ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد السابع والسبعون
تاريخ الإصدار: 2 – آذار – 2025م
www.ajsp.net

"الحماية القانونية للبيانات الشخصية في المعاملات الالكترونية في ظل التشريع الاردني والتشريع الاوروبي (GDPR) دراسة مقارنة"

إعداد الباحثة:

لينا رياض الرمحي

رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير 2024 / إشراف الدكتور مهند أبو مُغلي

جامعة عمان العربية – كلية القانون– قسم القانون الخاص

https://doi.org/10.36571/ajsp7719

الإصدار الثامن – العدد السابع والسبعون
تاريخ الإصدار: 2 – آذار – 2025م
www.ajsp.net
ISSN: 2663-5798 || Arab Journal for Scientific Publishing

المُلخص:

تناولت هذه الدراسة موضوعا حديث النشأة، ألا وهو حماية البيانات الشخصية، وذلك من خلال تناول الأحكام القانونية المتعلقة بها وفقا لقانون حماية البيانات الشخصية الأردني، وGDPR.

هدفت هذه الدراسة، إلى تقديم أفضل الطرق لحماية البيانات الشخصية، وتحسين القوانين بما يتماشى مع التشريع المقارن، كما وبرزت أهمية الدراسة، في توضيح نقاط ضعف التشريع الأردني، وبيان مدى انسجامه مع معايير الحماية التي وفرها التشريع المقارن، ابتداء من الحقوق التي وفرها للأفراد، والمبادئ التي ارتكز عليها، وأدوات تنفيذ القانون، وضمان الامتثال له، وصولا إلى بيان مدى كفاية التشريع الأردني لحماية البيانات الشخصية، وذلك باتباع المنهج الوصفي، والمنهج التحليلي، والمنهج المقارن.

وكان من أبرز النتائج التي توصلت إليها الدراسة، كثرة الاستثناءات على النص التشريعي، كما وتوصلت الدراسة إلى وجود ازدواجية بين مسؤوليات، ومصالح الهيئات التي أنشأها المشرع بموجب القانون.

ومن أبرز التوصيات، تحديد الاستثناءات بشكل دقيق، وتعزيز الرقابة الدورية على المؤسسات، وتوعية الأفراد بحقوقهم، وضمان الموازنة بين حماية الحقوق الفردية، والمصالح المشروعة، وبالنسبة لهيئات تنفيذ القانون، كانت التوصية أن يتم تشكيلها بإتباع أسس ذات آلية محددة، وواضحة بموجب القانون.

كلمات مفتاحية: حماية البيانات الشخصية، الحق في المحو، الخصوصية الرقمية، البيانات الشخصية الحساسة،GDPR , DPO.

المقدمة:

في إطار التحولات الرقمية المتسارعة على مستوى العالم، أصبحت حماية البيانات الشخصية قضية محورية بالنسبة للحكومات والشركات والمواطنين على حد سواء، وبالنسبة للتشريع الأردني فهو يشهد خطوات حقيقية نحو تنظيم، وتحقيق التوازن بين حماية الخصوصية من جهة، وحرية الاستخدام والتبادل التجاري للبيانات من جهة أخرى، فقد أصبح الاهتمام بحماية البيانات الشخصية جزءًا من إستراتيجيات تطوير الاقتصاد الرقمي، وتعزيز الشفافية، والمساءلة في التعامل مع البيانات، وبالإضافة إلى أن الدستور الأردني نص في مادته السابعة على حق الأفراد بالخصوصية، وعلى تجريم الاعتداء على خصوصيتهم، وتجلى اهتمام المشرع الأردني بهذه الحماية، من خلال قيامه بعمل تشريع خاص لحماية البيانات الشخصية، القانون رقم (24) لسنة 2023. (الدستور الأردني،1956)

ستقوم الباحثة بتوضيح كيفية حماية البيانات ضمن التشريع الأردني، مُقارِنةً ذلك مع الحماية التي وفرها التشريع الأوروبي، والمتمثل في اللائحة العامة لحماية البيانات الشخصية، للوقوف على أهم المفارقات من إيجابيات وسلبيات التشريعين، والتحديات التي تواجه التشريع الأردني وتعيق الارتقاء به إلى مستوى الحماية التي وفرها ال GDPR، وفي النهاية العمل على إيجاد حلول عملية لهذه التحديات.

مشكلة الدراسة

1. عدم كفاية الأحكام التشريعية التي تضمن امتثال الأفراد، والكيانات التجارية للنص التشريعي.
2. كثرة الاستثناءات التي وردت على التشريع، مما أدى إلى إفراغ القاعدة التشريعية من مضمونها.

