو معنوي أو سلطة عامة أو أي هيئة أخرى تحدد بمفردها أو بالاشتراك مع الآخرين أغراض ووسائل معالجة البيانات الشخصية؛ حيث نصت المادة السابقة على أن نظام المعلومات يشمل: (مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات الكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية)؛ حيث يمكن تحديد أغراض ووسائل المعالجة من خلال القوانين أو اللوائح الوطنية أو المجتمعية من خلال المسؤول عن هذه المعالجة.

ويدخل في نطاق مسؤولية معالجة البيانات الشخصية، ما يعرف بالمناول[2]

ولم ينص المشرع الأردني وبشكل مفصل على تحديد مسؤولية المناول؛ مما يسمح بإقامة المسؤولية بدرجات مختلف، ويساهم في تحسين كفاءة حماية الضحايا فيما يتعلق بمعالجة البيانات الشخصية.

---

[1]. الصغير، جميل عبد الباقي (2015). الحق في الصورة والإثبات الجنائي، مجلة كلية القانون، القاهرة، 2(2)، ص23-44، Harkut, D., & Kasat, K. (2019). Artificial Intelligence-Scope and Limitations. InntechOpen.p12.ص32.

حيث يشير المناول إلى الشخص الطبيعي أو الاعتباري أو أي هيئة أخرى تعالج البيانات الشخصية نيابة عن المسؤل عن معالجة البيانات الشخصية[1].

فالمقصود هنا هو الشخص أو الهيئة التي حتى لو كان لديها الوسائل اللازمة لتنفيذ معالجة البيانات الشخصية، فإنها لا يمكنها تحديد الغرض الذي من أجله تتم هذه المعالجة طالما أنه يعمل نيابة عن المسؤول عن المعالجة[2].

يرى الباحث أن هذا الفهم من شأنه أن يسمح يتحقيق أعلى درجة من الحماية؛ لأنه سوف يلزم كل شخص طالما أنه يعمل نيابة عن المسؤول عن المعالجة.

وهذا المفهوم من شأنه أن يسمح بتحقيق أعلى درجة من الحماية؛ لأنه سوف يلزم كل شخص يتصرف نيابة عن المسؤول عن المعالجة باحترام الالتزامات المتعلقة بحماية الأشخاص الطبيعيين من خلال معالجة البيانات الشخصية[3].

كما يشمل مسؤولية معالجة البيانات ما يسمى بالغير؛ حيث يشير إلى كل شخص طبيعي أو اعتباري، أو السلطة العامة، أو الخدمة أو أي هيئة أخرى غير الشخص المعني، أو المسؤول عن المعالجة أو المناول والأشخاص الذين يكون لديهم صلاحيات في معالجة البيانات الشخصية؛ طالما أنهم يعملون تحت إشراف السلطة المباشرة للمسؤول عن المعالجة أو المناول [4].

---

[1] قاسم، محمد حسن (2011). الحماية القانونية لحياة العمال الخاصة في مواجهة بعض مظاهر التكنولوجيا الحديثة، منشورات الحلبي الحقوقية، لبنان، ص20

[2] بشابشة، زياد محمد (2015). الحماية القانونية لحق الإنسان في صورته، عمان، الأردن، ص20.

[3] آدم عبد البديع حسين (2000). الحق في احترام الحياة الخاصة ومدى الحماية التي يكفلها القانون الجنائي– دراسة مقارنة، دار النهضة العربية، القاهره، ص23.

[4] الشهاوي، محمد (2005). الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، ص41.

وقد أظهر هذا المفهوم أهميته في ضمان حماسة الشخص المعني من خلال إلزام الشخص الذي ليس مسؤولاً عن المعالجة أو المناولة ببعض الحقوق ولاسيما الحق في الإعلام[1].

وقد يكون الغير هو مستلم أو متلقي البيانات؛ ولكن هذا ليس هو الحال دائمًا، وهذا هو السبب الذي من أجله وضع التوجيه الخاص بالبيانات الشخصية خاصًا، وبشكل منفصل لمستلم أو متلقي البيانات[2].

ويدخل مستلم البيانات في موضوع المعالجة، حيث يشير إلى شخص طبيعي أو اعتباري، أو إلى السلطة العامة، أو أي هيئة أخرى تتلقى إرسال البيانات سواء من الغير أو غير ذلك[3].

ومع ذلك، فإن السلطات التي من المحتمل أن تتلقى بيانات في إطار تقصي الحقائق لا يمكن اعتبارها مستلم للبيانات[4].

---

(1) البهجي،عصمت (2005). حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية، دار الثقافة، الإسكندرية، ص22.

(2) بشابشة، زياد محمد (2015). الحماية القانونية لحق الإنسان في صورته، مرجع سابق، ص20.

(3) قاسم، محمد حسن (2011). الحماية القانونية لحياة العمال الخاصة في مواجهة بعض مظاهر التكنولوجيا الحديثة، منشورات الحلبي الحقوقية، لبنان، ص20.

(4) الشهاوي، محمد (2005). الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، ص41.

الفرع الثالث

تداول البيانات الخاصة بصور وفيديوهات الضحايا في قانون العقوبات الأردني

لم يعرف قانون العقوبات الأردني رقم (16) لسنة 1960 وتعديلاته جريمة انتهاك البيانات الشخصية إلكترونيًا الخاصة بمعلومات الضحايا تعريفًا دقيقًا، لأن تحديد تعريف عام لجريمة المرتكبة إلكترونيًا فيما يخص أي معلومات ترتبط بصور وفيديوهات الضحايا في القانون شيء غير مستحب خاصة إذا جاء في التعريف أية قصور أو شائبة، حيث اكتفت المادة رقم (296) منه بالحديث عن هتك العرض بالعنف أو التهديد: (1- كل من هتك بالعنف أو التهديد عرض انسان عوقب بالأشغال مدة لا تنقص عن أربع سنوات. 2- ويكون الحد الأدنى للعقوبة سبع سنوات إذا كان المعتدي عليه لم يتم الخامسة من عمره)؛ على الرغم من هذا النوع الجديد من الجرائم الذي ينتهك بيانات الضحايا من صور وفيديوهات وحسابات بنكية لهم لا يحدث دون وسيط، والمتمثل في الشبكة المعلوماتية والحاسب حيث أن كلاهما أساسي افتراضي من أجل تحقيقها. حيث نصت المادة (15) من قانون الجرائم الإلكترونية السابق الإشارة إليه عند التحدث عن الركن الشرعي للجريمة، حيث أنه في ظل التوصل إلى أن الانتهاك يمكن حصوله بالوسيلة الإلكترونية يتساوى فاعلها مع من ارتكبها بشكل مباشر. وإن تشكيل محاكم خاصة تفصل في الجرائم الخاصة بصور الانتهاكات المرتكبة إلكترونيًا أو ما يعرف بالجرائم الإلكترونية، يتطلب تطبق القانون الخاص بها، أو تخصيص غرف قضائية متخصصة من منطلق أن إشكالية هذه الجرائم المرتكبة إلكترونيًا التي تبدأ إلكترونيًا وتنتهي إلى محاكمات جنائية. وهذا يتطلب تعزيز دور وحدة مكافحة الجرائم الإلكترونية في مديرية الأمن، ولا

يعطي فرصة لأن يغفل القانون بعض النقاط، كموضوع حماية البيانات، وموضوع الابتزاز المادي عبر الإنترنت.

المطلب الثالث

العوائق (الإشكاليات) المرتبطة بجريمة انتهاك البيانات الشخصية إلكترونيًا

يشهده العالم ثورة في مجال التكنولوجيا، والتي تطورت بشكل سريع للغاية، وعلى الرغم من الاستفادة الهائلة من هذه التكنولوجيا، وفي مختلف المجالات، إلا أنها عملت على تعقيد الجرائم وتنوعها.

لا شك أن حداثة الجرائم الإلكترونية ومن ضمنها جريمة انتهاك البيانات الشخصية المرتكبة إلكترونيًا آثار العديد من الصعوبات، حول البحث في أدلة إثباتها للتوصل إلى معرفة مرتكبها، ومن أجل مكافحة هذا النوع الجديد من الجرائم، استلزم الواقع القانوني أن يكون هناك نوع توضيح وتفسير لهذا النوع من الجرائم[1].

وتتطلب جرائم انتهاك البيانات المرتكبة إلكترونيًا من الجاني معرفة ضحيته (2)، والذي نتج من خلال شبكة الإنترنت، لكي يسهل للجاني الكشف عن المصادر المالية للمجني عليهم، وقام الباحث بتفصيل الحديث عن جريمة انتهاك البيانات الشخصية المرتكبة إلكترونيًا إلى فروع ثلاث:

الفرع الأول: العوائق المرتبطة بالأدلة الإلكترونية

الفرع الثاني: العوائق المرتبطة بالإستدلال والتحقيق والتفتيش والضبط

الفرع الثالث: العوائق المرتبطة بالآليات الفنية وبالآليات التشريعية

---

[1] الجبور، محمد (2012). الجرائم الواقعة على الأشخاص في قانون العقوبات الأردني، دراسة مقارنة، ط1، دار المكتبة الوطنية، ص298.

[2] هروال، نبيلة (2007). الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجتمعي، الإسكندرية، ص217.

الفرع الأول

العوائق المرتبطة بالأدلة الإلكترونية

هناك فارق جوهري يميز جريمة انتهاك البيانات الشخصية التقليدية عن جريمة انتهاكها عبر الوسائل الإلكترونية الحديثة، حيث أن انتهاك البيانات الشخصية بصورة تقليدية يأتي بفعل مادي ملموس يفعله الجاني بشكل مباشر مع الضحية، بينما في جريمة انتهاك البيانات الشخصية إلكترونيًا فلا يحدث انتهاك ملموس بالإضافة إلى تخفي فاعله كما أن انتهاك البيانات الشخصية بالمعنى التقليدي يحتاج إلى جرأة أكبر من نظيره على الشبكة العنكبوتية، مستغلاً أن أحداً لا يعرف شخصيته الحقيقية، فيستخدم ما يساعده في عمله وسائل يقنع بها الضحية، وذلك من خلال "الإنترنت"، ومواقع التواصل الاجتماعي، ومن خلال البريد الإلكتروني، ومن خلال الرسائل الفورية وغيرها[1].

يرى الباحث أن اكتشاف جريمة انتهاك البيانات الشخصية إلكترونيًا يواجه مجموعة من العوائق، منها:

أولاً: عدم وجود الإثبات المرئي، حيث أن الإثباتات في تلك الجرائم يتم استخلاصها من معلومات وبيانات في صورة نبضات إلكترونية غير مرئية[2]، والتي تمر عبر الحاسب الآلي، ومن خلال شبكة "الإنترنت"، وغالبًا مشفرة، ولا يمكن للضحية العادي قراءتها، وبالتالي يمكن للجاني العبث في بيانات الحاسب الآلي وارتكاب جريمته دون ترك أي دليل مادي ملموس، ومحو الدليل في وقت قياسي فلا تصل إليه المحكمة ولا جهات التحقيق[3].

---

(1) حجازي، عبد الفتاح (2004). ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ص 24.

(2) العمري، محمد (2016). الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية، دارسة مقارنة، مجلة العلوم القانونية والسياسية، السنة السادسة، المجلد 2، العدد 2، عمان، الأردن، ص295.

(3) مصطفى، أحمد (2010). جرائم الحاسبات في التشريع المصري، دار النهضة العربية، القاهرة، ص 260.

ويستطيع المجرم طمس دليل جريمته طمسًا كاملاً فيتعذر كشف شخصيته وملاحقته، فضلاً عن أن الجناة الذين يستخدمون الوسائل الإلكترونية في ارتكاب جرائمهم يتميزون بالذكاء، وبالاتقان الفني للعمل الذي يقومون به، مما يسهل لهم إخفاء الدليل، وهذه من الصعوبات التي تعترض الإثبات في مجال الجرائم الإلكترونية، والتي تجعل من إقامة الدليل على هذه الجرائم أمر في منتهى الصعوبة[1].

ثانيا: صعوبات قانونية تتعلق بمدى قبول الأدلة الإلكترونية في الإثبات: حيث تظهر الصعوبات في الأنظمة القانونية التي تأخذ بنظام الإثبات المقيد، والذي يقوم على تقييد القاضي بالأدلة المنصوص عليها في القانون على سيل الحصر، وبالتالي فلا يقبل الدليل الإلكتروني إلا إذا نص القانون على قبوله[2].

وفي الغالب لا يوجد في تلك القوانين نص حجية الأدلة الإلكترونية، وفي المقابل، ففي نظام الإثبات الحر فإن القانون يمنح للخصوصية الحرية الكاملة في اختيار الدليل الذي يقنع القاضي الجزائي، وبالتالي تخض الأدلة الإلكترونية لحرية القاضي الجزائي في تقديرها فقد يأخذ بها وقد يطرحه، ويشترط لقبول الأدلة الإلكترونية الواقعية، ويتعين على القاضي مناقشة كافة مستخرجات الأدلة الإلكترونية مع المتهم، وهو أمر –أيضًا– يتسم بالصعوبة[3].

---

[1] العمري، محمد (2016). الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية، مرجع سابق، عمان، الأردن، ص295.

[2] مصطفى، أحمد (2010). جرائم الحاسبات في التشريع المصري، مرجع سابق، 260.

[3] هروال، نبيلة (2007). الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالاتمرجع سابق، ص217.

ثالثًا. قصور إجراءات الحول على الدليل الإلكتروني: ومن المعلوم أنه يشترط لصحة الدليل الإلكتروني أن يكون الحصول عليه تم بطريقة مشروعة، وبالشروط والإجراءات التي سنتها القوانين، والتي تكمن في إجراءات الحصول على الدليل الإلكتروني في جريمة هتك العرض الإلكتروني؛ حيث أنها إجراءات كثيرة ومرهقة بسبب أن هذه الأدلة غير ظاهرة أو مرئية[1]. وهناك مشكلات عدة تظهر على السطح تتعلق بضبط الأدلة، وذلك عندما تتعدد أماكن ارتكاب الجريمة داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الإنترنت[2].

رابعًا: المشكلات المتعلقة بالاستدلال والتحقيق، حيث أنه مما لا شك فيه أن إجراءات الاستدلال والمعاينة في الجرائم الإلكترونية ليست سهلة كالجرائم العادية بسبب طبيعة الجرائم الإلكترونية، وأن الجناة يقومون بمحو آثار الجريمة وذلك عن طريق مسح ملفات "الكوكيز" الموجودة على أجهزتهم بطرق مختلفة، حيث تظهر هذه الصعوبات في جريمة هتك العرض الإلكتروني من خلال ما يلي[3]:

أ. لا يوجد آثار مادية للجرائم الإلكترونية التي تقع على الشبكة العنكبوتية، ومنها جريمة هتك العرض الإلكتروني.

ب. نسبة الأعداد الكبيرة من الأشخاص الموجودين على مسرح الجريمة خلال مدة قد تطول على الأرجح، ما بين ارتكاب الجريمة وما بين الكشف عنها، فيمكن أن يحدث تغيير، أو تلفيق، أو عبث بآثار الجريمة، أو يمكن أن يزول بعضها.

---

(1) القرعان، محمود (2017). الجرائم الإلكترونية، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2017، ص233.

(2) المصري، نداء (2017). خصوية الجرائم المعلوماتية، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، ص77.

(3) حجازي، عبد الفتاح (2007). مباديء الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، ص182.

ج. عوائق إجراء الاستدلال وعوائق المعاينة التي تختلف حسب موضوع الجريمة الإلكترونية ذاتها، حيث أن الجرائم الواقعة على المكونات المادية للحاسب الآلي– الكمبيوتري، مثل الجرائم الواقعة على كل من: أشرطة الحاسب، والكابلات وسرقة الأقراص تمكن مأموري الضبط القضائي القيام من المعاينة، ومن إجراء التحفظ على الأشياء المادية التي تعد أدلة على ثبوت الجريمة، وعلى ضبطها دون أي عائق، ودون أي إخطار من قبل النيابة العامة.

أما الجرائم الواقعة على المكونات المعنوية، مثل اختراق بيانات الحاسب الآلي أو التزوير المعلوماتي وغيرها من الجرائم التي تقع على أشياء غير مادية، فتبرز عوائق عملية لمعاينتها[1].

د. العوائق المرتبطة بالأنظمة القانونية، والتي تبرز في الأنظمة القانونية التي تأخذ بنظام الإثبات المقيد، والذي يقوم على تقييد القاضي بالأدلة المنصوص عليها في التشريع، وبالتالي فلا يتم التعامل مع الدليل الإلكتروني إلا إذا نص المشرع على إجازته، وبشكل عام لا يوجد في القوانين سابقة الذكر نص على حجية أي دليل إلكتروني[2].

الفرع الثاني

العوائق المرتبطة بالإستدلال والتحقيق والتفتيش والضبط

هناك مجموعة من العوائق يذكرها الباحث على النحو الآتي"[3]

---

[1] هروال، نبيلة (2007). الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، مرجع سابق، ص217.

[2] حجازي، عبد الفتاح (2007). الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص182.