ولذلك سيتم الوقوف على أوجه القصور التشريعي وتوضيح القواعد القانونية المتعلقة بحماية البيانات الشخصية ومحاولة معالجتها، ويمكن تلخيص مشكلة الدراسة بالإجابة عن السؤال الآتي:

- ما مدى كفاية النصوص القانونية في استيعاب الجوانب المتعلقة بحماية البيانات الشخصية للفرد الأردني وفقا لقانون حماية البيانات الشخصية رقم (24) لسنة (2023)؟

أسئلة الدراسة:

تسعى الدراسة للإجابة عن التساؤلات التالية:

1- ما هي الأهمية القانونية لحماية البيانات الشخصية كجزء من المعاملات الإلكترونية؟
2- ما الإطار القانوني الذي تستند عليه حماية البيانات الشخصية في كل من التشريع الأردني والتشريع المقارن؟
3- ما الثغرات القانونية والتحديات التي تواجه حماية البيانات الشخصية في التشريع الأردني، مقارنة باللائحة الاوروبية؟

أهداف الدراسة:

تسعى الدراسة إلى تحقيق جملة من الأهداف هي:

- إظهار مدى التشابه والاختلاف بين التشريع الاردني والتشريع المقارن مما يسهل تحديد ثغرات التشريع الاردني.
- والعمل على تحسين، وتعزيز القوانين المحلية بما يتماشى مع التشريع المقارن، وتوضيح اهمية حماية البيانات الشخصية، وأثرها على الافراد والكيانات التجارية.

أهمية الدراسة:

تأخذ هذه الدراسة أهميتها من:

الأهمية النظرية:

ستسهم الدراسة في تفسير وتعزيز المعرفة حول التشريعات الاردنية في مجال حماية السجل الالكتروني بشكل عام وحماية البيانات الشخصية بشكل خاص، ومقارنتها مع التشريعات الاوروبية المتأثرة بتوجيهات الاتحاد الاوروبي واللائحة العامة لحماية البيانات (GDPR)، وكشف نقاط ضعف التشريع الاردني، ودراسة مدى انسجام التشريع الاردني مع الواقع العملي من جهة، وانسجامه ومواكبته التغيرات التقنية والتكنولوجية وتعزيز حماية حقوق الافراد والكيانات التجارية وحماية خصوصيتهم. كما وتسعى الدراسة لبيان التحديات والمعوقات التي تواجه تنفيذ النصوص القانونية.

الأهمية العملية:

توفر الدراسة نظرة للممارسين القانونيين بالعمل على تحسين الإطار القانوني من خلال التعرف على الثغرات القانونية في التشريع الأردني ومقارنتها بالتشريع الأوروبي مما يساهم في تحسين القوانين المحلية، وتطويرها بما يتماشى مع الواقع العملي، كما ان هذا سيؤدي الى خلق حماية عالية للبيانات مما يعزز ثقة المتعاملين بالتعاملات الالكترونية، وايضا تقليل المخاطر القانونية الناتجة عن الانتهاكات المحتملة للبيانات الشخصية وتجنب حدوثها، وستعمل الباحثة على أن يكون بحثها داعما، ومساندا، و مفيدا لوزارة الاقتصاد الرقمي والريادة، وللمحامين، وللقضاة، والعاملين في مجال المعاملات الالكترونية سواء التجارية او المدنية.

التعريفات الاصطلاحية والإجرائية:

GDPR: (General Data Protection Regulation) اللائحة العامة لحماية البيانات الشخصية: هي تشريع أُوروبي صادر عن البرلمان والمجلس الاوروبيين، يهدف الى توضيح المبادئ الاساسية مثل حماية البيانات الإلكترونية للأفراد وتعزيز الخصوصية، و توحيد قوانين حماية البيانات في جميع دول الاتحاد الأوروبي. (اسخيطه، 2018)

حماية البيانات الشخصية: مجوعة القواعد القانونية التي تنظم وتحدد الاجراءات المتبعة لحماية المعلومات الشخصية من الانتهاك او الاستخدام الغير مصرح به. (قانون حماية البيانات الشخصية رقم 24 لسنة 2023)

DPO: (Data Protection Officer) أو مسؤول حماية البيانات وهو شخص مكلف بالإشراف على استراتيجية حماية البيانات في المؤسسة، وضمان الامتثال للقوانين واللوائح المتعلقة بحماية البيانات. (اسخيطة،2018)

الحق في محو البيانات الشخصية: هو مفهوم نصت عليه المادة 17 /1/ه من اللائحة العامة لحماية البيانات الشخصية يتيح للأفراد إمكانية طلب إزالة معلوماتهم الشخصية من الإنترنت. (مشعل،2017)

الخصوصية الرقمية: تشير إلى حقوق الأفراد في التحكم بمعلوماتهم الشخصية وكيفية جمعها واستخدامها وتخزينها عبر الإنترنت. (مشعل، 2017)

البيانات الشخصية الحساسة: "وهي المعلومات التي تتعلق بشخص معين وتكون حساسة بطبيعتها، مما يتطلب حماية إضافية، وتشمل هذه البيانات: المعلومات الصحية، والبيومترية، والآراء السياسية وغيرها". (قانون حماية البيانات الشخصية رقم 24 لسنة 2023)

حدود الدراسة:

تتمثل حدود الدراسة ومحدداتها فيما يلي:

الحدود المكانية: الدراسة ستكون مقارنة ما بين التشريعين من أجل تحديد الثغرات القانونية التي تفتقر إليها القوانين والأنظمة المعمول بها في الأردن دون التطرق إلى تجارب دول أُخرى في هذا المجال.

الحدود الموضوعية: تركز الدراسة على حماية البيانات الشخصية للأفراد في المعاملات الإلكترونية، وتحليل الحقوق والالتزامات المترتبة على الأفراد والمؤسسات فيما بين التشريع الأردني والمقارن.

الحدود الزمانية: جرت الدراسة في سنة 2024، مما يجعل بعض القوانين غير ملائمة، او متقادمة بطريقة لا تتماشى مع التطور التكنولوجي الذي قد يحصل مستقبلا.

الدراسات السابقة ذات الصلة

لغرض البحث في موضوعات الدراسة قامت الباحثة بالرجوع إلى العديد من الدراسات السابقة ذات العلاقة بالدراسة:

أجرى **سويلم** (2022) دراسته التي اعتمدت على المنهج المقارن، فحلل الباحث التشريعات القانونية المصرية المتعلقة بحماية الخصوصية في مجال شبكة المعلومات الإلكترونية، وقارنها في ما جاء باللائحة الأوروبية لحماية البيانات الشخصية جنائياً ومدنيًا، كانت مشكلة دراسته تتمحور حول بيان مفهوم البيانات الشخصية الإلكترونية، وبيان الجهات التي تقف على حمايتها، وصولا إلى كيفية تعزيز هذه الحماية على الجانبين الجزائي والمدني، و كان أهم نتائجها أن المسؤولية القانونية تترتب على أي مساس بالبيانات الشخصية وبالتالي يترتب التعويض عن أي ضرر ينتج عن ذلك.

أجرت **عبد الرحمن** (2022) دراستها التي اعتمدت على المنهج الوصفي التحليلي لنصوص قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020، المتعلقة بموافقة الشخص المعني، ومقارنتها بما يقابلها من لائحة الإتحاد الأوروبي، وقانون حماية البيانات البريطاني، وكانت مشكلة دراستها تتمحور حول حماية التشريع المصري للبيانات الصحية الحساسة، وتأثير عدم حمايتها على الأمن المعلوماتي، والأمن الصحي، وكان من أهم نتائجها: أمن المعلومات والبيانات، جزء لا ينفصل عن استقرار المجتمع، وأهم التوصيات كانت: تحديد ضوابط موافقة الشخص المعني بالبيانات بصورة واضحة، وتحديد المقصود بالموافقة الصريحة.

التعقيب على الدراسات السابقة وموقع الدراسة الحالية منها.

تناولت الدراسات السابقة حماية الخصوصية وحماية البيانات الشخصية، وخصائصها وأهميتها قبل صدور قانون حماية البيانات الشخصية الأردني رقم (24) لسنة (2023)، فتميزت الدراسة الحالية عن الدراسات السابقة؛ من حيث تناولها للأحكام القانونية الجديدة المتعلقة بحماية البيانات الشخصية أن هذه الدراسة ستقوم على بيان أهمية توفير الحماية للبيانات الشخصية كونها جزء من السجل الإلكتروني الذي يعد جزءا هاما في المعاملات الإلكترونية، وذلك بمقارنته مع التشريع الأوروبي من حيث الإطار والأدوات التي يوفرها لهذه الحماية.

المنهجية والإجراءات:

دراسة الباحثة هذه تقوم على المنهجية العلمية وفي سبيل ذلك سلكت الباحثة في دراستها طرق البحث العلمي الآتية:

المنهج الوصفي إن الإشكالية والدراسة التي نقوم بها هي (الحماية القانونية للبيانات الشخصية في المعاملات الالكترونية في ظل التشريع الأردني والتشريع الأوروبي) وهي إشكالية تفرض علينا وصف ودراسة هذه الإشكالية من جميع الجوانب القانونية، والتشريعية، والقضائية، نظراً لعدم وجود تنظيم تشريعي يرتقي إلى مستوى التشريع الأوروبي في قوة الحماية للبيانات الشخصية.

المنهج التحليلي ستقوم الباحثة بجمع، وتحليل النصوص القانونية، والتشريعية المتعلقة بحماية البيانات في التشريع الأردني، والتشريع المقارن، وبالتحليل، والتوفيق بين هذه النصوص واشكالية البحث.

المنهج المقارن ستقوم الباحثة بإجراء مقارنة ومقابلة بين نصوص التشريع الأردني ومثيلاتها في التشريع الأوروبي، بهدف استخلاص الأحكام القانونية منها، وفهم الاختلافات، والاتفاقات فيما بينها، من حيث الحماية القانونية للبيانات الشخصية، ومقارنة مدى امتثال الأفراد والكيانات التجارية لتنفيذ القانون، المتعلق بها في الأردن ودول الإتحاد الأوروبي.