[3] أحمد محمود مطفى، جرائم الحاسبات في التشريع المصري، دار النهضة العربية، القاهرة، 2010، 260.

أولاً: ضعف الخبرة الفنية لدى جهات التحقيق، حيث أن معظم العوائق التي تعترض رجال التحقيق أثناء التحقيق في جريمة هتك العرض خلال الوسائل الإلكترونية الحديثة تحدث بسبب افتقارهم للخبرة الفنية في أساليب وطرق ارتكابها والتي تتم بأحدث الوسائل الإلكترونية، هي كون هذه الجرائم الإلكترونية تعد جرائم حديثة، وكون أن تقنياتها العالية تحتاج من القائمين إلى إجراءات معينة في عملتي التحقيق، والتفتيش، وذلك للإلمام بالأمور الفنية في مجال الجرائم الإلكترونية، للقيام بهذه الإجراءات على الوجه الصحيح القانوني.

ثانيًا: زخم المعلومات (البيانات) التي يجب ضبطها؛ حيث يجد المحقق نفسه أمام مهمة شافة عليه، وهي البحث عن عدد كبير من السجلات الخاصة بأجهزة الحاسب وبالملفات نفسها، وكم كبير من المعلومات على شبكة "الإنترنت" الأمر الذي يستلزم بذل جهد وخبرة فنية كبيرتين[1]

ثالثًا: تجاوز نطاق الدولة، حيث تكمن العوائق– أيضًا في أن معظم المعلومات التي يراد تفتيشها توجد في أجهزة تابعة لدولة غير عربية، مما يلزم زيادة التنسيق الدولي لمكافحتها.

ثالثًا: عدم وجود قواعد معينة للاحتفاظ بالمضبوطات الخاصة بالجرائم الإلكترونية، حيث أنه في الحقيقة يلاحظ أن التشريعات الجنائية لم تعرض لقواعد معينة لحفظ المضبوطات الخاصة بالجرائم الإلكترونية، لاسيما من عملية الإتلاف (للملفات الخاصة)، أو تعريضها لدرجات الحرارة العالية وغيرها من القواعد التي كان يجب النص على اتباعها لحفظ مضبوطات الجرائم الإلكترونية[2].

---

[1] فضل، علي (2003). إبراهيم فضل، الإساءة إلى المرأة، طبعة مكتبة الأنجلو مصرية، القاهرة، ص7.

[2] الجبور، حمد (2012). الجرائم الواقعة على الأشخاص في قانون العقوبات الأردني، مرجع سابق، ص298.

الفرع الثالث

العوائق المرتبطة بالآليات الفنية وبالآليات التشريعية

تعد جريمة انتهاك البيانات الشخصية إلكترونيًا من الظواهر الإجرامية المرتبطة بالجرائم الإلكترونية –على وجه الخصوص– والتي تقرع أجراس الخطر، باعتبارها من الجرائم التي تنشأ في بيئة تمتاز بتوظيف التكنولوجيا من قبل أشخاص من ذوي قدرات تقنية وفنية عالية، والتي أضحت مصدر تهديد للمجتمعات بشكل عام، لذا فإن بذل أقصى جهد لمواجهتها على المستوى التشريعي وعلى المستوى الفني من سلطات التحقيق، ومن الضابطة العدلية على المستويين الدولي والوطني[1].

ولقد تم انشاء قسم للإسناد وللتحقيق الفني –في المملكة الأردنية الهاشمية– لدى إدارة البحث الجنائي الأردني سنة (2008)، للتحقيق في جرائم تكنولوجيا المعلومات وتكنولوجيا "الإنترنت"[2].

وتم تطوير وحدة مكافحة للجرائم الإلكترونية في عام (2015)، واتبعت وحدة مكافحة الجرائم الإلكترونية أساليب تحقيقه في التتبع الفني مثل التصيد الإلكتروني،ومثل الهندسة الاجتماعية التي تعتمد على المهارة الفردية للمحقق، والتي تتبع الهوية الرقمية للمستخدم وصولاً إلى العنوان الرقمي (IP).

---

[1] حجازي، عبد الفتاح (2004). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 24.

[2] البخيت، محمد (2017). المشكلات القانونية والمشكلات العملية في جرائم هتك العرض (دراسة مقارنة)، رسالة ماجستير، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ص16، ص 17.

وتمكن التقنية السابقة من تحديد هوية المستخدم الذي يرتكب الجرائم الإلكترونية(1). وذلك بالتعاون مع المؤسسات ومع الشركات الدولية والمحلية وشركات الاتصالات ومؤسسات المجتمع الدولي[2].

---

(1) البخيت، حمد (2017). المشكلات القانونية والمشكلات العملية في جرائم هتك العرض (دراسة مقارنة)، رسالة ماجستير، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ص16، ص 17.

(2)Hudasi, L (2020). Artificial intelligence usage opportunities in smart city data management. **Interdisciplinary Description of complex Systems**: INDECS, 18(3), 382-388, p112.

الفصل الثالث

الحماية الجزائية للبيانات الشخصية

تبرز الحماية الجزائية للبيانات الشخصية كمطلب أساسي لتقليل مستوى الجريمة الإلكترونية، ومنها جريمة انتهاك حرمة البيانات الشخصية، وما يترتب عليها من مشكلات اجتماعية، واقتصادية، ونفسية للضحايا[1].

وعلى الرغم من أن اقتحام خصوصية الآخرين وبياناتهم الشخصية من قبل أي كان جهة أو أفراد عملاً غير مقبولاً ومرفوضًا، ومجرمًا قانونيًا؛ إلا أن التجاوزات في ارتفاع مستمر[2].

وتتطلب الحماية الجزائية للبيانات الشخصية سن التشريعات التي تنظم البيئة الرقمية من خلال حماية البيانات الشخصية في ظل سهولة جمعها والاحتفاظ بها ومعالجتها[3]. ولمنع الاعتداء على حق المواطنين في حماية بياناتهم الشخصية، وخصوصيتهم المقررة بموجب أحكام الدستور والقوانين ذات العلاقة[4]. وبينت المادة (8) من قانون حماية البيانات الشخصية الأردني تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) إلى (6) من هذا القانون بحق كل من قام بارتكاب أي منها بسبب تأديته وظيفته أو عمله أو باستغلال أي منهما.

---

(1) حسين، آدم (2000). الحق في احترام الحياة الخاصة ومدى الحماية التي يكفلها القانون الجنائي– دراسة مقارنة، دار النهضة العربية، القاهره، ص23.

(2) عثمان، بكر (2016). المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي، أطروحة دكتوراه (غير منشورة)، جامعة طنطا: مصر.

(3) سيد، أشرف جابر والشافي، خالد (2013). حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع فيس بوك، بحث منشور بكلية الحقوق، جامعة حلوان: مصر، ص12.

(4) ربايعة، عبد اللطيف (2016). الجرائم الإلكترونية (التجريم والملاحقة والإثبات)، رسالة ماجستير (غير منشورة)، جامعة اليرموك، إربد: الأردن، ص20.

ولأن الحماية الجزائية ترتبط بصور الجرائم الواقعة على البيانات الشخصية وفقًا لقانون الجرائم الإلكترونية؛ فقد قام الباحث بتناولها على النحو الآتي:

المبحث الأول: صور الجرائم الواقعة على البيانات الشخصية وفقًا لقانون الجرائم الإلكترونية والذي قسمه إلى:

المطلب الأول: أشكال الجرائم الإلكترونية الواقعة على البيانات الشخصية، والذي تناولة من خلال:

الفرع الأول: البوصلة التقنية المعروفة بالكوكيز

الفرع الثاني: التصيد الاحتيالي الإلكتروني

الفرع الثالث: سرقة هوية الشخص

المبحث الأول

صور الجرائم الواقعة على البيانات الشخصية وفقًا لقانون الجرائم الإلكترونية

جاء قانون قانون الجرائم الإلكترونية ساعيًا لأهداف عدة إنبثق تحتها قانون حماية البيانات الشخصية لإيجاد إطار قانوني يوازن بين آليات حقوق الأفراد في حماية بياناتهم الشخصية وبين السماح بمعالجة البيانات والمعلومات والاحتفاظ بها في ظل الفضاء الإلكتروني[2]. بالإضافة إلى انتشار مفاهيم البيانات الضخمة والذكاء الاصطناعي، ولتأسيس أطر تنظيمية لحفظ البيانات الشخصية وإجراء المعالجة عليها ضمن قيود والتزامات واضحة؛ الأمر الذي يعزز الثقة للفرد[3].

وفي هذا الشأن تناول الباحث بعض الصور التي يترتب عليها الاعتداء على خصوصية المعلومات عبر التكنولوجيا الحديثة، والذي قسمه إلى: أشكال الجرائم الإلكترونية الواقعة على البيانات الشخصية (المطلب الأول)، حيث تناولها من خلال البوصلة التقنية المعروفة بالكوكيز (الفرع الأول)، والتصيد الاحتيالي الإلكتروني (الفرع الثاني)، وسرقة هوية الشخص (الفرع الثالث)

---

(1) لامي، بارق (2017). جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، مرجع سابق، ص20.

(2) الجمعية الأردنية للمصدر المفتوح (2022). مشروع قانون حماية البيانات الشخصية لسنة (2022)، التقرير السنوي لعام 2022، ص6.

(3) وزارة الاقتصاد الرقمي والريادة (2021). قانون حماية البيانات الشخصية لسنة (2021)، التقرير السنوي لعام 2021، ص9.

المطلب الأول

صور الجرائم الإلكترونية

تعبر أشكال الكشف عن المعلومات الشخصية التي يستخدمها الآخرون للتعدي على خصوصيات الأفراد، والتي تشمل معلومات حساسة مثل عنوان (IP)، أو عنوان البريد الإلكتروني، والموقع الجغرافي، وعنوان المنزل والعمل الخاص بالضحية عن ضرورة التفكير في آلية تمنع ممارسة التطفل على الآخرين واقتحام خصوصياتهم[1]. لذا تناول الباحث في هذا المطلب أشكال (صور) هذا التطفل الخاص بالمعلومات الشخصية التي تبرز جريمة التعدي على خصوصيات الأشخاص من خلال فروع ثلاث:

الفرع الأول

البوصلة التقنية المعروفة بالكوكيز

تضع معظم مواقع الويب، عندما يتم زيارتها ملفًا صغيراً على القرص الصلب الخاص بحاسوب الشخص المعني؛ حيث يتصل بالخادم الخاص وبالموقع الذي تتم زيارته من قبله؛ ويقوم هذه الخادم بإرسال هذه الملفات إلى القرص الصلب الخاص بحاسوب المستخدم عند زيارة هذا الأخير لأي موقع من المواقع على شبكة الإنترنت[2]. ويحتفظ بنسخة من هذه الرسائل لديه؛ وقد يتعرض المستخدم لانتهاك خصوصيتهم، وجمع المعلومات عنهم خلال تصفحهم للمواقع؛ حيث يستطيع الكوكيز معرفة عنوان (IP)، وكذلك طريقة الاتصال بالإنترنت والمواقع التي يتم زيارتها، ونوع الجهاز المعالج وكذلك البيانات التي يطلب من المستخدم إدخالها كالاسم والبريد الإلكتروني، ورقم البطاقة الائتمانية والعنوان وغير ذلك من البيانات[3].

---

(1) تومي، فضيلة (2017). أيديولوجيات الشبكات بالاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، مرجع سابق، ص30.

(2) العنزي، زياد (2018). المسؤولية القانونية عن طرد عضو من المجموعة في مواقع التواصل الاجتماعي، مرجع سابق، ص12.

(3) العنزي، زياد (2018). المسؤولية القانونية، المرجع السابق، ص12.

الفرع الثاني

التصيد الاحتيالي الإلكتروني

يقصد بالتصيد الاحتيالي مجموعة من التقنيات التي يستخدمها الهاكرز من أجل جمع المعلومات الشخصية عن مستخدمي الإنترنت[1]. ويعد التصيد الاحتيالي من أكثر الطرق انتشاراً لقرصنة حساب فسيبوك؛ بحيث يقوم قراصنة التصيد بإنشاء صفحة تسجيل وهمية أو إنشاء استنساخ من صفحة تسجيل الدخول المختصة بالمستخدم، بحيث يبدو من خلال المظهر الخارجي لها أنها تمثل صفحة فسيبوك الحقيقية[2].

كما أن التصيد يستخدم الرسائل الخاصة بالبريد الإلكتروني من أجل الحصول على الأموال بطرق احتيالية، وكذلك إلى جمع المعلومات السرية التي نقل معظمها من رسائل البريد الإلكتروني؛ بهدف الاعتداء إلى سرقة المعلومات السرية مثل الاسم والعنوان وكلمة السر ورقم بطاقة الائتمان ورقم الهاتف وغيرها من البيانات[3].

ويبدو ذلك من خلال قيام القراصنة باستخدام مواقع الويب الزائفة ورسائل البريد الإلكتروني الخاصة بالهيئات الحكومية أو مواقع مصارف أو بنوك أو العلاقات التجارية الكبرى لإقناع مستخدمي الإنترنت بالكشف عن تفاصيل بطاقات الائتمان الخاصة بهم أو عن أي بيانات أو معلومات شخصية يمكن استخدامها في الوصول إلى حسابات مصرفيه أو تغطية عمليات تبييض أموال أو غير ذلك من تصرفات تتاج إلى إثبات هوية[4].

---

(1) المؤيد، محمد (2009). صور المسؤولية التقصيرية الناشئة عن الاعتداء على بيانات الكمبيوتر والتعامل عبر الإنترنت وتسوية منازعاتها، مجلة الدراسات الاجتماعية، المجلد الثاني، العدد الثامن والعشرون، ص20.

(2) لامي، بارق (2017). جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، مرجع سابق، ص20.

(3) جبالي، كامل (2016). حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق، جامعة أسيوط في الفترة من (12–13) إبريل.

(4) الغويري، ضيف الله (2014). ضمانات الحق في الحماية الخاصة في النظام السعودي، مرجع سابق، ص20.

الفرع الثالث

سرقة هوية الشخص

يقصد بسرقة هوية الشخص قيام شخص بسرقة هوية شخص آخر، ويتظاهر أمام الناس بأنه الشخص نفسه من أجل الحصول على أمواله؛ كما يمكن أن يكون ذلك من أجل تحقيق أغراض مختلفة مثل طلب قرض أو شراء السلع أو البضائع نيابة عنه، أو الاستفادة من الخدمات التي يتمتع بها المضرور مثل خدمات التأمين الصحي عن طريق الاستعانة بتقديم المستندات الخاصة بهذا الأخير مثل جواز السفر أو بطاقة التأمين الصحي[1]. وترتبط مشكلة سرقة هوية الشخص بالبرامج الضارة المثبتة على جهاز الحاسوب، والتي تشير بدورها إلى البرامج العدائية أو المتطفلة أو المزعجة التي تتسلل مستترة لأجهزة الحاسوب، والتي يطلق عليها ونسميتها بالبرامج الضارة يرجع إلى أنها ناشئة عن الكلمات (Malicious) بمعنى خبيث وكلمة (software) بمعنى برنامج[2]

وتثبت هذه البرامج الخبيثة بدون علم المستخدم المضرور من أجل جمع المعلومات الأكثر خصوصية، وكذلك الحصول على الدخول غير المرخص للأنظمة المعلوماتية[3].

وهناك عدة أنواع من البرامج الضارة؛ حيث يعتبر أخطرها هو (Ngkeyloggi) الذي يرصد لوحة المفاتيح الخاصة بالمستخدم دون علمه؛ كما يمكنها معرفة كلمة المرور والرسائل الخاصة، وكذلك المعلومات الأكثر خصوصية للمستخدم، ثم تقوم بإرسالها إلى الهاكرز أو المحتالين من أجل تحليلها واستخلاص المعلومات ذات الأهمية للمستخدم[4].

---

(1) الجمعية الأردنية للمصدر المفتوح (2022). مشروع قانون حماية البيانات الشخصية، مرجع سابق، ص9.

(2) وزارة الاقتصاد الرقمي والريادة (2021). قانون حماية البيانات الشخصية لسنة (2021)، مرجع سابق، ص6.

(3) السكر، سلطان فياض (2022). جريمة انتهاك سرية المعلومات عبر الوسائل الالكترونية ، مرجع سابق، 20.

(4) ظاهر، سفيان (2023). الحماية الجزائية لصورة الانسان الشخصية عبر الوسائل الالكترونية، دراسة مقارنة، رسالة ماجستير (غير منشورة)، كلية الحقوق جامعة الزرقاء، الزرقاء: الأردن.

ويعد استخدام البيانات الشخصية الخاصة بقبول مستخدم جديد على مواقع التواصل الاجتماعي، حيث يعاني مستخدمي الفيس بوك يوميًا من بعض المخاطر عند تقديمهم طلبات تسجيل الشبكات الاجتماعية، ومن هذه المخاطر: اختراق الحساب، وتوزيع الصور الفاضحة، وصعوبة إزالة أو إلغاء الحساب، وما إلى ذلك[1].

فإذا لتتوافر الحماية بطريقة كافية للمعلومات عن طريق الإعدادات؛ فإن هذه المعلومات تصبح متاحة، ويمكن استخدامها من أجل تحقيق أغراض غير مرغوب فيها أو غير قانونية[2].

ومن هذا المنطلق، يجب مراعاة الحيطة والحذر من جانب مستخدمي مواقع التواصل الاجتماعي حتى لا يتعرضون إلى أضرار الشبكات الاجتماعية ومحاولة السيطرة على سمعتهم الرقمية؛ فهذه الأخيرة تعتمد بشكل كبير على المستخدم نفسه بالنظر إلى أنه هو الذي يقوم بنشر المعلومات والصور الخاصة به، وكذلك مشاركة الروابط على الشبكات الاجتماعية؛ لأن هذه المجموعة تمثل ملفه الشخصي الرقمي[3].

ولأن الصور أو الأشكال السابقة التي طرحها الباحث ترتبط بضرورة وجود عقوبات حاسمة، قام الباحث بتناول عقوبات انتهاك حرمة البيانات الشخصية المنفذة تكنولوجيا في المطلب الثاني:

---

(1) الخلايلة، عايد (2011. المسؤولية التقصيرية الالكترونية، دراسة مقارنة، (ط2)، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص20.

(2) حموري، شهد والمصري، ريم (2014). قانون حماية البيانات الشخصية الأردني، ما يمكن تعلمه من تجارب الدول الأخرى، مقالة منشورة على مدونة حبر، متاحة عبر الرابط الإلكتروني: www:7iber.com/wp-content/uploads/2016/01/Reem.pdf.، تمت الزيارة بتاريخ: 15-9-2023، الساعة 8:35 صباحًا.

(3) المغربي، جعفر محمود وعساف، حسين شاكر (2010). المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول، دار الثقافة للنشر والتوزيع، عمان، الأردن، ص20.

يرى الباحث أن قانون الجرائم الإلكترونية رقم (17) لسنة (2023) الحالي لم يفصل هذه الصور مقارنة بالقانون السابق، وذلك من خلال ما يلي:

أولاً: الإشارة إلى العقوبة الجزائية بالنسبة لانتهاك هذه البيانات، وليس بالنسبة لصورها، حيث بينت المادة (3/ أ) منه على أنه: (يعاقب كل من دخل أو وصل قصداً إلى الشبكة المعلوماتية أو نظام المعلومات أو وسيلة تقنية المعلومات أو أي جزء منها بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح بالحبس مدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر أو بغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (600) ستمائة دينار أو بكلتا هاتين العقوبيتين).

ثانيًا: مساواة العقوبة الجزائية لصور انتهاكات البيانات في المادة (4/أ) من القانون الحالي: (إذا كان الدخول أو الوصول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو نشرها أو غعادة نشرها أو خسارة سريتها أو تشفيرها أو حذفها أو إضافتها أو حجبها أو إفشلئها أو التقاطها فيعاقب الفاعل بالأشغال المؤقتة وبغرامة لا تقل عن (5000) خمسة الآف دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار، ويعاقب بالأشغال المؤقتة مدة لا تقل عن خمس سنوات والغرامة (25000) خمسة وعشرين ألف دينار إذا تمكن من تحقيق النتيجة).

المطلب الثاني

عقوبات انتهاك حرمة البيانات الشخصية المنفذة تكنولوجيا

يقوم المجرمون بنشر معلومات عن الضحايا، وقد يقوم الأصدقاء بالكتابة عنهم أو نشر صور لهم ولعائلاتهم، ويمكن أن تكون سجلات الجهات الحكومية قابلة للبحث-على سبيل المثال-، كصور منازلهم وقيمته، وشهادات ميلادهم، ونسخ من توقيعهم[1]

وقد تكشف مجموعات الأنشطة التي يرتداها الضحايا؛ كالنوادي والروابط الاحترافية عن اسمهم بالكامل أو مكان عملهم أو تاريخ تبرعهم[2].

وهذا يتطلب إيجاد عقوبات حاسمة بحق المجرمين الذين ينتهكون هذه البيانات ويستخدموها لأغراض عدة؛ إلا أن المشرع الأردني لم يُفصّل هذه العقوبات فيما يخص انتهاك حرمة البيانات الشخصية إلا في حالات محددة، قام الباحث بتناولها في فروع ثلاث، هي:

الفرع الأول: عقوبة الدخول قصداً إلى الشبكة المعلوماتية

الفرع الثاني: عقوبة استخدام وسيلة إلكترونية للضرر بالبيانات

الفرع الثالث: عقوبة الدخول دون تصريح للبيانات

---

(1) حموري، شهد والمصري، ريم (2014). قانون حماية البيانات الشخصية الأردني، ما يمكن تعلمه من تجارب الدول الأخرى، مقالة منشورة على مدونة حبر، متاحة عبر الرابط الإلكتروني: www:7iber.com/wp-content/uploads/2016/01/Reem.pdf.، تمت الزيارة بتاريخ: 15-9-2023، الساعة 8:35 صباحً، مرجع سابق. Muise, A., Christofides, E., & Desmarais, S(2009). More information than you ever wanted: Does Facebook bring out green –eyed monster of jealousy, CyberPSYChology & Behavior. 12(4), 441-444

(2) Change, W. (2019). A. Data Environmental Management Systems in the Convention and Exhibition Industry. *Ekoloji Dergisi*.(107). المغربي، جعفر محمود وعساف، حسين شاكر (2010). المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول، دار الثقافة للنشر والتوزيع، عمان، الأردن، ص12

الفرع الأول
عقوبة الدخول قصداً إلى الشبكة المعلوماتية

تم تحديد عقوبة جريمة الدخول قصداً إلى الشبكة المعلوماتية في قانون الجرائم الإلكترونية رقم (17) لسنة (2023) على النحو التالي:

أولاً: الحبس مدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر أو بغرامة مالية لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (600) ستمائة دينار.

حيث نصت المادة (3/ أ) من هذا القانون على أنه: (يعاقب كل من دخل أو وصل قصداً إلى الشبكة المعلوماتية أو نظام المعلومات أو وسيلة تقنية المعلومات أو أي جزء منها بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح بالحبس مدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر أو بغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (600) ستمائة دينار أو بكلتا هاتين العقوبيتين).

ثانيًا: الحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن (3000) ثلاثة الآف دينار ولا تزيد على (1500) خمسة عشر ألف دينار.

حيث فصلت المادة (3/ب) من هذا القانون الحديث في جريمة الدخول قصداً إلى الشبكة المعلوماتية بقولها: (إذا كان الدخول أو الوصول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو نشر او إعادة نشر أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو خسترة سريتها أو تشفير أو إيقاف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات أو تقنية معلومات أو أي جزء منها فيعاقب الفاعل بالحبس مدة

لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن (3000) ثلاثة الآف دينار ولا تزيد على (1500) خمسة عشر ألف دينار إذا تمكن من تحقيق النتيجة).

ثالثًا: الحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (600) ستمائة دينار ولا تزيد على (3000) ثلاثة آلاف دينار).

حيث نصت المادة (3/ج) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023): (يعاقب كل من دخل أو وصل قصداً إلى موقع إلكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو تشفيره أو إيقافه أو تعطيله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (600) ستمائة دينار ولا تزيد على (3000) ثلاثة آلاف دينار).

رابعًا: الأشغال المؤقتة وبغرامة لا تقل عن (5000) خمسة الآف دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار.

حيث نصت المادة (4/أ) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023): (إذا كان الدخول أو الوصول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو نشرها أو إعادة نشرها أو خسارة سريتها أو تشفيرها أو حذفها أو إضافتها أو حجبها أو إفشائها أو التقاطها فيعاقب الفاعل بالأشغال المؤقتة وبغرامة لا تقل عن (5000) خمسة الآف دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار، ويعاقب بالأشغال المؤقتة مدة لا تقل عن خمس سنوات والغرامة (25000) خمسة وعشرين ألف دينار إذا تمكن من تحقيق النتيجة).

خامسًا: الحبس مدة لا تقل عن أربعة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار).

حيث نصت المادة (4/ج) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023): (يعاقب كل من دخل أو وصل قصداً إلى موقع إلكتروني يعود للوزارات أو الدوائر الحكومية أو المؤسسات الرسمية العامة أو المرسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار).

الفرع الثاني

عقوبة استخدام وسيلة إلكترونية للضرر بالبيانات (قانون الجرائم الإلكترونية رقم (17) لسنة (2023)، وقانون الاتصالات الأردني، وقانون العقوبات الأردني حتى 2023)

حدد قانون الجرائم الإلكترونية رقم (17) لسنة (2023)، وقانون الاتصالات الأردني، وقانون العقوبات الأردني حتى (2023) عقوبة استخدام وسيلة إلكترونية للضرر بالبيانات على النحو التالي:

أولاً: الحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن (1500) ألف وخمسمائة دينار ولا تزيد على (1500) خمسة عشر ألف دينار.

حيث نصت المادة (5/أ) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023) على: (يعاقب كل من قام بإنشاء حساب أو صفحة أو مجموعة أو قناة أو ما يماثلها على منصات التواصل

الاجتماعي ونسبها زوراً إلى شخص طبيعي أو معنوي بالحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن (1500) ألف وخمسمائة دينار ولا تزيد على (1500) خمسة عشر ألف دينار أو بكلتا هاتين العقوبيتين).

ثانيًا: الأشغال المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن (25000) خمسة وعشرين ألف دينار ولا تزيد على (75000) خمسة وسبعين ألف دينار.

حيث بينت المادة (8) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023) أنه: (يعاقب كل من قام بأحد الأفعال المنصوص عليها في المواد (3) و(5) و(6) و(7) و(8) من هذا القانون إذا وقعت على نظام المعلومات أو تقنية المعلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع أو التقاص أو التسويات أو أي من الخدمات المصرفية المقدمة من البنوك والشركات المالية بالأشغال المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن (25000) خمسة وعشرين ألف دينار ولا تزيد على (75000) خمسة وسبعين ألف دينار.

ثالثًا: الحبس مدة لا تقل عن ستة أشهر أو بغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار).

حيث بينت المادة (12) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023): (كل من تحايل على العنوان البروتوكولي باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها يعاقب بالحبس مدة لا تقل عن ستة أشهر أو بغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار).

رابعًا: الحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على 200 دينار.

بينت المادة (76) من قانون الاتصالات الأردني حتى عام (2023): (كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على 200 دينار أو بكلتا العقوبيتين).

خامسًا: الحبس مدة لا تزيد على سنتين

حيث نصت المادة (161) من قانون الاتصالات الأردني حتى عام (2023): (كل من شجع غيره بالخطابة أو الكتابة، أو بأية وسيلة أخرى على القيام بأي فعل من الأفعال التي تعتبر غير مشروعة بمقتضى المادة (156) من هذا القانون يعاقب بالحبس مدة لا تزيد على سنتين).

سادسًا: الحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على خمسين ديناراً.

نصت المادة (163) من قانون الاتصالات الأردني حتى عام (2023): (كل من طبع، أو نشر، أو باع، وعرض للبيع أو أرسل بالبريد كتابًا، أو نشره، أو كراسًا، أو إعلانًا، أو بيانًا، أو منشوراً، أو جريدة لجمعية غير مشروعة أو لمنفعتها، أو صادرة منها يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على خمسين ديناراً).

يلاحظ الباحث من خلال العقوبات التي تم عرضها ما يلي:

1. شدد قانون الجرائم الإلكترونية الحالي في مدة الحبس وفي مبلغ الغرامة.
2. لم يتناول قانون العقوبات الأردني الحالي ما يخص عقوبة الدخول قصداً إلى الشبكة المعلوماتية، وعقوبة استخدام وسيلة إلكترونية للضرر بالبيانات من حيث الغرامة والحبس.

3. لم يحدد قانون الاتصالات الأردني الحالي عقوبة صارمة فيما يخص استخدام وسيلة إلكترونية للضرر بالبيانات، حيث نصت المادة (71) منه: (كل من نشر أو أشاع مضمون أي اتصال بواسطة شبكة اتصالات عامة أو خاصة أو رسالة هاتفية اطلع عليها بحكم وظيفته أو قام بتسجيلها دون سند قانوني يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (100) دينار ولا تزيد على (300) دينار أو بكلتا العقوبيتين. وكذلك حدد عقوبة مخففة مقارنة بقانون الجرائم الإلكترونية فيما يخص الدخول قصداً إلى الشبكة المعلوماتية، والتي بينها الباحث–سابقًا–

4. أعطى قانون الجرائم الغلكترونية الحالي صلاحيات أوسع للمدعي العام المختص وللمحكمة المختصة صلاحيات إصدر أمر إلى القائمين على نظام المعلومات الإلكتروني وصلاحيات في التعامل مع هذا النوع الجديد من الجرائم الإلكترونية مقارنة بقانوني الاتصالات والعقوبات الحاليين، حيث أعطت المادة (33/أ) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023) للمدعي العام المختص وللمحكمة المختصة اتخاذ ما يلي:

أولاً: إزالة أو حظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو أي منشور أو محتوى أو منع الوصول إليه أو حظر المستخدم أو الناشر مؤقتًا خلال المدة المحددة في القرار.

ثانيًا: إزالة أو حظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو أي منشور أو محتوى أو منع الوصول إليه أو حظر المستخدم أو الناشر مؤقتًا خلال المدة المحددة في القرار.

ثالثًا: الحفظ العاجل للبيانات والمعلومات اللازمة لإظهار الحقيقة وتخزينها والمحافظة على سلامتها.

رابعًا: الحفاظ على السرية.

كما أن قانون الجرائم الإلكترونية الحالي في نص المادة (31/ أ) بين أن المحكمة تقضي في حال الإدانة بما يلي:

أولاً: مصادرة الأجهزة أو البرامج أو الأدوات أو الوسائل أو المواد المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال منها.

ثانيًا: وقف او تعطيل أو حجب عمل أي نظلم معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانونن كليًا أو جزئيًا للمدة التي تقررها المحكمة.

ثالثًا: حذف المعلومات أو البيانات على نفقة الفاعل.

رابعًا: إغلاق المحل الذي استخدم لارتكاب أي من الجرائم المنصوص عليها في هذا القانون لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة.

في حين أن المادة (64) من قانون الاتصالات الأردني الحالي أعطى صلاحيات أقل في التعامل مع جريمة انتهاك البيانات الشخصية للمواطن الأردني، حيث حددها بما يلي:

1- لموظفي الهيئة ضبط أي أجهزة أو معدات اتصال غير مرخصة أو مخالفة للقانون أو تستعمل في نشاط غير مرخص له قبل إيصاال خطي يبين نوع الأجهزة ومواصفاتها وتسليم هذه الأجهزة إلى الهيئة).

2- تصادر المضبوطات غير القابلة للترخيص أما الأجهزة المسموح بترخيصها فيتم الاحتفاظ بها إلى حين ترخيصها.

3- وجود نص وحيد في هذا القانون يشير إلى العقوبة دون تحديدها في المادة (65/ب): (لا يجوز نشر أو إشاعة مضمون الرسائل التي تم التقاطها في معرض تتبع مصدر الرسالة بموجب الفقرة (أ) من هذه المادة، ويعاقب الموظف الذي يقوم بنشر أو إشاعة مضمون تلك الرسائل بالعقوبات المقررة قانونًا).

المبحث الثاني

الأساس القانوني لقيام المسؤولية الجزائية وموقف المشرع الأردني من جريمة انتهاك الحياة الخاصة

يعد مشروع قانون حماية البيانات الشخصية الأردني لسنة (2022) من القوانين المهمة التي تعد الأساس القانوني لقيام المسؤولية الجزائية، والذي يعنى بقضايا جرمية عدة، منها الجرائم الإلكترونية، التي تتطلب أن يكون قانون الجرائم الإلكترونية الأردني وقانون حماية البيانات الشخصية الأردني –الذي أشار إليهما الباحث في الأبواب السابقة من رسالته الحالية– قادرين على تنظيم ومواجهة الجرائم الصادرة عن البيئة الرقمية لغايات حفظ حقوق المواطنين الأردنيين والمقيمين وخصوصيتهم المقررة بموجب أحكام الدستور والقوانين ذات العلاقة.

لذا قام الباحث بتقسيم هذا المبحث إلى مطلبين:

المطلب الأول: موقف المشرع الأردني من التعدي على البيانات الشخصية الإلكترونية والوسائل الجرمية لانتهاكها

المطلب الثاني: موقف المشرع الأردني من جريمة انتهاك الحياة الخاصة

المطلب الأول

موقف المشرع الأردني من التعدي على البيانات الشخصية الإلكترونية والوسائل الجرمية لانتهاكها

ترتبط البيانات الشخصية بالمعاملات التكنولوجية (عبر الإنترنت)؛ حيث يرتبط–على سبيل المثال– لا الحصر تسجيل الاشتراك في خدمة ما أو شراء شيء ما– بمعلومات مثل عنوان شحن، أو رقم بطاقة ائتمان، ولكن في معظم الحالات، تقوم الشركات بشكل عام بجمع البيانات عن طريق الاسم، وتعقب مواقع الويب، وصفحات الويب التي يقوم الضحايا بزيارتها[1].