وتم تقسيم هذه الدراسة إلى المبحثين التاليين:

المبحث الأول: قانون حماية البيانات الشخصية الأردني ومقارنة نطاق تطبيقه مع GDPR

قام المشرع الأردني بإصدار قانون حماية البيانات الشخصية رقم 24 لسنه 2023 بتاريخ 17 سبتمبر 2023، والذي بدأ العمل به اعتبارا من 17 مارس 2024، ودعى القانون جميع الكيانات التي تتعامل بالبيانات أن تصوب أوضاعها قبل نفاذ أحكامه، خلال مده سنة من تاريخ العمل به، على أن تبدأ فترة الامتثال في مارس 2025. (مديرية حماية البيانات الشخصية،2024)

يهدف هذا القانون إلى تعزيز الخصوصية والثقة الرقمية، وحماية البيانات، من خلال تنظيم ومعالجة البيانات الشخصية، وضمان حقوق الأفراد في الوصول إلى بياناتهم، وتصحيحها، وحذفها والاعتراض على استخدامها، ولتحقيق الحقوق والحريات الدستورية التي نص عليها الدستور الأردني، وإيجاد إطار قانوني يوازن بين آليات حقوق الأفراد في حمايه البيانات الشخصية، وبين السماح بمعالجة البيانات، والسعي إلى سد الثغرات القانونية، التي تضمنها قانون المعاملات الإلكترونية الملغي (2001)، والمعدل بموجب قانون المعاملات الإلكترونية رقم (15) لسنة (2015)، والذي أيضا جاء حاملاً في طياته، قصورًا واضحاً في مجال حماية البيانات الشخصية.(ربيحات،2024)(الجعافرة،2022)

وعلى رأس الأهداف السابقة الذكر لقانون حماية البيانات الشخصية هو هدف الوصول في تعزيز حمايه البيانات الشخصية في الاردن إلى مرتبة الحماية التي فرضهاGDPR، لذلك جاء هذا القانون متأثراً إلى حدٍ كبير بالتشريع المقارن، وكان ذلك التأثر واضحاً من خلال نصوصه التي حددت حقوق الشخص المعني، والإجراءات المتبعة لحمايتها، فكانت الأهداف التي سعى قانون حماية البيانات الشخصية الأردني إلى تحقيقها والحقوق التي فرضها للفرد؛ هي ذات الأهداف والحقوق التي جاءت بها وسعت لحمايتها اللائحة الأوروبية، وكذلك توحدت المبادئ التي ارتكز عليها التشريعان.

أما المادة الثالثة من قانون حماية البيانات الشخصية الأردني، فقد نصت على أن يكون سريان تطبيق القانون بأثر رجعي من لحظة نفاذه، ويعني ذلك سريانه بأثر رجعي على جميع البيانات الشخصية في المعاملات الإلكترونية التي تم جمعها ومعالجتها قبل نفاذه، ويُخضع للقانون كلا القطاعين العام والخاص في تنظيم كيفية جمع، ومعالجة، وتخرين البيانات الشخصية، وقد أخرج من نطاق تطبيقه معالجة الأشخاص الطبيعيين لبياناتهم الشخصية. (ربيحات،2024)

نستنتج مما سبق؛ أن قانون حماية البيانات الأردني، يتوافق في نطاق تطبيقه من حيث الأشخاص والموضوع مع اللائحة العامة لحماية البيانات الشخصيةGDPR، إلا أنه يختلف معه في ضيق نطاق التطبيق الجغرافي، حيث أنه يسري على الأشخاص الأردنيين فقط المقيمين على الأراضي الأردنية، إلا أن ال GDPR يشمل رقعة جغرافية أكبر، وهي دول الإتحاد الأوروبي، وقد حددت المادة الثالثة منه النطاق الإقليمي لتطبيقه والتي نصت على أن يطبق على كل مما يلي:

1. "فروع الشركات الأوروبية التي تقوم بمعالجة البيانات الشخصية لأفراد الإتحاد الأوروبي والتي تقع ضمن الإتحاد الأوروبي وخارجه طالما أن المعالجة في هذه الشركات تخضع لمراقب أو معالج في دول الإتحاد الأوروبي.

2. في حال كانت المعالجة تتم على بيانات أفراد موجودين ضمن نطاق الإتحاد الأوروبي جغرافياً، لكن المعالجة تتم من قبل شركات، أو فروع لشركات، ليست خاضعة لمراقب، أو معالج ضمن الإتحاد الأوربي، وذلك في الحالات التي تكون فيها المعالجة مترافقة مع ما يلي:
   أ- عرض بضائع، أو خدمات على أشخاص ضمن الإتحاد الأوروبي، سواء كان مقابلها مادي أو من دون مقابل.
   ب- إذا كانت المعالجة مرافقة لمراقبة سلوك هؤلاء الأشخاص؛ مادام هذا الأمر تم ضمن الإتحاد الأوروبي.
3. معالجة البيانات الشخصية لمراقب ليس له فرع في الإتحاد الأوروبي لكنه يخضع لقانون إحدى الدول الأعضاء بموجب القانون الدولي للدول الأعضاء". (اسخيطة، 2018) (GDPR, Article 2,3) (المادة3 من قانون حماية البيانات الشخصية،2023)