ولأن جريمة انتهاك البيانات الشخصية للأفراد من الجرائم الخطيرة قام الباحث بتناول موقف المشرع الأردني في هذا المطلب منها وبشكل مفصل، وذلك على النحو الآتي:

الفرع الأول: موقف المشرع الأردني من جريمة الوصول إلى عنوان (IP) للضحية وجريمة السرقة

الفرع الثاني: موقف المشرع الأردني من الوسائل الجرمية لانتهاكات البيانات الشخصية

---

(1) حموري، شهد والمصري، ريم (2014). قانون حماية البيانات الشخصية الأردني، ما يمكن تعلمه من تجارب الدول الأخرى، مقالة منشورة على مدونة حبر، متاحة عبر الرابط الإلكتروني: www:7iber.com/wp-content/uploads/2016/01/Reem.pdf.، تمت الزيارة بتاريخ: 15-9-2023، الساعة 8:35 صباحًا، مرجع سابق، ص20.

الفرع الأول

موقف المشرع الأردني من جريمة الوصول إلى عنوان (IP) للضحية وجريمة السرقة

أولاً: جريمة الوصول إلى عنوان (IP)

وعلى الرغم من خطورة الوصول إلى عنوان (IP) للضحية إلا أن المشرع الأردني لم يتطرق بالتفصيل إلى هذه الجزئية الخطيرة في أمن البيانات الشخصية الإلكترونية[1]. وإنما أشار لها بشكل عام في نص المادة (9/ب) من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015، حيث بين: (يعاقب كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا أو عقليا، أو توجيهه أو تحريضه على ارتكاب جريمة، بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة آلاف دينار). ونصت المادة (9/أ) من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015: (أ- يعاقب كل من ارسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالا إباحية وتتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة آلاف دينار). خاصة أن المعلومات عملية تعتمد في خصوصيتها على الإنترنت، وعلى إمكانية التحكم بما ما يتوافر منها للوصول إليها من قبل المجرمين[2].

---

[1] المغربي، جعفر محمود وعساف، حسين شاكر (2010). المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول، مرجع سابق، ص20

[2] الخلايلة، عايد (2011. المسؤولية التقصيرية الالكترونية، دراسة مقارنة، (ط2)، مرجع سابق، ص13,

وفي ظل تسهيل الأفراد إمكانية الوصول إلى بياناتهم الشخصية؛ عند قيامهم بالأنشطة اليومية عبر الإنترنت، حيث يمكنهم الكشف عن معلوماتهم الشخصية دون قصد، ويمكن أن يشمل ذلك معلومات حساسة مثل عناوين منازلهم أو بيانات عملهم، خاصة أن معاملات التسويق عبر الإنترنت –غالبًا– ما تتطلب بطاقة الائتمان وعنوان المنزل[1]. ويمكن الوصول إلى المعلومات الشخصية للأفراد من خلال جمع البيانات التي تقوم بها بعض الشركات والحكومات والمؤسسات، وذلك من خلال إعداد حساب إلكتروني، وإجراء عملية شراء، والتسجيل في مسابقات، والتقاط جزء في أحد الاستطلاعات، وتنزيل البرامج مجانًا، وتصفح الويب، واستخدام التطبيقات على جهاز الحاسوب الخاص بالضحايا، ونشر الصور أو الحالة الخاصة بهم إلكترونيًا[2].

وبالتالي يرى الباحث أن ما تقوم به بعض الشركات يسهل اختراق البيانات الشخصية الإلكترونية للأفراد، وذلك من خلال[3]:

أولاً: قد تستخدم الشركات والقائمين على التوظيف هذه المعلومات، والتي تشكل سنعة الضحايا، لقياس مدى ملائمتها للطلب الذي تقدمت به الضحية بحسن نية، كطلب العمل.

ثانيًا: قد يستخدم المجرمون بيانات إلكترونية لاستهداف الضحايا بالرسائل الخادعة للتصيد الاحتيالي، وسرقة هوياتهم، وارتكاب الجرائم.

ثالثًا: يمكن البحث عن المعلومات والبيانات الخاصة الإلكترونية للضحايا المخزنة على الورق، والمخزنة إلكترونيًا لإنشاء ملف تعريفي كامل خاص بالضحية.

---

(1) الشوابكة، محمد امين (2011). جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص30.

(2) الزعبي، علي احمد (2006). حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، مرجع سابق، ص20.

(3) Cortellazzo, L., Bruni, E., and Zampieri, R., (2019). The Role of Leadership in a Digitalized World: Ar reciew, Front Psychol. 10(1), 12-44

ثانيًا: جريمة سرقة البيانات الشخصية الإلكترونية:

إن سرقة البيانات معروفة أيضًا بسرقة المعلومات، وهي النقل غير القانوني لمعلومات شخصية أو سرية أو مالية، ويمكن لهذه المعلمات أن تشمل كلمات مرور أو كود برنامج أو خوارزميات أو عمليات أو تقنيات خاضعة لحقوق الملكية، وتعتبر سرقة البيانات انتهاكًا كبيراً للأمن، والخصوصية مع احتمالية وقوع عواقب وخيمة بالنسبة لكل من الأفراد والشركات[1].

ويقصد بسرقة البيانات عملية سرقة معلومات رقمية مخزنة على أجهزة الحاسوب أو خوادم أو أجهزة إلكترونية للحصول على معلومات سرية أو انتهاك الخصوصية[2]. ويمكن أن تكون البيانات المسروقة أي شيء من معلومات الحساب المصرفي إلى كلمات المرور على الإنترنت، ورقم جواز السفر، ورقم رخصة القيادة، ورقم الضمان الاجتماعي، والسجلات الطبية[3].

وتشمل سرقة البيانات الشخصية الإلكترونية–كذلك–وصول شخص غير مصرح له إلى معلومات شخصية أو مالية يمكنه حذفها أو تغييرها أو منع الوصول إليها بدون إذن المالك[4]. وتحدث سرقة البيانات في العادة بسبب رغبة جهات ضارة في بيع المعلومات أو استخدامها في سرقة الهوية[5].

---

(1) الهميم، عبد اللطيف (2003). احترام الحياة الخاصة، مرجع سابق، ص22.

(2) الهميم، عبد اللطيف (2003). مرجع سابق، ص22.

(3) الزعبي، علي احمد (2006). حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، مرجع سابق، ص20.

(4) الشوابكة، محمد امين (2011). جرائم الحاسوب والانترنت، مرجع سابق، ص19

(5) الهيتي، محمد حماد (2006)، جرائم الحاسوب، دراسة تحليلية، دار المناهج للنشر والتوزيع، الطبعة الاولى، عمان، الأرد، ص12.

ويمكن للصوص البيانات من سرقة معلومات كافية، ويمكنهم استخدامها للوصول إلى حسابات آمنة أو إصدار بطاقات ائتمان باستخدام اسم الضحية أو استخدام هوية الضحية بطريقة أخرى لصالح أنفسهم[1]. وكانت سرقة البيانات في وقت من الأوقات مشكلة كبيرة للشركات والمؤسسات، ولكن إزداد الوضع سوءاً، وصارت الآن مشكلة متنامية للأفراد كذلك[2]. وكلمة "سرقة" في مصطلح سرقة البيانات لا تعني حرفيًا نزع المعلومات من الضحايا، بل ما يحدث عند سرقة البيانات هو أن الجاني بكل بساطة ينسخ معلومات الضحايا كي يستخدمها هو بنفسه[3].

وتحدث جريمة سرقة البيانات الشخصية إلكترونيًا لغايات التعدي على التالية:

أ. **الأمن الوطني أو العلاقات الخارجية للأردن أو السلامة العامة أو الاقتصاد الوطني؛** حيث نصت المادة (4/ج) من قانون الجرائم الإلكترونية الحالي: (يعاقب كل من دخل أو وصل قصداً إلى موقع إلكتروني يعود للوزارات أو الدوائر الحكومية أو المؤسسات الرسمية العامة أو المؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار).

---

(1) الشوابكة، محمد امين (2011). جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص11.

(2) الزعبي، علي احمد (2006). حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، طرابلس: بيروت، ص20.

(3) الشوابكة، محمد امين (2011). جرائم الحاسوب والانترنت، مرجع سابق، ص20.

ب. **تشويه سمعة الضحية (القدح والذم)**؛ حيث نصت المادة (76) من قانون الاتصالات الأردني لعام (2023): (كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على 200 دينار أو بكلتا العقوبيتين).

ج. إدخال الضحية في قضايا الشرف (الترويج للدعارة)؛ حيث فرضت المادة (13) من قانون الجرائم الإلكترونية الأردني الحالي: الغرامة على من ينقل أو يروج للأعمال الإباحية الجنسية، حيث نصت على أنه: (يعاقب كل من أرسل أو نشر أو أعد أو أنتج أو حفظ أو عالج أو عرض أو طبع أو اشترى أو باع أو نقل أو روج أنشطة أو أعمالاً إباحية باستخدام الشبكة المعلوماتية، أو تقنية المعلومات أو نظام المعلومات أو موقع إلكتروني بالحبس مدة لا تقل عن ستة أشهر أو بغرامة لا تقل عن 3000 آلاف دينار ولا تزيد على 6000 آلاف دينار).

د. الاستغلال المالي؛ حيث لم ينص القانون الحالي صراحة على الاستغلال المالي ولكنه دار حوله بنص المادة (23) منه: (كل من أنشأ أو أدار موقعًا إلكترونيًا أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو تقنية المعلومات أو أدار محفظة إلكترونية للدعوة أو الترويج لجمع التبرعات أو الصدقات دون ترخيص بالحبس مدة لا تقل عن 6 أشهر ولا تزيد على سنة، وبغرامة لا تقل عن ثلاثة آلاف دينار ولاى تزيد على خمسة آلاف دينار)

ويمكن استخدام مصطلح انتهاك البيانات الشخصية الإلكترونية، وأيضًا تسرب البيانات بشكل تبادلي عند مناقشة سرقة البيانات، لكنهما في الحقيقة مختلفان؛ حيث يحدث تسرب البيانات عند الكشف عن بيانات حساسة عن طريق الخطأ، سواء عبر الإنترنت أو عبر محرك أقراص صلبة،

ويوفر هذا للمجرمين الإلكترونيين إمكانية الوصول بشكل غير مصرح به إلى بيانات حساسة بدون أي جهد من جانبهم[1].

وعلى النقيض، يشير انتهاك البيانات الشخصية إلى هجمات إلكترونية متعمدة[2].

يلاحظ الباحث أن قانون الجرائم الإلكترونية رقم (17) لسنة (2023) الحالي لم يفص موضوع (IP)، وإنما عرض لها بشكل عام في أكثر من نص، منها ما جاء في نص المادة (8): (يعاقب كل من قام بأحد الأفعال المنصوص عليها في المواد (3) و(5) و(6) و(7) و(8) من هذا القانون إذا وقعت على نظام المعلومات أو تقنية المعلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع أو التقاص أو التسويات أو أي من الخدمات المصرفية المقدمة من البنوك والشركات المالية بالأشغال المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن (25000) خمسة وعشرين ألف دينار ولا تزيد على (75000) خمسة وسبعين ألف دينار.

---

[1] الهيتي، محمد حماد (2006)، جرائم الحاسوب، دراسة تحليلية، دار المناهج للنشر والتوزيع، الطبعة الاولى، عمان، الأرد، ص12.

[2] الهميم، عبد اللطيف (2003). احترام الحياة الخاصة، دار عمان للنشر والتوزيع، عمان، ص20.

الفرع الثاني

موقف المشرع الأردني من الوسائل الجرمية لانتهاكات البيانات الشخصية

تحدث سرقة البيانات الشخصية الإلكترونية أو السرقة الرقمية من خلال مجموعة من الأساليب التي يعتمدها المجرمون، قام الباحث بتناولها من خلال:

أولاً: الوسائل الجرمية المرتبطة بالهندسة الاجتماعية وكلمات المرور الضعيفة

تعد الهندسة الاجتماعية الشكل الأكثر شيوعًا والتي تشير إلى التصيد الاحتيالي، ويحدث التصيد الاحتيالي عندما يتنكر المجرم في هيئة جهة موثوقة لخداع الضحية، وجعله يفتح رسالة بريد إلكتروني أو رسالة نصية أو رسالة فورية تحتوي على تطبيق ذي أهداف دنيئة، والأشخاص الذين يقعون ضحية لهجمات التصيد الاحتيالي من أهم أسباب سرقة الهوية[1].

ولم يشير المشرع الأردني في نصوصه الحالية إلى مصطلح الهندسة الاجتماعية.

[1] سيد، أشرف جابر والشافي، خالد (2013). حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع فيس بوك، بحث منشور بكلية الحقوق، جامعة حلوان: مصر، ص20.

كما لم يشر المشرع الأردني في نصوصه الحالية إلى محددات تكنولوجية واضحة تتناول موضوعات تخص البرامج، ومنها تقنية الكلمة المرورية، وإنما تناول بشكل عام تعريف البيانات الشخصية كما بين الباحث في مستهل دراسته الحالية.

ثانيًا: الوسائل الجرمية المرتكزة على الثغرات الآمنة في النظام والتهديدات الداخلية:

حيث تؤدي تطبيقات البرامج أو أنظمة الشبكات التي يتم تصميمها أو تنفيذها بشكل سيء إلى إيجاد ثغرات آمنة يمكن للجناة استغلالها واستخدامها في البيانات، ومن هذه الثغرات برامج مكافحة الفيروسات[1].

وكما بين الباحث سابقًا فإن النظام التكنولوجي المعتمد في سرقة البيانات لم يتم تناوله بشيء من التفصيل، وإنما خص الجريمة الإلكترونية بشكل عام.

وللإنصاف فإن القانون الجديد أضاف في المادة (16) ما مصطلحًا جديداً وهو اغتيال الشخصية؛ حيث نصت هذه المادة على أنه: (كل من أشاع أو عزا أو تسبب قصداً دون وجه حق إلى أحد الأشخاص أو ساهم في ذلك عن طريق الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو الموقع الإلكتروني أو منصات التواصل الاجتماعي أفعالاً من شأنها اغتيال شخصيته يعاقب بالحبس مدة لا تقل عن 3 أشهر أو بغرامة لا تقل عن 5000 دينار ولا تزيد على 20000 دينار أو بكلتا هاتين العقوبيتين)؛ أي أنه من وجهة نظر الباحث فإن موضوع اغتيال الشخصية هو تجريم للجاني في حق المجني عليه من حيث سرقة بياناته الخاصة التي تدخل ضمن حدود الحياة الخاصة له، والتي سيتطرق إليها الباحث في الأبواب القادمة من هذه الدراسة.

---

[1] لامي، بارق (2017). جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، مرجع سابق، ص20.

ومن المعروف أن الموظفين العاملين في الشركة يملكون حق الوصول إلى البيانات الشخصية الإلكترونية للعملاء، وبهذا يمكن للموظفين المحتالين أو المتعاقدين الساخطين نسخ هذه البيانات الشخصية أو تعديلها أو سرقتها[1]. ورغم هذا، لا تقتصر التهديدات الداخلية بالضرورة على الموظفين الحاليين؛ بل يمكن أن تشمل كذلك الموظفين والمتعاقدين السابقين أو شركاء سابقين يملكون حق الوصول إلى أنظمة الشركة التي يعملون بها، أو أي معلومات حساسة للعملاء[2].

ثالثًا: الوسائل الجرمية المستندة على الخطأ البشري والتنزيلات المخترقة والأفعال الحقيقية:

ليس من اللازم أن تكون انتهاكات البيانات بسبب هجوم خبيث، بل أحيانًا ما تحدث بسبب حدوث خطأ بشري، وتشمل الأخطاء الشائعة كإرسال رسالة بريد إلكتروني عن طريق الخطأ إلى عنوان بريدي غير صحيح أو إرفاق مستند خاطيء أو تسليم ملف ورقي إلى شخص لا ينبغي له أن يكون لديه حق الوصول إلى المعلومات الواردة فيه، ويمكن أيضًا أن يتضمن الخطأ البشري تكوينًا خاطئًا، مثل ترك الموظف لقاعدة بيانات تحتوي على معلومات حساسة عبر الإنترنت دون أي قيود على كلمة المرور[3].

---

(1) الغويري، ضيف الله (2014). ضمانات الحق في الحماية الخاصة في النظام السعودي، مجلة المدير الناجح، المجلد الثامن، العدد الثاني عشر، ص20.

(2) المؤيد، محمد (2009). صور المسؤولية التقصيرية الناشئة عن الاعتداء على بيانات الكمبيوتر والتعامل عبر الإنترنت وتسوية منازعاتها، مجلة الدراسات الاجتماعية، المجلد الثاني، العدد الثامن والعشرون، ص30.

(3) كامل، جبالي (2016). حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق، جامعة أسيوط في الفترة من (12-13) إبريل، ص21.

ويستطيع المجرمون أن يقوموا بتنزيل برامج أو بيانات من مواقع إلكترونية مخترقة مصابة بفيروسات مثل الفيروسات المتنقلة أو البرمجيات الضارة، ويعطي هذا للمجرمين إمكانية وصول غير مصرح به إلى أجهزتهم؛ مما يتيح لهم سرقة البيانات الشخصة الإلكترونية للعملاء[1].

وبعض سرقة البيانات لا تكون نتيجة جريمة إلكترونية، بل أفعال حقيقية تتسبب فيها، ومن أمثلة هذا سرقة ورق عمل أو أجهزة: (مثل الحواسيب المحمولة أو الهواتف أو أجهزة التخزين)، ومع زيادة ثقافة العمل من المنزل والعمل عن بعد، ازدادت فرص فقدان الأجهزة أو سرقتها، إذ كنت تعمل في مكان عام (مثل مقهى كبير)[2]. ويمكن لأي شخص أن ينظر إلى شاشة الضحية، ويراقب لوحة المفاتيح فيها من أجل سرقة بيانات تسجيل الدخول للحسابات، ومسح البطاقات، حيث يتم هذا عن طريق إدخال المجرمين لجهاز صغير في أجهزة قراءة بطاقات الائتمان، حيث تعتبر هذه طريقة أخرى من طرق سرقة البيانات الشهيرة[3].

وفي حال تعرض شركة تحتفظ بمعلومات عن الضحية لهجوم بسبب حدوث مشكلة في قاعدة البيانات أو الخادم، يمكن وقتها أو يصل المهاجمون إلى المعلومات الشخصية لعملاء تلك الشركة. والمعلومات المتاحة للجمهور[4].

---

(1) حموري، شهد والمصري، ريم (2014). قانون حماية البيانات الشخصية الأردني، ما يمكن تعلمه من تجارب الدول الأخرى، مقالة منشورة على مدونة حبر، متاحة عبر الرابط الإلكتروني: www:7iber.com/wp-content/uploads/2016/01/Reem.pdf.، تمت الزيارة بتاريخ: 15-9-2023، الساعة 8:35 صباحًا، مرجع سابق، ص20.

(2) ربايعة، عبد اللطيف (2016). الجرائم الإلكترونية (التجريم والملاحقة والإثبات)، رسالة ماجستير (غير منشورة)، جامعة اليرموك، إربد: الأردن، ص33.

(3) الجمعية الأردنية للمصدر المفتوح (2022). مشروع قانون حماية البيانات الشخصية لسنة (2022)، مرجع سابق، ص9.

(4) وزارة الاقتصاد الرقمي والريادة (2021). قانون حماية البيانات الشخصية لسنة (2021)، مرجع سابق، ص6.

ويوجد الكثير من المعلومات التي يمكن العثور عليها في النطاقات العامة؛ أي أنه يمكن الوصول إليها عن طريق البحث الإلكتروني، والبحث في منشورات إلكترونية للضحايا[1].

إن أي بيانات شخصية يخزنها فرد أو شركة أو مؤسسة يمكن أن تكون هدفًا محتملاً لسارقي البيانات، ومن هذه البيانات: سجلات العملاء، والبيانات المالية (معلومات بطاقة الائتمان أو بطاقة الخصم المباشر، والأكواد المصدرية والخوارزميات)، وأوصاف عمليات الملكية، ومنهجيات التشغيل، وبيانات الشبكة (أسماء المستخدمين وكلمات المرور، وسجلات الموارد البشرية وبيانات الموظفين، والمستندات الخاصة المخزنة على أجهزة الحاسوب في الشركة التي يعمل بها الضحايا)[2].

ويمكن أن تقع عواقب وخيمة نتيجة سرقة البيانات الشخصية (انتهاك البيانات الشخصية)، ومنها قضايا محتملة يرفعها العملاء الذين تعرضت بياناتهم للاختراق، ومطالب لفدية من مهاجمين، وتكاليف الإصلاح، مثل استعادة الأنظمة التي تمت اختراقها أو إصلاحها، وتضرر السمعة وفقدان العملاء، وغرامات أو عقوبات من الجهات المختصة، وتختلف باختلاف مجال العمل، ووقت تعطيل حتى يتم استعادة البيانات[3].

ويعاني الأشخاص الذين تم اختراق بياناتهم الشخصية، من أزمات مالية ونفسية بسبب سرقة هوياتهم[4].

---

(1) السكر، سلطان فياض (2022). جريمة انتهاك سرية المعلومات عبر الوسائل الالكترونية في التشريع الاردني، رسالة ماجستير (غير منشورة)، كلية الحقوق، جامعة الشرق الاوسط، عمان: الأردن، ص11.

(2) الشوابكة، محمد امين (2011). جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص5

(3) الخلايلة، عايد (2011. المسؤولية التقصيرية الالكترونية، دراسة مقارنة، (ط2)، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص6.

(4) ظاهر، سفيان (2023). الحماية الجزائية لصورة الانسان الشخصية عبر الوسائل الالكترونية، دراسة مقارنة، رسالة ماجستير (غير منشورة)، كلية الحقوق جامعة الزرقاء، الزرقاء: الأردن، ص20.

ويمكن حماية البيانات الشخصية الإلكترونية من المجرمين الإلكترونيين عن طريق الاعتماد على كلمات مرور قوية تتكون من (12) حرفًا على الأقل أو أكثر من ذلك، وتتألف من مزيج من الحروف الكبيرة، والصغيرة بالإضاقة إلى الرموز والأرقام، بحيث تشكل عبارة ذات مغزى يسهل تذكرها بعد جمع الفرد للحرف الأول من كل كلمة؛ حيث أن كلمات المرور ذات الأرقام المتسلسلة، أو المعلومات الشخصية التي قد يخمنها المجرمون، مثل تاريخ ميلاد الضحية تسهل عملية انتهاك البيانات الشخصية للأفراد[1].

يرى الباحث أن البيانات الشخصية المسروقة للضحايا يمكن أن تكون أي شيء من المعلومات عن الحساب المصرفي إلى كلمات المرور على الإنترنت، ورقم جواز السفر، ورقم رخصة القيادة، ورقم الضمان الاجتماعي والسجلات الطبية والاشتراكات الخاصة بهم.

ويرى الباحث أن قانون حماية البيانات الشخصية الأردني لسنة (2021) في الفرع (أ) من المادة (8) أعطى الصلاحية لصاحب البيانات الشخصية في الاحتفاظ بسرية هذه البيانات، وتجنبه بالتالي كافة الوسائل التي عرضها الباحث فيما سبق، حيث أن نص هذه المادة أعطى لصاحب البيانات حقوق منها: (يحظر القيام بمعالجة البيانات الشخصية دون موافقة صاحبها، وتنفيذ القيام بمعالجة البيانات الشخصية دون موافقة صاحبها، واتخاذ خطوات بناء على طلب الشخص المعني بالمعالجة، وتنفيذ التزام يرتبه القانون خلافًا لالتزام عقدي أو صدور أمر حماية المصالح الحيوية للشخص المعني بالمعالجة، ولا يجوز أن تتجاوز معالجة البيانات الشخصية الغرض الذي جعلت من أجله).

---

[1] المغربي، جعفر محمود وعساف، حسين شاكر (2010). المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول، دار الثقافة للنشر والتوزيع، عمان، الأردن، ص12 و الزعبي، علي احمد (2006). حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، طرابلس: بيروت، ص5.

يلاحظ الباحث أن موقف المشرع الأردني من الوسائل الجرمية لانتهاكات البيانات الشخصية في قانون الجرائم الإلكترونية رقم (17) لسنة (2023) مقارنة بما طرحه في القانون السابق ما يلي:

أ. **المؤسسات، فصل القانون الحالي العقوبة الجزائية انتهاكات البيانات الشخصية للوزارات والدوائر الحكومية والمؤسسات الرسمية العامة والمؤسسات العامة والأمنية والمالية والمصرفية والشركات،** وذلك في نص المادة (4/ج) منه: (يعاقب كل من دخل أو وصل قصداً إلى موقع إلكتروني يعود للوزارات أو الدوائر الحكومية أو المؤسسات الرسمية العامة أو المرسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار).

ب. **وسائل التواصل الاجتماعي، حدد** قانون الجرائم الإلكترونية رقم (17) لسنة (2023) الحالي في المادة (5/أ) منه العقوبة الجزائية فيما يخص وسائل التواصل الاجتماعي بقوله: (يعاقب كل من قام بإنشاء حساب أو صفحة أو مجموعة أو قناة أو ما يماثلها على منصات التواصل الاجتماعي ونسبها زوراً إلى شخص طبيعي أو معنوي بالحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن (1500) ألف وخمسمائة دينار ولا تزيد على (1500) خمسة عشر ألف دينار أو بكلتا هاتين العقوبيتين).

ج. **البطاقات المزورة،** بين قانون الجرائم الإلكترونية رقم (17) لسنة (2023) الحالي العقوبة الجزائية فيما يخص البطاقات المزورة في المادة (8/أ–3) بقوله: (قبل التعامل بالبطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني أو بيانات وسائل الدفع الإلكتروني المستولى عنها بطريقة غير مشروعة مع علمه بعدم مشروعيتها).

د. **الحق العام والحق الشخصي،** حيث بينت المادة (38) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023): (تقام دعوى الحق العام والحق الشخصي على المشتكى عليه أمام المرجع القضائي المختص إذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باستخدام الشبكة المعلوماتية أو تقنية معلومات أو نظام معلومات أو منصة تواصل اجتماعي أو موقع إلكتروني أو بأي وسيلة نشر إلكترونية داخل المملكة، أو ارتكبت خارج المملكة وألحقت أضراراً بأي من مصالحها أو مواطنيها أو المقيمين فيها أو ترتبت آثار الجريمة فيها كليًا أو جزئيًا).

هـ. **سرعة البت في العقوبة الجزائية،** حيث نصت المادة (34) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023): (تعطى القضايا المرتكبة خلافًا لأحكام هذا القانون صفة الاستعجال وتعقد جلساتها مرة واحدة على الأقل في الأسبوع وعلى أن يفصل فيها خلال مدة لا تزيد على ثلاثة أشهر من تاريخ ورودها لقلم المحكمة).

و. **صلاحيات جديدة للمدعي العام،** حيث أعطت المادة (33/أ) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023) للمدعي العام المختص وللمحكمة المختصة صلاحيات إصدر أمر إلى القائمين على نظام المعلومات الإلكتروني اتخاذ ما يلي:

(أ. إزالة أو حظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو أي منشور أو محتوى أو منع الوصول إليه أو حظر المستخدم أو الناشر مؤقتًا خلال المدة المحددة في القرار.

(ب. إزالة أو حظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو أي منشور أو محتوى أو منع الوصول إليه أو حظر المستخدم أو الناشر مؤقتًا خلال المدة المحددة في القرار.

(ج- الحفظ العاجل للبيانات والمعلومات اللازمة لإظهار الحقيقة وتخزينها والمحافظة على سلامتها).

سابعًا: الحفاظ على السرية، حيث نصت المادة (31/ أ) من قانون الجرائم الإلكترونية رقم (17) لسنة (2023) تقضي المحكمة في حال الإدانة بما يلي:

(أ. مصادرة الأجهزة أو البرامج أو الأدوات أو الوسائل أو المواد المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال منها.

(ب. وقف او تعطيل أو حجب عمل أي نظلم معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانونن كليًا أو جزئيًا للمدة التي تقررها المحكمة.

ج- حذف المعلومات أو البيانات على نفقة الفاعل.

د- المحل الذي استخدم لارتكاب أي من الجرائم المنصوص عليها في هذا القانون لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة).

ومن خلال ما سبق يلاحظ الباحث أن قانون الاتصالات الأردني حتى عام (2023) كان أقل مواكبة لخطورة التكنولوجيا مقارنة بقانون الجرائم الإلكترونية رقم (17) لسنة (2023) الحالي، حيث أنه لم يحدد طبيعة انتهاكات البيانات الشخصية، وإنما اكتفى ببيانها من خلال الارسال والاستقبال،

أي اكتفى بالتعريف، وذلك بقوله: (الاتصالات نقل أو بث أو استقبال أو إرسال الرموز أو الإشارات أو الأصوات أو الصور أو البيانات مهما كانت طبيعتها بواسطة الوسائل السلكية أو الراديوية أو الضوئية أو بأي وسيلة أخرى من الأنظمة الإلكترونية).

وعلى الرغم من أن أن المادة (6/د) من قانون الاتصالات الأردني حتى عام (2023) نصت على حماية حقوق المستخدمين بقولها: (حماية مصالح المستفيدين ومراقبة الأشخاص والجهات المرخص لها للتأكد من الالتزام بشروط الرخصة بما في ذلك مواصفات الخدمات المقدمة وجودتها وأسعارها واتخاذ الإجراءات القانونية اللازمة بحث من يخالف هذه الشروط)، وأن المادة (62) منه– أيضًا– فصلت دور المسؤول: (للرئيس أو من يفوضه خطيًا حق الدخول إلى أي مكان يشتبه بأنه يحتوي على أجهزة أو شبكات غير مرخصة أو أجهزة تستعمل للتشويش على شبكات الاتصالات أو تمارس فيها أي نشاطات مخالفة لهذا القانون أو الأنظمة الصادرة بموجبه ولهم تفتيش المكان لاستثناء بيوت السكن حيث يجب الحصول على إذن من المدعي العام المختص قبل الدخول وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه على الرئيس).

إلا أن هذا القانون لم يدخل اليانات بصيغة تواكب التطورات السريعة في انتهاكات البيانات الشخصية، حيث بينت المادة (57) من قانون الاتصالات الأردني حتى عام (2023): (للهيئة بالاتفاق مع المرخص له وضع القواعد والإجراءات التي يجب اتباعها عند تلقي المرخص له لشكاوى إزعاج وإجراءات التحقق من هذه الشكاوى والقواعد اللازمة لتقليل اتصالات الإزعاج بشكل عام).

أي أن الموضوع اقتصر فقط على الشكاوى والإزعاج بدون عقوبة جزائية محددة.

المطلب الثاني

موقف المشرع الأردني من جريمة انتهاك الحياة الخاصة

يعمل منتهكو الشخصية على نشر بعض المعلومات عن شخصيات اعتبارية ذات صبغة سياسية، أو مالية، الأمر الذي دفع الكثيرين على التساؤل هل هذا يندرج تحت حق التعبير عن الرأي أو حق الحصول على المعلومة، أم أن هذا الأمر يعتبر تعدي على خصوصية الآخرين؟

حيث يأبى الإنسان بطبيعته الاجتماعية أن يتدخل أحد في شأن من شؤونه الخاصة، وهذا ما يعبر عنه بالحياة الخاصة للإنسان والتي تشمل أيضًا الحق في السرية المهنية، وسرية المراسلات والمحادثات، وحرمة المساكن، وحرية الاعتقاد والفكر، والمسألة العاطفية والعائلية والروحية والمالية، حيث تعد هذه المظاهر الاجتماعية الضرورية لحياة البشر، وجزء لا يتجزأ من وجودهم، مما يتطلب حمايتها أيًا كان الشخص المعتدي وبغض النظر عن المعتدى عليه أو الوسيلة المستعملة في الاعتداء[1].

ومع التطورات التكنولوجية، أصبح الإنسان عاريًا ومكشوفًا، وبات بالإمكان وفي أي وقت اختراق حياته الخاصة، ويترتب بالتالي على المشرع الأردني وضع قيد شديد على حرية الإعلام في نشر ما يعد حياة خاصة للأفراد[2].

---

(1) العجارمة، نوفان (2021). الدستور الأردني يجرم الاعتداء عل حرمة الحياة الخاصة، مقالة منشورة على موقع : www.ammonnewa.net، تم الدخول إليه 7-10- 2023- الساعة 11:12 ظهراً.

(2) Cortellazzo, L., Bruni, E., and Zampieri, R., (2019). The Role of Leadership in a Digitalized World: Ar reciew, Front Psychol. 10(1), 12-44

والحياة الخاصة فكرة مرنة ومتغيرة نسبية وتختلف باختلاف الزمان والمكان والأشخاص، فما يعد من الحياة الخاصة للفرد في الأردن قد لا يكون ذلك في الدولة الأوروبية مثلاَ، وما يعد من الحياة الخاصة في زمن مضى قد لا يكون كذلك الآن أو في المستقبل، كما أن الحياة الخاصة للمشاهير تختلف عنها بالنسبة للأشخاص العاديين، وتختلف أيضًا باختلاف القيم والعادات والتقاليد السائدة في كل المجتمع [1].

ولقد وردت حماية الحياة الخاصة في صلب مواد الدستور الأردني، وهذا يعد ضمانة دستورية مهمة للمواطنين، ويعطي قدسية للحياة الخاصة وسياج لها من أن ينال منها أو يمسها تشريع أو قانون، وذلك عملاً بمبدأ سمو الدساتير وما يترتب عليه من عدم جواز تقييد هذه الحياة الخاصة أو المساس بها بأية وسيلة وإلا كانت غير دستورية، خاصة أن الإنسان يولد ويكتسب بعض الحقوق خلال فترة حياته وبعض الحقوق يولد بها [2].