المطلب الأول: ماهية البيانات الشخصية والحساسة وفق التشريعين

لم يُعرِف المشرع في قانون المعاملات الإلكترونية الأردني رقم (15) لسنة (2015) الأردني مفهوم البيانات الشخصية بشكل مباشر، إلا أنه في المادة الثانية ذكر عدة تعريفات، ما يهمنا منها هنا هو التفاصيل التي ذكرها لوصف المعلومات الإلكترونية بأنها عبارة عن" رموز، وبيانات، وصور، ونصوص، وأصوات، وقواعد بيانات....". وكذلك أنه اعتبر كل من البريد الإلكتروني، والرسائل القصيرة، أو أي تبادل للمعلومات إلكترونيا؛ هو رسالة بيانات.

من خلال استقراء هذين التعريفين، نجد أنهما أشارا إلى وصف طبيعة المعلومات، التي تحويها رسالة البيانات، والتي إذا ما قارناها بتعريف البيانات الشخصية، الوارد في قانون حماية البيانات الشخصية (2023)، نجد أنها هي نفسها تعد بيانات شخصية أو حساسة إلا أن قانون المعاملات الإلكترونية لم يعرفها ولم يأتي على ذكرها بشكل صريح ومخصص في نصوصه.

قانون حماية البيانات الشخصية قام بتعريف البيانات الشخصية، والبيانات الشخصية الحساسة في المادة الثانية منه، وقد كان تعريفه متوافقاً إلى حد ما مع التعريف الذي نصت عليه اللائحة الأوروبية، وقد ذكر في نصه: "..... مهما كان مصدرها، أو شكلها بما في ذلك البيانات المتعلقة بشخصه أو وضعه العائلي أو أماكن تواجده." نجد بالرجوع إلى عبارة مهما كان مصدرها، تبين مبدئيا أن هذا القانون وضع لحماية البيانات الشخصية بشكل عام، بغض النظر عن ما إذا كان جمعها، وحفظها، وتخزينها تم بطريقة إلكترونية أو غير إلكترونية، وهذا أيضا ما أكدته هذه المادة عندما عرفت قواعد البيانات بأنها سجلات تحتوي معلومات شخصية حتى لو كانت هذه السجلات ورقية، فالفيصل هو وجود معلومات شخصية مخزنة عليها، ليشملها نطاق حماية قانون حماية البيانات الشخصية.

ونجد هنا أنه توافق مع اللائحة الأوروبية بهذا، حيث أن المادة الثانية البند الأول منها أكدت على حماية البيانات الشخصية، سواء كانت إلكترونية، أو غير إلكترونية، سواء كانت لمعاملات مدنية أم تجارية، فالمهم هو أنها تحوي بيانات شخصية، لأشخاص مشمولين ضمن نطاق حمايتها الإقليمية.

كما وأن المشرع الأردني في نفس المادة وعند الحديث عن البيانات الشخصية الحساسة، ذكر: " ...أو أي معلومات أو بيانات يقرر المجلس اعتبارها حساسة إذا كان إفشاؤها أو سوء استخدامها يلحق ضررًا بالشخص المعني بها"، وباستقراء هذا النص نجد أن المشرع ترك أمر تحديد ما إذا كانت حساسة أم لا سلطة تقديرية بيد مجلس حماية البيانات؛ حتى يصار إلى اعتبارها حساسة في حال لم تكن من ضمن البيانات المذكورة في التعريف، لكن هنا يستوقفنا سؤال لو مثلًا تم الإخلال بأمن، بيانات حساسة لشخص ما فهل عليه أن

يعود للمجلس ويتأكد بعد ذلك، فيما إذا كانت حساسة أم لا؟؟؟ أم من الأفضل أن تكون هذه البيانات محددة منذ البداية بنص القانون، لكل من المعالج والمراقب، ليقوموا بحمايتها كبيانات حساسة تحتاج لتوفير حماية مشددةٍ لها؟ (قانون حماية البيانات الشخصية، 2023)

ترى الباحثة، إنه وبالرغم من حرص المشرع على المرونة في هذا القانون، إلا أن هذه ثغرة في النص التشريعي، كون البيانات الحساسة ونظراً لطبيعتها كان يجب الاهتمام أكثر بتفصيلها، وحصرها، حتى يتم تشديد الحماية عليها، وتشديد العقوبة على الشركات في حال عدم الامتثال للقوانين المفروضة عليهم لحمايتها، وأخيراً كي لا يترك مجال للاختلاف مستقبلاً فيها بين المراقب والمعالج، أو القضاة، أو العاملين في مجال البيانات الشخصية.

وضع المشرع الأردني على هذه البيانات قيداً يستند إليه قرار المجلس للفصل فيما إذا كانت حساسة أو لا، وهو "....إذا كان إفشاؤها أو سوء استخدامها يلحق ضراً بالشخص المعني"، وهذا القيد من خلال هذه الدراسة تجد الباحثة أنه ما هو إلا إضافة لا داعي لها حيث أن الحماية المدنية بشكل عام تقوم دائما طالما أن هناك مسؤولية تقصيرية نتيجة فعل، أو عقدية نتيجة الإخلال بالتزام عقدي ترتب ضرراً وعلاقة سببية تربط بينهما، وبإسقاط ذلك على موضوعنا هنا نجد أن الانتهاك لخصوصية الفرد مجرم بحد ذاته، وهو ليس فيصلاً في تحديد ما إذا كانت هذه البيانات حساسة أم لا، بل إن تحقق الضرر ووجود الرابطة السببية بينه وبين الفعل، ما هو إلا وسيلة لإيقاع العقوبة على الفاعل.(شرقاوي ،2022)

اللائحة الاوروبية كانت أكثر توضيحاً، في تفسير وبسط مفهوم البيانات الشخصية، من المشرع الأردني، بالرغم من أنها لم تضع نصًا خاصاً يضم تعريف مصطلح البيانات الحساسة، بل ضمت البيانات الحساسة والشخصية في مصطلح واحد، إلا أنها قامت بتعريف كل من البيانات الوراثية، والبيانات الطبية، والبيانات البيومترية، كلٌ في تعريف منفصل يضفي عليها صفة الوضوح والتحديد، ويمنع الخلط فيما بينها وبين غيرها من خلال إعطاء أمثلة واضحة عليها، وبذلك لم تترك أمر تقدير ماهية البيانات الحساسة إلى سلطة أخرى غير سلطة القانون، كما فعل المشرع الأردني عندما ترك أمر تحديد مالم يتم ذكره منها إلى المجلس. (GDPR, 2018)

ولا ننسى هنا أن نذكر أن المشرع الأردني جعل المعلومات الجنائية من ضمن البيانات الحساسة، وهذا ما لم تأتِ على ذكره اللائحة الأوروبية بشكل مباشر، وأخيرا نستنتج أن كلا التشريعين فرضا حماية على البيانات الشخصية، وجعلاها مشددةً أكثر على الحساسة منها، نظراً لطبيعتها، إلا أنهما اختلفا في بعض فئات البيانات التي تصنف كبيانات حساسة.

المطلب الثاني: المبادئ العامة وحقوق الأفراد

الفرع الأول: مقارنة المبادئ العامة في التشريعين

تتنوع المبادئ التي تم تحديدها في قانون حماية البيانات الشخصية الأردني، والتي هدف منها المشرع إلى ضمان حماية البيانات الشخصية للأفراد، وتعزيز حقوقهم في هذا المجال، وهذه المبادئ تتماشى مع المعايير الدولية لحماية البيانات، وخصوصاً ال GDPR وتتلخص هذه المبادئ التي نص عليها القانون في:

1. مبدأ الشفافية والمساءلة:

وهذا المبدأ يقتضي أن تجمع المعلومات، وتعالج بطرق قانونية، وشفافة، وبعلم الأشخاص المعنيين، بحيث يجب أن يكون الأفراد على علم ودراية بالمعلومات التي يتم جمعها، وما الغرض من المعالجة، وهذا ما نصت عليه المادة الرابعة البند ب الفرع الأول، من التشريع الأردني، وقد وضح المشرع الأردني في المادة التاسعة الأمور التي على المعالج إطلاع الشخص المعني عليها، إلا أن المشرع الأردني لم يعالج حالة ما إذا كانت البيانات يتم جمعها من شخص ثالث، كما فعل المشرع الأوربي وهذا ما ستقوم الباحثة بتوضيحه عند الحديث عن الحقوق التي منحها القانون للأفراد، وبالتحديد الحديث حق الوصول والاطلاع.

أما المساءلة والتي يقصد بها مساءلة الشخص المسؤول عن حماية البيانات، فقد تم النص عليها في المادة الثالثة عشر والمادة عشرون على ب من التشريع الأردني، وباستقراء نص المادة نجد أن المشرع الأردني توافق مع التشريع المقارن من حيث أن جعل المعالج والمسؤول يعرضان نفسهما للعقوبة والمساءلة في حال عدم حفاظهما على سرية البيانات، وبذلك تتعرض للعقوبة الجهة المتسببة بحدوث الخطأ المؤدي إلى تسريب البيانات، أو التعدي عليها، نتيجة عدم امتثاله لنصوص القانون.

ومن وجهة نظر الباحثة؛ إن كلا التشريعين يشترطان أن تتم معالجة البيانات بشكل قانوني وشفاف، مع تزويد الأفراد بالمعلومات الضرورية حول كيفية معالجة بياناتهم، إلا أن مبدأ الشفافية في التشريع الأردني بحاجة إلى الكثير من الاهتمام والتعزيز كونه يمنح الأفراد التمتع بحقوقهم التي فرضها القانون لهم ليأتي مبدأ المساءلة جنبا إلى جنب مع الشفافية، ويؤكدان على الحماية للحقوق الشخصية، ويدعمان احترام خصوصية الأفراد، وبالنهاية يعد ذلك مؤشراً على امتثال المؤسسات للقانون، مما يعزز الثقة في المعاملات الرقمية.