ذلك أن الحق في الحياة الخاصة يعتبر حق نسبي يتغير نطاقه بتغير الزمان والمكان، وإن ماهية الحق في الخصوصية أو الحياة الخاصة ينطوي على إشكالات صعبة التحديد؛ لأن هذا الحق في ذاته أمر من الصعب ضبطه بدقة؛ لارتكانه لفكرة نسبية تتغير بتغير الزمان والمكان وعادات الناس وتقاليدهم وأخلاقياتهم؛ وتطور الحياة وعوامل البيئة الثقافية والاجتماعية والاقتصادية[3].

---

(1) الشوابكة، محمد (2011). جرائم الحاسوب والغ نترنت–الجريمة المعلوماتنية، (ط4)، دار وائل للنشر والتوزيع، الأردن.، ص6.دي، محمد (2015). الجرائم المستحدثة في ظل العولمة، (ط1)، دار جليس الزمان، عمان: الأردن، ص20.

(2) الزرفي، علي (2020). الجريمة المعلوماتية الماسة بالحياة الخاص– دراسة مقارنة–، (ط1)، مصر: المكتب الإقليمي، ص20.

(3) الشوابكة، محمد (2011). جرائم الحاسوب والغ نترنت–الجريمة المعلوماتنية، (ط4)، مرجع سابق، ص6. دي، محمد (2015). الجرائم المستحدثة في ظل العولمة، مرجع سابق، ص20.

الفرع الأول

الاعتداء على الحريات والحقوق

رسخ الدستور الأردني حق الحياة الخاصة وحرمة التعدي عليها في المادة (7) من منه والتي تناولت:

أ. الحرية الشخصية مصونة.

ب. كل اعتداء على الحقوق والحريات العامة أو حرمة الحياة الخاصة للأردنيين جريمة يعاقب عليها القانون.

ومن حيث المكان يلاحظ الباحث أن أصل تحديد نطاق الحياة الخاصة كان يعتمد في الأساس على النطاق المكاني، ففي ذلك نفرق بين الأماكن العامة والأماكن الخاصة، حيث أن الأماكن الخاصة هي محمية بالكلية لطبيعة تلك الأماكن فالإنسان في تلك الأماكن لا يكون حذراً تجاه الغير فيتعامل بسجيته بقدر لا يحب أن يطلع الغير عليه، أما الأماكن العامة فالأصل فيها أنها لا تشملها الحماية إلا أن ذلك مقرون بقدر معين حيث أنه لابد أن لا تبيح تلك الإباحة التصنت أو التقاط الصور والتعدي على خصوصيات الآخرين[1].

---

[1] محمد، نصر (2016). المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، (ط1)، مركز الدراسات العربية، مصر، ص11. الشوابكة، محمد (2011). جرائم الحاسوب والإنترنت-الجريمة المعلوماتية، (ط4)، دار وائل للنشر والتوزيع، الأردن، ص22.

وقد يختلف نطاق الحياة الخاصة من حيث الأشخاص باختلافهم أنفسهم، فمع تطور المجتمعات ظهرت ما تسمى بالشخصيات العامة، وترتب على ذلك أن تقلص الحق في الحياة الخاصة لتلك الشخصيات، ويظهر ذلك فيما نراه من تناول بعض جوانب حياتهم وإتاحة تصويرهم في الأماكن العامة، ويؤخذ ذلك في الاعتبار إذا ما صار نزاع حول التعدي على حرمة الحياة الخاصة بهم[1]. وبالنسبة للنطاق الإلكتروني، فنظراً للتطور الحديث ظهرت الحياة الموزاية والذي يقصده الباحث بهذا المصطلح تلك الحياة الإلكترونية التي أصبحت جزء لا يتجزأ من حياتنا، والتي يوجد فيها ما يشمله الحق في الحياة الخاصة، حيث يوجد قدر فيها لا يحب ان يشاركه الأشخاص على الملأ، وعلى سبيل المثال تعد المحادثات الخاصة بين الأفراد سواء كانت نصية أو عن طريق القيديو جزء من الحياة الخاصة، وعلى النقيض لا تعد الكتابات التي يشاركها الأشخاص على العامة جزء من تلك الحياة الخاصة[2].

وبالنسبة للخصوصية بمعنى خصوصية المعلومات(حق الأفراتد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم، متى وكيف أو إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين). فقد عرفت بأنها حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه، وعملية معالجتها آليًا، وحفظها، واستخدامها في صنع القرار الخاص به أو المؤثر فيه[3].

---

(1) فاضل، باسم (2021). حماية الخصوصية عبر البيئة الرقمية، (ط1)، دار الفكر الجامعي، الإسكندرية، ص6.

(2) الفاعوري، فتحي (2021). شرح قانون الجرائم الإلكترونية، (ط1)، دار وائل للنشر، عمان: الأردن، ص9.

(3) محمد، نصر (2016). المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، (ط1)، مركز الدراسات العربية، مصر، ص20.

في حين يلاحظ الباحث أن النطاق بالإذن يكون المتحكم فيه وهو صاحب الحق ذاته فقد يسمح الشخص بالتعرض لجزء من حياته الخاصة، وفي هذه الحالة لابد من أن يتقيد الممنوح له الإذن بما أذن له به صاحب وإلا كان متعديًا على الحق في الحياة الخاصة.

ويؤكد ذلك أن تنازل المجني عليه وتصالحه في الدعوى الخاصة بالتعدي على الحياة الخاصة يسقط دعوى الحق العام، وفي ذلك نصت المادة (52/1) من قانون العقوبات الأردني على: (صفح المجني عليه يسقط دعوى الحق العام والعقوبات المحكوم بها التي لم تكتسب الدرجة القطيعة في أي من الحالات التالية: 1- إذا كانت إقامة الدعوى تتوقف على اتخاذ صفة الادعاء بالحق الشخصي أو تقديم شكوى 2- صفة التعدي على الحياة الخاصة وسند التجريم).

والتعدي على حرمة المسكن (كل مكان معد للسكن والإ يواء وفقًا لما هو متعارف عليه في مكان معين في زمن معين) وغاية تجريم المشرع التعدي على المسكن لأن الإنسان قد لا يكترث لما يلبس أو كيف يتصرف في تلك الأماكن فلا يحب أن يراه أو كيف يتصرف في تلك الأماكن فلا يحب أن يراه الغير خاصة إذا تحدثنا عن حرمة المرأة.

وفي ذلك نصت المادة (347/2) من قانون العقوبات الأردني على: (خرق حرمة المنزل والاماكن والحياة الخاصة:

1- من دخل مسكن آخر أو ملحقات مسكنه خلافًا لإرادة ذلك من له الحق في اقصائه عنها عوقب بالحبس مدة لا تتجاوز الستة أشهر.

2- ويقضي بالحبس من ثلاثة أشهر إلى سنة إذا وقع الفعل ليلاً وبالحبس من ستة أشهر إلى سنتين إذا وقع الفعل بواسطة العنف على الأشخاص أو الكسر او باستعمال السلاح لعدة أشخاص مجتمعين.

3- لا تجري الملاحقة في الحالة المنصوص عليها في الفقرة الأولى، إلا بناء على شكوى الفريق الآخر.

فتصدي الادعاء العام حال دخول المسكن يكون موقوفًا على شكوى صاحب الحق، ويرجع ذلك لما بيناه من أن نطاق الحياة الخاصة للفرد قد يتحدد بناء على إذن منه فلا يتصور أن يأذن الشخص بدخول آخر لمنزله ويتم مقاضاة الأخير. ومن ذلك -أيضًا-التعدي باستراق السمع أو البصر في تلك الحالة يكون التعدي على الحياة الخاصة عن طريق محاولة معرفة ما لا يحب صاحب الحق إذعته عن طريق السمع أو البصر سواء كانت مباشرة أم بواسطة الأجهزة الحديثة، والغاية من هذا التجريم لا يختلف عن الغاية في تجريم دخول المسكن حيث أن تتبع الشخص فس ما يقول أو يفعل قد يضر به. ويندرج تحت هذا العنصر التعدي على المراسلات والاتصالات الخاصة التي يجريها الأشخاص فيما بين بعضهم البعض طالما أن طرفا الحديث قد حجباها عن الآخرين[1]، فقد نصت المادة (8) من الاتفاقية الأوروبية لحقوق الإنسان على: (1-لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته. 2. لا يجوز للسلطة العامة أن تتعرض لممارسة، وهذا الحق إلا وفقًا للقانون وبكل تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم).

ولم يجرم المشرع الجزائي الأردني التصوير خفية في مكان خاص إذا تم بإذن المدعي العام، ولكن عدم التجريم لا يعني أن هذا التصوير يعد مشروعًا لأن فيه اعتداء على حرية الإنسان.

---

[1] العبادي، محمد (2015). الجرائم المستحدثة في ظل العولمة، (ط1)، دار جليس الزمان، عمان: الأردن، ص9.

وفي ذلك نصت المادة (348) من قانون العقوبات على أنه: (يعاقب بناء على شكوى المتضرر بالحبس مدة لا تقل عن ستة أشهر وبالغرامة مائتي دينار كل من خرق الحياة الخاصة للآخرين باستراق السمع أو البصر بأي وسيلة كانت بما في ذلك التسجيل الصوتي أو التقاط الصور أو استخدام المنظار، وتضاعف العقوبة في حال التكرار).

ولم يقف المشرع الأردني عند حد وقوع جريمة التعدي فعلاً فيما يخص جرائم التعدي على الحياة الخاصة بل جرم فعل التهديد بالتعدي عليها أو التعرض لحياته الخاصة.

وفي ذلك نصت المادة (415/1/أ) من القانون السابق: (مع عدم الإخلال بأي عقوبة أشد ورد النص عليها في أي تشريع آخر:- يعاقب بالحبس مدة لا تقل عن سنتين كل من قام بنفسه أو بواسطة غيره باستعراض القوة أمام شخص أو التلويح له بالعنف أو بتهديده باستخدام القوة أو العنف معه أو مع زوجة أو أصوله أو فروعه أو أقاربه حتى الدرجة الثالثة أو التهديد بالافتراء عليه أو على أي حد منهم بما يشينه أو بالتعرض لحرمة حياته أو حياة أي منهم الخاصة...)

وفيما يخص التعدي بالنشر حرص المشرع الأردني على أن يكون هذا الحق مقيداً بقدر من المحافظة على حق الآخرين في الحياة الخاصة، ولقد رسخ المشرع الأردني ذلك.

وفي ذلك نصت المادة (4) من قانون المطبوعات والنشر وتعديلاته على: (تمارس الصحافة مهمتها بحرية في تقديم الأخبار والمعلومات والتعليقات وتسهم في نشر الفكر والثقافة والعلوم في حدود القانون وفي إطار الحفاظ على الحريات والحقوق والواجبات العامة واحترام حرية الحياة الخاصة للآخرين وحرمتها).

يرى الباحث أن التعدي الإلكتروني تناوله المشرع الأردني منعًا من إفلات المجرمين من العقاب، حيث ساوى المشرع الأردني بين ارتكاب الجرائم بالوسائل العادية وارتكابها بالوسائل الإلكترونية.

وفي نطاق تناول الباحث حمابة الحق في الحياة الخاصة وبموجب نصوص القانون فإن التعدي على الحياة الخاصة بالوسائل الإلكترونية يأخذ ذات حكم التعدي العادي، وفي ذلك نصت المادة (15) من قانون الجرائم الإلكترونية الحالي (2023) على: (كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشتراك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع).

ومن نصوص التجريم للتعدي على الحياة الخاصة التي وردت في قانون الجرائم الإلكترونية: إدخال أو نشر برنامج إلغاء أو حذف، حيث نصت المادة (4) منه على: (يعاقب كل من أدخل أو نشر أو استخدم قصداً برنامجًا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو اتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار).

حيث أن الالتقاط أو التصنت أو شطب البيانات موضوع يرتبط بحرمة الحياة الخاصة، وهذا ما أكدت عليه المادة (5) من ذات القانون من حيث إيقاع العقوبة بالجاني: (يعاقب كل من قام قصداً

بالتقاط أو باعتراض أو بالتنصت أو أعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار).

وبالتالي يمكن القول أن أركان جريمة التعدي على الحياة الخاصة لا يمكن فصلها عن أي جريمة، والتي تتطلب يشترط لقيامها ما يشترط لقيام كافة الجرائم بركنيها المادي والمعنوي، حيث أن[1]:

أولاً: الركن المادي، ويتكون من:

1- **النشاط الجرمي،** هو عبارة عن السلوك الذي يتخذه الفرد ويشكل تعديًا على حق الآخرين في الحياة الخاصة، ومن الأمثلة النظر عبر المنظار أو التسجيل الصوتي.
2- **النتيجة الجرمية:** تتمثل النتيجة الجرمية في جريمة التعدي على الحياة الخاصة في وجود خرق لحياة المجني عليه الخاصة بأي شكل من الأشكال.
3- **العلاقة السببية:** لكي يتم تأثيم المجرم على فعل التعدي على حق الحياة الخاصة فلابد أن يكون التعدي الواقع على المجني عليه في حياته الخاصة قد وقع بمناسبة فعل المتهم.
4- **الركن المعنوي (القصد الجرمي):** لكي تتم معاقبة المجرم على فعل التعدي على الحياة الخاصة فلابد أن يكون قد ارتكب الفعل بالتدريج وإرادة لإتيان هذا الفعل.

---

[1] الزيود، فادي (2022). جريمة الاعتداء على الحياة الخاصة بالوسائل الإلكترونية في التشريع الأردني ومدى مواءمتها مع الاتفاقيات الدولية، رسالة ماجستير، جامعة عمان العربية، عمان: الأردن، ص22.

وفي ذلك نصت المادة (4) من قانون المطبوعات والنشر وتعديلاته على أن هناك استثناءات واردة على الحق في الحياة الخاصة[1]

أولًا: تعقب مرتكبي الجرائم: وسائل الاتثال تعد شكل من الأشكال الحياة الخاصة التي كفلها التشريع الأردني بالحماية، لكن الاستثناء قد يرد على هذا الحق متى كان في ذلك خدمة للكشف عن جريمة معينة، وفي ذلك نصت المادة (88) من قانون أصول المحاكمات الجزائية وتعديلاته نصت على: (للمدعي العام أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق كافة الرسائل البرقية كما يجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة.

ثانيًا: حماية الأمن الوطني: (حماية الأمن الوطني غاية مقدمة على أي حق، وفي سبيل ذلك فقد تم الاعتراف دوليًا بإباحة التعدي على الحياة الخاصة للأشخاص متى كان ذلك ضروريًا للحفاظ على الأمن الوطني، وفي ذلك نصت المادة (8) من الاتفاقية الأوروبية لحقوق الإنسان نصت على: (1- لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته. 2. لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقًا للقانون، وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوف الآخرين وحرياتهم).

---

[3]الزيود، فادي (2022). جريمة الاعتداء على الحياة الخاصة بالوسائل الإلكترونية في التشريع الأردني ومدى مواءمتها مع الاتفاقيات الدولية، مرجع سابق، ص44. الشوابكة، محمد (2011). جرائم الحاسوب والغ نترنت- الجريمة المعلوماتية، (ط4)، مرجع سابق، ص6.

وورد في الحكم رقم (2702) لسنة (2021) في محكمة التمييز الأردنية بصفتها الجزائية– الصادر بتاريخ 2021–10–28، وبتطبيق القانون على وقائع الدعوى وجدت المحكمة: (إن قيام المشتكى عليه بتركيب كاميرا فيديو وتصوير زوجته وبناتها من زوج آخر دون علمهم أو إذنهم يشكل كافة أركان وعناصر جرم خرق الحياة الخاصة مما ستوجب مساءلته عنه كون أن الحياة الخاصة حق دستوري مصان لكل إنسان ولو وجدت علاقة زوجية أو حرمة شرعية فإن ذلك لا ينفي بقاء الحرية الشخصية والحياة الخاصة للفرد وعدم جواز المساس بها).

وفي ضوء ما تقدم قررت المحكمة: (عملاً بأحكام المادة (1777) من قانون أصول المحاكمات الجزائية إدانة المشتكى عليه عن جرم استراق النظر خلافًا للمادة (348) مكررة من قانون العقوبات والحكم عليه بالحبس لمدة ستة أشهر والفرامة مشتي دينار والرسوم).

ولم يرتض المشتكي عليه (المحكوم عليه) بقرار محكمة صلح جزاء السلط فطعن فيه استئنافًا لدى محكمة بداية جزاء السلط بصفتها الاستئنافية.

ونظرت محكمة الاستئناف في الدعوى رقم (241/2021)، وأصدرت قراراها بتاريخ (17/2/2021)، حيث قضت برد الاستئناف موضوعًا وتأييد القرار المستأنف وإعادة الأوراق إلى مصدرها.