2. مبدأ تحديد الغرض:

يقتضي هذا المبدأ أن البيانات يجب أن تجمع لغرض محدد، ومشروع ولا يجوز استخدامها لأغراض أخرى غير تلك التي تم جمعها من أجلها، وهذا المبدأ يرتبط مع حق تخصيص نطاق المعالجة، كما ونصت عليه المادة السابعة البندين أ و ب من قانون حماية البيانات الشخصية الأردني، وكذلك التشريع الأوروبي في المادة الخامسة البند الأول الفرع ب، الذي منع استخدام البيانات لغير الغرض الذي جمعت من أجله، وتم أخذ موافقة الأفراد عليه.

وبالنتيجة، ترى الباحثة، أن كلا التشريعين اشترطا تحديد الغرض من جمع البيانات، وتحديد الغاية من المعالجة لتكون قانونية ومشروعة، إن هذا المبدأ يتفق مع حق الشخص المعني بالعلم بالغرض الذي جمعت من أجله بياناته، وبالتالي تحديد موقفه من الموافقة أو الرفض، لإجراء هذه المعالجة بناء على الغرض منها، فالأصل أن تعتبر المعالجة غير قانونية في حال كانت على غرض غير محدد من البداية وغير موافق عليه من صاحب البيانات.

3. مبدأ تقليص البيانات:

هذا المبدأ يتطلب من المعالجين جمع الحد الأدنى من البيانات المراد معالجتها، فلا يجوز جمع بيانات لا تتوافق مع الغرض من المعالجة، وبذات الوقت يجب أن يلتزم المسؤول بجمع الحد الأدنى، من البيانات هذا المبدأ يتكامل مع مبدأ تحديد الغاية، وقد نصت عليه المادة السابعة البند ب من التشريع الأردني، وقد وافق ذلك مع GDPR في المادة الخامسة البند الأول فرع c، التي اشترطت أن تكون البيانات المعالجة مقيدة بشكل كبير بالغرض من المعالجة.

من رأي الباحثة إن هذا المبدأ يحقق الأمان للبيانات الشخصية، كونه يفرض على المعالج الالتزام بجمع البيانات الضرورية للمعالجة، دون غيرها، مما يحفظ للأفراد خصوصيتهم، ويدعم كل من مبدأ الدقة في جمع المعلومات ومبدأ تحديد الغرض من الجمع.

4. مبدأ دقة البيانات:

مبدأ دقة البيانات ينص على أن تكون هذه البيانات محدثة وصحيحة ومتوافقة مع الواقع، وهذا ما نصت عليه المادة السابعة البند د، من التشريع الأردني، وهذ المبدأ يدعمه حق الفرد في تصحيح، وإضافة وتعديل البيانات الذي نص عليه المشرع الأردني في المادة الرابعة/ب/3، وتوافق ذلك مع المادة الخامسة/1/ د من اللائحة العامة؛ والتي أوجب أيضا أن تكون البيانات دقيقة ومحدثة، خالية من أي خطأ قد يؤثر على حقوق أو خصوصية الأفراد، وهذا يقتضي على المسؤول القيام مباشرة بتصحيح، أو تعديل، أو حذف البيانات الغير متوافقة مع هذا المبدأ.

5. مبدأ الاحتفاظ في البيانات لفترة محددة:

باستقراء نص المادة السادسة/ب من قانون حماية البيانات الشخصية 2023، نجد أن المشرع وضع قاعدة عامة ألا وهي عدم الاحتفاظ في البيانات عند الانتهاء من غرض المعالجة، ووضع على هذه القاعدة استثناء، يجيز الاحتفاظ بالبيانات، في حال كان هناك نص قانوني يسمح بذلك، وهنا أيضًا نجد أن المشرع الأردني سار على نهج التشريع الأوروبي، والذي أوجب في المادة الخامسة/e/1 أيضا عدم الاحتفاظ في البيانات، كقاعدة عامة الهدف منها الحفاظ على الخصوصية، وحماية البيانات من التعدي، أو الاختراق، مالم يكن هناك نص قانوني يجيز ذلك، كالاحتفاظ بها مثلا لأغراض، الأبحاث العلمية، أو للمصلحة العامة.

التشريع الأوروبي حدد تفاصيل القيام بتحقيق هذا المبدأ من حيث؛ أنه أوجب على المتحكمين وضع حدود زمنية للحذف، والتأكد من علم الشخص المعني بالفترة اللازمة للاحتفاظ في البيانات، وبالنظر إلى المادة الثانية عشر من التشريع الأردني، نجد أن المشرع ذكر من ضمن واجبات المعالج وفي الفقرة (ج) تحديداً، محو البيانات بعد الانتهاء من مدة المعالجة أو تسليمها للشخص المسؤول.

ترى الباحثة، أن المشرع الأردني عندما أعطى المعالج هذا الخيار لم يحدد الآلية ولا مصير النسخ الاحتياط من البيانات، أو النسخ التي تم نقلها لمتلقٍ داخلي أو خارجي، وذلك لما لهذا الحق من أهمية في تحقيق هذا المبدأ، وحماية خصوصية الأفراد.