الفرع الثاني

انتهاكات البيانات الشخصية كفعل ضار في قانون العقوبات الأردني

يعد الفعل الضار مصدراً من مصادر الالتزام، حيث حصر القانون الإلتزامات التي تفرض على الأشخاص في العقد، وفي الفعل النافع، وفي الفعل الضار، وفي العرف، من المعروف أن التشريعات لم تضع تعريفًا محدداً للفعل الضار، وتركت هذه المسألة للفقه، مما أدى إلى كثرة تعريفات الفعل الضار وتنوعها تبعًا لآراء الفقهاء ونزعاتهم الشخصية، وتبعًا للظروف المحيطة بالمجتمع، وبمسؤولية الشخص عن فعله الشخصي متى وقع منه إخلال بإلتزام قانوني سابق هو عدم الإضرار بالغير، والذي يحتم عليه أن لا يقدم على إرتكابه[1]. ومن الجدير بالذكر أن قانون العقوبات الأردني لم يتناول أحكامًا تفصيلية للمسؤولية الجنائية عن الفعل الضار، في حال ارتكاب جريمة انتهاك البيانات الشخصية، في حين أن القانون المدني الأردني في المواد (256-287) منه بين هذه المسؤولية من جوانبها المختلفة، وذلك وفق ما نصت عليه هذه المادة: (كل إضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر).

وبالنظر إلى الضرر الذي تحدثه جريمة انتهاك البيانات الشخصية إلا أن قانون العقوبات ركز على الغرامة المادية والحبس، ولم يخضع الضرر المعنوي للمعايير الشخصية بشكل أكثر من المعايير الموضوعية، ولذلك فهو يعد من الأضرار الصعبة التقدير، ومن البينات المهمة في إثبات الحقوق الجزائية تقرير الخبرة الذي يصدره القاضي الجزائي، من خلال البينات العملية التي تعتمد على الإطلاع المباشر على محل الدعوى للتعيين، وتحديد نوع وقيمة الضرر محل رفع الدعوى، وقد نظم المشرع الأردني إجراءات تقرير الخبرة في قانون أصول المحاكمات الجزائية.

---

[1] أمجد، منصور (2011). النظرية العامة للالتزامات، مصادر الالتزام، ط6، عمان: دار الثقافة للنشر والتوزيع، ص262.

وبالتالي هناك ضرورة لتحديد نوع العقوبة بناء على طبيعة الضرر الذي أحدثته هذه الجريمة الإلكترونية (جريمة انتهاك البيانات الشخصية) الجديدة على المجتمع الأردني، وخاصة عند دخولها في تقدير القاضي الجزائي من حيث[1]:

أولاً: حالة المضرور (ضحية جريمة انتهاك البيانات الشخصية)

حيث تعكس حالة المضرور عنصراً رئيسًا من العناصر المؤثرة في كتابة تقرير الخبرة الذي يصدره القاضي الجزائي في حالة تشابة الفعل الضار، ويقصد بحالة المضرور: "حالة المضرور الجسمية والصحية؛ فمن كان حاداً "عصبيًا" فإن الإنزعاج الذي يصيه من حادث معين يكون ضرره أشد بكثير مما يلحق شخصًا آخر يكون سليم الأعصاب، ويقصد بحالة المضرور: "ما تعرض له المضرور من ضرر في سمعته أو شرفه أو اعتباره"، وإن الأصل في القانون أن حالة المضرور(الحالة الناجمة عن الفعل الضار نفسه) تساعد في تحديد تقدير الضرر، وفي التعويض عنه[2]. وإن الأصل في التعويض أن يكون من جنس الفعل الضار، كالضرر تمامًا كما هو الأمر بالنسبة إلى انتهاك بيانات الضحية في النشر في وسائل الإعلام، فالجزاء في مثل هذه الحالات يكون من جنس الفعل الضار [3].

---

(1) حنون، محمد (2000). الإعتبارات المؤثرة في تقدير التعويض عن الفعل الضار، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2000، ص151، وما بعدها، وكذلك الدكتور عبدالله مبروك النجار: التعسف في استعمال حق النشر، دراسة فقهية مقارنة، دار النهضة العربية، القاهرة، 1995، ص507، وما بعدها، وكذلك الساعدي، جليل (2000) الظروف الملابسة للضرر، مجلة العلوم القانونية، العدد الأول، المجلد الحادي عشر.، ص215، وما بعدها.

(2) العبادي، محمد (2015). الجرائم المستحدثة في ظل العولمة، (ط1)، دار جليس الزمان، عمان: الأردن، ص18.

(3) الشوابكة، محمد (2011). جرائم الحاسوب الإنترنت–الجريمة المعلوماتية، مرجع سابق، ص6. الشامي، سلامة (2018). جرائم الاعتداء على الحق في الخصوصية في ضوء التطور التكنولوجي، جامعة الأقصى، غزة، ص40.

ثانيًا: تطبيق القاضي الجزائي للقانون

للتوصل إلى الإلتقاء على الكثير من عناصر تقدير التعويض عن الفعل الضار (جريمة انتهاك البيانات الشخصية)؛ يقوم القضاة بتطبيق القانون، وبتحري إرادة المشرع للتوصل إلى التعويض العادل عن الفعل الضار؛ ولأن القضاء والفقه في سبيل تحديد عناصر تقدير تعويض الضرر الذي يلحق بمن وقعت عليهم جريمة انتهاك بياناتهم الشخصية، لا بد وأن يعملان بنصوص القانون من أجل عدم مخالفة نص، ولغرض تطبيق القانون، ولذلك فإنهما عند إحصائهما لهذه الظروف كانا يحددان دقة تقرير الخبرة للتعويض عن الضرر للفعل الضار[1]. وعلى الرغم من أن اجتهاد القاضي الجزائي في تقدير الضرر إلا أنه لم يرد نص واضح وصريح في قانون العقوبات الأردني بالنسبة لتقدير هذا التعويض وفقًا لنوع وصور جريمة انتهاك البيانات الشخصية.

ثالثًا: الظروف التي تلابس المضرور (ضحايا جريمة انتهاك البيانات الشخصية)

تُعد الظروف الملابسة عند كتابة تقرير الخبرة في تقدير الضرر من جراء انتهاك البيانات الشخصية للضحايا من الأمور التي تناولتها المادة (80) من قانون العقوبات الأردني: (الظروف التي تصاحب أو تلابس المضرور)، وليس المسؤول، فالظروف الشخصية التي تحيط بالمضرور، وما قد أفاده بسبب التعويض، كل ذلك يدخل في حساب القاضي الجزائي عند تقدير التعويض، وذلك لأن التعويض يقاس بمقدار الضرر الذي لحق بالمضرور بالذات، ومن ثم فهو يقدر على أساس ذاتي لا على أساس موضوعي.

---

(1) الشوابكة، محمد (2011). جرائم الحاسوب والإنترنت–الجريمة المعلوماتية،ى مرجع سابق، ص6.. العبادي، محمد (2015). الجرائم المستحدثة في ظل العولمة، (ط1)، دار جليس الزمان، عمان: الأردن، ص30.

ولم ينص قانون العقوبات الأردني على تقدير محدد في تقرير الخبرة بناء على الظروف الملابسة، على الرغم من ضرورة تحديد الخبير عند كتابة تقرير الخبرة الظروف الملابسة التي تكشف عن مدى الضرر، ومن ثم التعويض عنه بالطريقة المناسبة، والتي قد يكون لها أثراً كبيراً على تقدير التعويض عن الضرر؛ ومن ذلك ما يطرحه الباحث في انتهاكات البيانات الشخصية لفرد عادي، أو لشخص أو دائرة ذات شخصية اعتبارية في الأردن، حيث يفوق ضرر انتهاكات البيانات الشخصية في –جسامته– ما يلحق بفرد بسيط.

ويرجع اختلاف تقدير القاضي الجزائي في هذه الحالة إلى أن المؤسسات والمواطنين من ذوي الشخصية الاعتبارية يترتب عليهم خسارة مالية كبيرة –في حال اختراق بياناتهم الشخصية–مقارنة بعامل مصنع–هلى سبيل المثال–.

وبالنسبة لنظام الخبرة أمام المحاكم النظامية لسنة (2018) تبين أنه نظم شؤون الخبرة أمام المحاكم النظامية؛ حيث تناول في مطلعه سجل الخبرة من خلال تناوله لسجل شؤون الخبرة وما يدون فيه، كما وضح تشكيل مجلس شؤون الخبرة واجتماعاته وقراراته وصلاحيات المجلس، ومن ثم تناول شروط إعتماد الخبراء والجهة المختصة بنظر الشكاوي على الخبراء.

وبين الباحث أن هذ النظام تناول كذلك الرسوم المعتمدة لتسجيل الخبراء، كما أشار في نهايته إلى منح مجلس شؤون الخبرة إصدار التعليمات اللازمة لتنفيذ أحكام نظام شؤون الخبرة.

وبالتالي يراعي القاضي الجزائي الحالة المالية، والظروف العائلية للمضرور، إذ يكون لها دور كبير في تقديره التعويض عن الضرر الذي أصابه نتيجة اختراق بياناته الشخصية، ومما لا شك فيه أن الظروف الملابسة التي تكلم عنها الفقه كعناصر مؤثرة عند كتابة تقرير الخبرة لتقدير التعويض عن جريمة انتهاك البيانات الشخصية –والتي عرض الباحث لها سابقًا– تشمل الضرر

المعنوي والمادي معًا. لذا فإن الباحث عوّل على النصوص التي تم الإشارة إليها سابقًا عند الحديث عن صور هذه الجريمة الإلكترونية؛ أي أن قانون العقوبات الأردني لم يتناول تقدير القاضي الجزائي للتعويض المعنوي بنصوص محددة، أنما تناول التعويض المادي بالنصوص سابقة الذكر، حاله كحال قانون الجرائم الإلكترونية الحالي والتي لا يرى الباحث ضرورة لتكرارها في هذا الفرع.

ولما كانت حياة الفرد بصورتها المستحدثة المرتبطة بتكنولوجيا المعلومات مهددة بالعديد من الانتهاكات والاعتداءات التي تحدث فعلاً ضاراً، سيما في ظل التطور التكنولوجي المتسارع وظهور وسائل الاتصال المتطورة، الأمر الذي أوجد الحاجة إلى لسد الفراغ تشريعي في النصوص التقليدية لحماية ما يتم تداوله من معلومات وأسرار من خلال شبكة الإنترنت، ولحماية سرية الاتصالات والمراسلات، لذلك يعتبر الحق في الحياة الخاصة أو حق الخصوصية من أهم وأبرز حقوق الإنسان التي كفلتها الدساتير على مختلف أنماطها والتي تصنف كفعل ضار في حال حدوث انتهاكات في البيانات[1].

لذا يعتبر الحق في الحياة الخاصة أحد أهم الحقوق اللصيقة التي تثبت للإنسان منذ ولادته وغالبًا ما يصب حصر جوانبها والتمييز بحدود واضحة بين ما يعد من الحياة الخاصة للفرد وما يعد من الحياة العامة.

---

[1] الشوابكة، محمد (2011). جرائم الحاسوب والإنترنت–الجريمة المعلوماتية، مرجع سابق، ص6. العبادي، محمد (2015). الجرائم المستحدثة في ظل العولمة، مرجع سابق، ص30.

وجاء قانون الاتصالات رقم (13) لسنة (1995) لتنظيم وحماية الاتصالات كافة بما فيها خدمات تكنولوجيا المعلومات ولتسهيل إيصال الخدمة واستخدامها وفقًا للقوانين الناظمة والشروط والضوابط المحددة من قبل هيئة تنظيم قطاع الاتصالات.

أما ما يتعلق بالحق في الحياة الخاصة، فقد ورد النص عليه في المادة (76) من قانون الاتصالات الأردني والتي نصت على: (كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على 200 دينار بأو بكلتا العقوبيتين).

وبالتدقيق في النص المشار إليه يتضح بأنه خاص بالرسائل المتبادلة عبر شبكات الاتصالات، سواء شبكة عامة أو خاصة، وبالرجوع لتعريف شبكات الاتصالات العامة وفقًا لأحكام المادة (2) من ذات القانون نجد انها منظومة اتصالات أو مجموعة منظومات لتقديم خدمة الاتصالات العامة للمستفيدين وفقًا لأحكام القانون، أما شبكات الاتصالات الخاصة فهي تلك المنظومة من الاتصالات تصل لمصلحة شخص واحد أو مجموعة من الأشخاص تجمعهم ملكية مشتركة لخدمة حاجاتهم الخاصة، وتقوم الجريمة وفق هذا النص على ركننين أساسيين: الركن المادي الذي يقوم عند اتخاذ الفاعل أي سلوك من اعتراض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات، كما أن النص طال كل من شجع الغير على القيام بمثل هذه السلوكيات، والركن المادي للجريمة يرتكز على عدة عناصر، بحيث إذا توافرت هذه العناصر تقوم الجريمة وهي: السلوك الجرمي (النشاط المادي الذي يصدر عن المجني ومن شأنه إحداث النتيجة على النحو الذي حدده القانون)، والنتيجة الجرمية المتحققة (الأثر المترتب على السلوك الإجرامي

والذي يأخذه المشرع في الاعتبار بالتكوين القانوني للجريمة وهي العدوان الذي ينال من المصلحة المحمية قانونيًا)، والعلاقة السببية (الربط بين النشاط الإجرامي والنتيجة)، والتي بينها الباحث سابقًا.

وفي هذه الجريمة يقوم الركن المادي بالقيام بأي فعل كاعتراض الرسائل أو تحويرها أو إعاقتها أو شطب محتوياتها شريطة أن تكون تلك الرسائل مرسلة من خلال شبكة الاتصالات.

وبالنسبة للركن المعنوي للجريمة، فهو يتمثل في:

أولاً: القصد العام القائم على العلم والإ رادة، بحيث يكون الفاعل عالمًا بسلوكه بأن الرسالة هي عبر شبكات الاتصالات واتجاه إرادته لتحقيق النتيجة المبتغاة من سلوكه.

وفي ذلك قررت محكمة صلح جزاء عمان (إن قيام هذا الجرم هو الاعتداء على الحياة الخاصة والتي تقوم على ممارسة الشخص لأموره الشخصية التي لا يرغب باطلاع الغير عليها حفاظًا على خصوصيته، وأنه ومن صريح نصوص المادتين (71)، و(76) من قانوم الاتصالات فقد تطلبتا أن يكون التسجيل من شخص اطلع على المكالمة بحكم وظيفته، فالنص جاء لحماية مخابرات الأفراد الهاتفية من اعتراضها أو الاطلاع عليها من قبل الأشخاص ذوي الصلاحية، وبالنسبة لعبارة أو تسجيلها ولو وردت بعد عبارة "بحكم وظيغته" إلا أنها معطوفة عليها أعمالاً للأثر اللغوي لحرف العطف "أو" وهو ما يتفق والغاية التشريعية من النص والذي لا ينطوي على تسجيل المكالمات من قبل أطراف المكالمة، إنما من شخص ثالث يعترضها بحكم وظيفته)[1].

---

[1] (قرار محكمة صلح جزاء عمان رقم 5414/ 2020 تاريخ 7/16/ 2020).

النتائج:

توصل الباحث إلى النتائج التالية:

1. لم ينص قانون حماية البيانات الشخصية الأردني لسنة (2022) على تفصيل معالجة البيانات الشخصية الإلكترونية إلا من تعريف فقط للمنظمين لهذه المعالجة من مسؤولين، ومتلقين، من خلال نص المادة (2) منه.
2. لم يحدد المشرع الأردني نطاق الحماية الجزائية–كل على حدة– فيما يخص المعطيات التي ترتبط بها: (رقم الجوال، عنوان البريد الإلكتروني، ورقم بطاقة الائتمان، والبيانات الشخصية (الصوت، وبصمات الأصابع، والحمض النووي، والبيانات البيومترية للضحايا) على اختلاف تأثيرها ونسبة ضررها على الضحايا على الرغم من وجود مراقب يشرف على هذه البيانات في نص المادة (2) من قانون حماية البيانات الشخصية الأردني لسنة (2022).
3. لم يحدد المشرع الأردني نصوصًا تتعلق بتناول البطاقات، حيث أنه ينظر لمفهوم البطاقات بشكل منفصل حتى لا يتم الخلط بينها وبين معالجة البيانات الشخصية.
4. لم ينص المشرع الأردني وبشكل مفصل على تحديد مسؤولية المناول.
5. تبرز الحماية الجزائية للبيانات الشخصية كمطلب أساسي لتقليل مستوى الجريمة الإلكترونية، ومنها جريمة انتهاك حرمة البيانات الشخصية، وما يترتب عليها من مشكلات اجتماعية، واقتصادية، ونفسية للضحايا.
6. تتطلب الحماية الجزائية للبيانات الشخصية سن التشريعات التي تنظم البيئة الرقمية من خلال حماية البيانات الشخصية في ظل سهولة جمعها والاحتفاظ بها ومعالجتها، ولمنع الاعتداء على

حق المواطنين في حماية بياناتهم الشخصية، وخصوصيتهم المقررة بموجب أحكام الدستور والقوانين ذات العلاقة.

7. لم يُفصّل المشرع الأردني في العقوبات الجزائية فيما يخص انتهاك حرمة البيانات الشخصية إلا في حالات محددة، وهي: الدخول قصداً إلى الشبكة المعلوماتية، واستخدام وسيلة إلكترونية للضرر بالبيانات، والدخول دون تصريح للبيانات.
8. لم يتطرق قانون الجرائم الإلكترونية الحالي إلى نص محدد ومفصل لجريمة الوصول إلى عنوان (IP) للضحية، وإلى مصطلح التصيد الاحتيالي.

التوصيات:

في ضوء نتائج الدراسة يوصي الباحث المشرع الأردني بما يلي:

- يوصي الباحث المشرع الأردني بإيجاد عقوبات رادعة بحق المجرمين الذين ينتهكون هذه البيانات ويستخدموها لأغراض عدة.
- يوصي الباحث المشرع الأردني بإيجاد نصوص مفصلة بالعناصر المحددة للنطاق الجزائي لجريمة انتهاك البيانات الشخصية كالهوية الشخصية (الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية).
- يوصي الباحث المشرع الأردني بإضافة نصوص محددة ترتبط بـ: (رقم الجوال، عنوان البريد الإلكتروني، ورقم بطاقة الائتمان، والبيانات الشخصية (الصوت، وبصمات الأصابع، والحمض النووي، والبيانات البيومترية للضحايا) وجريمة البطاقات، وجريمة الوصول إلى عنوان (IP) للضحية، والتصيد الاحتيالي.
- يوصي الباحث المشرع الأردني بنصوص محددة وصريحة تتناول: الدخول قصداً إلى الشبكة المعلوماتية، واستخدام وسيلة إلكترونية للضرر بالبيانات، والدخول دون تصريح للبيانات.

المصادر والمراجع

أولاً: الكتب القانونية

- إبراهيم، خال (2009). **الجرائم المعلوماتية**، دار الفكر الجامعي: عمان.
- أبو حجيلة، علي (2011). **الحماية الجزائية للعرض في القانون الوضعي والشريعة الإسلامية**، ط1، دار الثقافة للنشر والتوزيع.
- أبو عامر، محمد (2010). **قانون العقوبات**/ القسم العام، دار الجامعة الجديدة، عمان.
- أبو فارة، يوسف (2012). **الأعمال الإلكترونية**، جامعة القدس المفتوحة، رام الله.
- الأهواني، حسام الدين (1978). **الحق في احترام الخصوصية**، دار النهضة العربية، القاهرة.
- بشابشة، زياد محمد (2015). **الحماية القانونية لحق الإنسان في صورته**، عمان، الاردن.
- بكار، حاتم (2002). **سلطة القاضي الجنائي**، منشأة المعارف–الإسكندرية.
- بني عيسى، حسين (2002). **شرح قانون العقوبات، القسم العام**، دار وائل للنشر، الطبعة الأولى، الأردن.
- البهجي، عصمت (2005). **حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية**، دار الثقافة، الإسكندرية، ص22.
- الجبور، محمد (2012). **الوسيط في قانون العقوبات، دار وائل للنشر**، الطبعة الأولى، عمان.
- الجبور، محمد (2019). **الجرائم الواقعة على الأشخاص في قانون العقوبات الأردني**، ط1، دار المكتبة الوطنية.

- حجازي، عبد الفتاح (2007). **مباديء الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية**، المحلة الكبرى، مصر.
- حجازي، مصطفى أحمد عبد الجواد (2004). **المسؤولية المدنية للصحفي عن انتهاك حرمة الحياة الخاصة**، دار النهضة العربية، القاهرة، ص22.
- حجازي، مي (2004). **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت**، دار الكتب القانونية، القاهرة.
- الزعبي، علي احمد (2006). **حق الخصوصية في القانون الجئائي**، المؤسسة الحديثة للكتاب، طرابلس: بيروت.
- سرور، أحمد فتحي (2015). **القانون الجنائي الدستوري**، دار وائل: عمان.
- الشامي، سلامة (2018). جرائم الاعتداء على الحق في الخصوصية ف ضوء التطور التكنولوجي، جامعة الأقصى، غزة.
- الشهاوي، محمد (2005). **الحماية الجنائية لحرمة الحياة الخاصة**، دار النهضة العربية، القاهرة، ص41.
- الشوابكة، محمد (2011). جرائم الحاسوب والغ نترنت–الجريمة المعلوماتنية، (ط4)، دار وائل للنشر والتوزيع، الأردن.
- العبادي، محمد (2015). الجرائم المستحدثة في ظل العولمة، (ط1)، دار جليس الزمان، عمان: الأردن.
- القرعان، محمود أحمد (2017). **الجرائم الإلكترونية**، ط1، دار وائل للنشر والتوزيع: الأردن.

- المصري، نداء (2017). **خصوصية الجرائم المعلوماتية**، رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين.
- مصطفى، أحمد محمود (2010). **جرائم الحاسبات في التشريع المصري**، دار النهضة العربية، القاهرة.
- المغربي، جعفر محمود وعساف، حسين شاكر (2010). **المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول**، دار الثقافة للنشر والتوزيع، عمان، الأردن.
- هروال، نبيلة (2007). **الجوانب الإجرائية لجرائم الإنترنت في مرحلة الاستدلالات**، دار الفكر الجامعي، الإسكندرية.
- الهيتي، محمد حماد (2006)، **جرائم الحاسوب**، دراسة تحليلية، دار المناهج للنشر والتوزيع، الطبعة الاولى، عمان، الأرد، ص12.
- الهميم، عبد اللطيف (2003). **احترام الحياة الخاصة**، دار عمان للنشر والتوزيع، عمان.

ثانيًا: الأبحاث

- آدم عبد البديع حسين (2000). **الحق في احترام الحياة الخاصة ومدى الحماية التي يكفلها القانون الجنائي**– دراسة مقارنة، دار النهضة العربية، القاهره، ص23.
- أبو عيد، عارف (2008). جرائم الإنترنت: دراسة مقارنة، **مجلة الشارقة للعلوم الشرعية والقانونية**، المجلد 5، العدد (3): 44–87، الإمارات، الشارقة.
- بحر، ممدوح خليل (1996). **حماية الحياة الخاصة في القانون الجنائي**، دراسة مقارنة، دار النهضة العربية، القاهرة.

- التهامي، سامح (2011). الحماية القانونية للبيانات الشخصية، **مجلة الحقوق**، المجلد 2، العدد (4)، ص33-55.
- الجنزوري، سمير (2015). السلطة التقديرية للقاضي في تحديد العقوبة، دراسة مقارنة بين القانون الإيطالي والقانون المصري، **المجلة الجنائية القومية**، المجلد 3، العدد (1)، 44-80، القاهرة، مصر.
- حسنية، أحمد (2017). الجريمة الإلكترونية بين الشرعية الجنائية والإجراءات، **مجلة جامعة الأزهر**، المجلد 2، العدد(19)، 22-140، القاهرة، مصر.
- الخلايلة، عايد (2011. **المسؤولية التقصيرية الالكترونية، دراسة مقارنة**، (ط2)، دار الثقافة للنشر والتوزيع، عمان: الاردن.
- الديحاني، فهيد (2014). الطبيعة القانونية للحق في الصورة الشخصية وحمايته المدنية في القانون الكويتي، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 28، العدد (56)، ص12-22.
- الزرفي، علي (2020). **الجريمة المعلوماتية الماسة بالحياة الخاص**- دراسة مقارنة-، (ط1)، مصر: المكتب الإقليمي.
- سدي، عمر (2020). المسؤولية الجنائية للطبيب على إفشاء السر، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، المجلد التاسع، العدد الثالث.

- سيد، أشرف جابر والشافي، خالد (2013). **حماية خصوصية مستخدمي مواقع التواصل الاجتماعي في مواجهة انتهاك الخصوصية في موقع فيس بوك**، بحث منشور بكلية الحقوق، جامعة حلوان: مصر.
- شكري، عادل (2008). **الجريمة المعلوماتية وأزمة الشرعية الجزائية**، مركز دراسات الكوفة، جامعة الكوفة، المجلد 2، العدد(7):133-175، الكوفة، العراق.
- الصغير، جميل عبد الباقي (2015). الحق في الصورة والإثبات الجنائي، **مجلة كلية القانون**، القاهرة، 2(2)، ص23-44، ص32.
- العمري، محمد (2016). الإثبات الجزائي الألكتروني في الجرائم المعلوماتية، دراسة مقارنة، **مجلة العلوم القانونية والسياسية**، السنة السادسة، المجلد 2، العدد (2)، 295، عمان، الأردن.
- العنزي، زياد (2018). المسؤولية القانونية عن طرد عضو من المجموعة في مواقع التواصل الاجتماعي في التشريع الأردني، **مجلة علوم الشريعة** والقانون، المجلد الرابع والخمسون، العدد الثاني.
- الغويري، ضيف الله (2014). ضمانات الحق في الحماية الخاصة في النظام السعودي، **مجلة المدير الناجح**، المجلد الثامن، العدد الثاني عشر، ص22-45.
- فضيلة، تومي (2017). أيديولوجيات الشبكات بالاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق، **مجلة العلوم الإنسانية والاجتماعية**، جامعة قصدي مرباح، الجزائر، المجلد الثاني، العدد الثلاثون، ص11-23.

- قاسم، محمد حسن (2011). **الحماية القانونية لحياة العمال الخاصة في مواجهة بعض مظاهر التكنولوجيا الحديثة**، منشورات الحلبي الحقوقية، لبنان، ص20
- الأكلبي، علي (2019). البيانات الضخمة واتخاذ القرار، بحث منشور في **مجلة الدراسات التكنولوجية**، الرياض، 15(2)، 12-34.
- لريد، أحمد (2011). ضوابط السلطة التقديرية للقاضي الجنائي في تخفيف الجزاء، **المجلة الأكاديمية للدراسات الاجتماعية والإنسانية**، المجلد 2 ، العدد(2)144-202، القاهرة، مصر.
- ممدوح، شريهان حسن (2020). الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي، **المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECS)**، المجلد 2، العدد الواحد والعشرون (كانون الثاني) جامعة شقراء، المملكة العربية السعودية.
- المؤيد، محمد (2009). صور المسؤولية التقصيرية الناشئة عن الاعتداء على بيانات الكمبيوتر والتعامل عبر الإنترنت وتسوية منازعاتها، **مجلة الدراسات الاجتماعية**، المجلد الثاني، العدد الثامن والعشرون، ص11-33.

ثالثًا: رسائل الماجستير

- الجبور، جواهر (2013). **السلطة التقديرية للقاضي في إصدار العقوبة بين حديها الأدنى والأعلى**، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، عمان: الأردن.

- ربايعة، عبد اللطيف (2016). **الجرائم الإلكترونية (التجريم والملاحقة والإثبات)**، رسالة ماجستير غير منشورة، جامعة اليرموك، إربد: الأردن.
- الزيود، فادي (2022). **جريمة الاعتداء على الحياة الخاصة بالوسائل الإلكترونية في التشريع الأردني ومدى مواءمتها مع الاتفاقيات الدولية**، رسالة ماجستير، جامعة عمان العربية، عمان: الأردن.
- السكر، سلطان فياض (2022). **جريمة انتهاك سرية المعلومات عبر الوسائل الالكترونية في التشريع الاردني**، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الاوسط، عمان: الأردن.
- سليم، بوزيدي (2016). الاعتداء على الحق في الصورة في ظل التطورات التكنولوجية الحديثة، رسالة ماجستير غير منشورة، جامعة عبد الرحمن، ميرة: الجزائر.
- صغير، يوسف (2013). **الجريمة المرتكبة عبر الإنترنت**، رسالة ماجستير غير منشورة، جامعة مولود معمري، الجزائر.
- ظاهر، سفيان(2023). **الحماية الجزائية لصورة الانسان الشخصية عبر الوسائل الالكترونية**، دراسة مقارنة، رسالة ماجستير غير منشورة، كلية الحقوق جامعة الزرقاء، الزرقاء: الأردن.
- العجمي، عبدالله دعش (2014).**المشكلات العملية والقانونية للجرائم الإلكترونية:** دراسة مقارنة، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، الأردن، عمان: الأردن.

- العنزي، سليمان مهجع (2003). **وسائل التحقيق في جرائم نظم المعلومات**، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأهلية، المملكة العربية السعودية.
- لامي، بارق (2017). **جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني**، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، عمان: الأردن.
- المصري، نائل فايز (2017). **خصوصية الجرائم المعلوماتية**، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية، فلسطين.

رابعًا: أطاريح الدكتوراه

- الجبوري، بيرك فارس (2009). **حقوق الشخصية وحمايتها المدنية**، دراسة مقارنة، أطروحة دكتوراه غير منشورة، جامعة القاهرة، القاهرة: مصر.
- صادق، طارق (2015). **الجرائم الإلكترونية جرائم الهاتف المحمول**– دراسة مقارنة، أطروحة دكتوراه غير منشورة، (ط1)، جامعة حلوان، حلوان: مصر.
- عثمان، بكر (2016). **المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التواصل الاجتماعي**، أطروحة دكتوراه غير منشورة، جامعة طنطا: مصر.

خامسًا: المؤتمرات:

- كامل، جبالي (2016). **حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية**، كلية الحقوق، جامعة أسيوط في الفترة من (12–13) إبريل.

سادسًا: التشريعات الأردنية

- الاتفاقية الأوروبية لحقوق الإنسان.
- الجمعية الأردنية للمصدر المفتوح (2022). **مشروع قانون حماية البيانات الشخصية لسنة (2022)**، التقرير السنوي لعام 2022.
- العقوبات الأردني رقم (16) لسنة (1960).
- قانون الاتصالات رقم (15) لسنة (1995) حتى (2023).
- قانون الجرائم الإلكترونية رقم (17) لسنة (2023).
- قانون المطبوعات والنشر الأردني وتعديلاته لعام(2023).
- وزارة الاقتصاد الرقمي والريادة (2021). **قانون حماية البيانات الشخصية لسنة** (2021)، التقرير السنوي لعام 2021.

سابعًا: مراجع الإنترنت:

- حموري، شهد والمصري، ريم (2014). قانون حماية البيانات الشخصية الأردني، ما يمكن تعلمه من تجارب الدول الأخرى، مقالة منشورة على مدونة حبر، متاحة عبر الرابط الإلكتروني: www:7iber.com/wp-content/uploads/2016/01/Reem.pdf.، تمت الزيارة بتاريخ: 15-9-2023، الساعة 8:35 صباحًا.

المراجع الأجنبية

Belharet, A. (2020). **A Study on the Impact of Artificial Intelligence on Project Management of Technology Information Systems**.

Change, W. (2019). A. **Data Environmental Management Systems in the Convention and Exhibition Industry**. Ekoloji Dergisi.2(2), 107

Cortellazzo, L., Bruni, E., and Zampieri, R., (2019). The Role of Leadership in a Digitalized World: **Ar reciew, Front Psychol**. 10(1), 12-44.

Harkut, D., & Kasat, K. (2019). **Artificial Intelligence-Scope and Limitations**. InntechOpen.

Hudasi, L (2020). Artificial intelligence usage opportunities in smart city data management. **Interdisciplinary Description of complex Systems**: INDECS, 18(3), 382-388.

Koh, J. L., Chai, C. S., Wong, B., & Hong, H.Y. (2015). **Artificial Intelligence, Conceptions and applications in teaching and Learning** . *Springer.*

Muise, A., Christofides, E., & Desmarais, S(2009). More information than you ever wanted: Does Facebook bring out green –eyed monster of jealousy, **CyberPSYChology & Behavior**. 12(4), 441-444.

The Scope of Criminal Protection for Electronic Personal Data in Jordanian Law

Preprard By

Falaah M Dawwud AL-Duykat

Supervised By

Dr: Muhamad Salim AL-Shahin

ABSTRACT

The study aimed to Know the scope of criminal protection for electronic personal data in Jordanin Law; the Legal concept of personal data rekates to victims who have been subjected to the crime of breaching their personal data through technology with their specific elements; such as personal identity, so that data od apersonal nature for victims os consideted, in the legal sense, an electronic crime punishable by law, therefore, in the first chapter, the researcher in his corrent study explained itsbbtreatment of personal data and the scope of its protection with regard to identifying the victim, and the coditions for obtaining personal data, the effects of processing it, and its impact on privacy, in the second chapter, the researcher also discussed the scope of criminal protection for personal data in accordance with the current cybercrime law; such as the technical compass Known as cookies and electronic phishin and theft of aperson's identity. On the other hand, the criminal penalties for violating the sancitiy of personal data through technology, which included the penalty for accessing the information network, the penalty for using an electronic means to damage the data, and the penalty for unauthorized access to the data, this is by reference to the Jordanian Penal Code No (16) of (1960) and Cybercrime Law No (17) of (2023) and Communications Law No (15) of (1995) and its amendments (2023) and

Jordanian Press and Publishing Law and its anendments and the European Convention on Human Rights. The researcher concluded that the Jordanian Legislator, in the text of Article (2) of the Personal Data Protection Law of (2022), supported the safety of data and the main role of the Council of Ministers with regard to the conditiond fpr disclosing this data, Howrver, he did not specify the scope of criminal protection with regard to data related to personal data , such as mobile number, email address, and credit card number and Personal datd (voice, fingerprints, DNA, and biometric data of the victims). The Jordanian Legislator also did not specify in the current electronic crimes and communications law texts related to the crime of cards and the crime of cards and the crime of accessing the victm;s (IP)address. These two term technical cultural compass Known as cookies and the term phishing.