6. مبدأ السرية والنزاهة:

أكد المشرع الأردني في المادة السابعة/هـ، و، ز من قانون حماية البيانات الشخصية على ضرورة الالتزام بالسرية عند معالجة البيانات، وحمايتها من الوصول الغير مصرح به أو استخدامها بطرق تتسبب في الأذى أو الضرر للأفراد، وقد حددت المادة الثانية عشر/د، والمادة الثالثة عشر، من ذات القانون، أن المسؤول والمعالج هما المسؤولان عن تحقيق هذا المبدأ.

وباستقراء نصوص المواد المذكورة، نجد أن المشرع الأردني توافق مع التشريع المقارن في المادة الخامسة/f/1، الذي جعل من مسؤوليات المتحكم ضمان مستوى من السرية، والنزاهة يكفل أمن المعلومات وحمايتها من الانتهاك، مع ملاحظة، ترك قرار تحديد الإجراء المتخذ، من أجل ضمان ذلك إلى كلٍ من المتحكم في التشريع الأوروبي، وإلى المسؤول في التشريع الأردني، ليختار الإجراء الأنسب لطبيعة ونوع البيانات لحمايتها من المخاطر المحتملة.

وبالنتيجة نجد أن التشريع الأردني قد وافق التشريع المقارن، في استنادهما إلى مبدأ السرية والنزاهة، من خلال تأكيد ضرورة حماية البيانات الشخصية، وحفظ سرية الأفراد من الاستغلال، أو المعالجة الغير قانونية.

7. مبدأ الموافقة:

أعطى المشرع الأردني للشخص المعني الحق بالموافقة المسبقة على معالجة جميع بياناته، فكما وضحت المادة الرابعة/أ، والمادة الثانية عشر، أن على المعالج إعلامه بأنه ينوي البدء بالمعالجة، ليتسنى له خيار الموافقة أو الرفض على هذه العملية، وكذلك وضحت المادة(5/أ) من قانون حماية البيانات الشخصية الشروط التي يجب أن تستند إليها الموافقة، لتكون صحيحة وقانونية تسمح بإجراء معالجة مشروعة، وكانت كما يلي:

1. اشترط أن تكون الموافقة واضحة ومحددة حيث أنه من البداية على معالج البيانات، ووفقا للحقوق التي فرضها المشرع للشخص المعني، أن يخبره بشكل واضح وصريح بشروعه في معالجة بياناته وبالغرض من هذه المعالجة، ليكون للفرد بالتالي الحق في رفضها أو قبولها، بطريقة صريحة ودون إكراه، سواء خطياً أو إلكترونيا.
2. أن تكون الموافقة تبدأ مع المعالجة وتنتهي عند الانتهاء منها، ففي حال انتهى المعالج من الغرض الذي جمعت البيانات من أجله، وتمت الموافقة بناءً عليه، فعلى المعالج ألا يقوم باستخدام البيانات مجدداً لغرض أخر استنادا للموافقة السابقة.
3. اشترط المشرع في طلب الموافقة أن يكون مفهوماً للشخص المعني من حيث اللغة فلا تكون الكلمات مبهمة، تحمل أكثر من معنى، وللشخص المعني حرية الوصول إليه وسحبها.
4. لم ينسى المشرع فاقد الأهلية، أو الصبي صغير السن ناقص الأهلية، كونهم أشخاص لا يملكون القدرة في التعبير الصحيح عن الإرادة، أو الأهلية لإجراء تصرفات قانونية، فاشترط موافقة الولي، أو الوصي، كلّ حسب حالته.
5. لم يتطرق إلى الموافقة على المعالجة الآلية والتنميط، بالرغم من أنهم أكثر أنواع المعالجة استخداما سواء في مجال التجارة الإلكترونية أو في الإعلانات التجارية، أو حتى في المجالات السياسية.
6. ولم يحدد متى وفي أي مرحلة يمكن سحب الموفقة، على عكس التشريع الأوروبي، الذي سمح بشكل صريح في القانون على سحبها بأي وقت من المعالجة، وحدد أن تتوقف المعالجة عن الحد الذي وصلت عنده.

ورغبة من المشرع بزيادة الحماية على البيانات الشخصية، وكونه لا يسمح لأيّ كان بالاطلاع على بيانات الآخر، دون علمه، وموافقته، فقد نص بصريح العبارة في المادة الخامسة البند ب على الالتفات عن الموافقة، في حال قام المعالج بالحصول عليها بطرق احتيالية، أو طرق مضللة للشخص المعني، أو في حال تم استعمال البيانات بطريقة مختلفة تماما، عما تمت الموافقة عليه، كأن يكون المعالج أخذ الموافقة لغرض معين، ثم قام بعمل معالجة لغرض آخر، غير معلوم للشخص المعني، وفي هذه الحالة فإن المعالج يعرض نفسه للمساءلة القانونية، تبعا لشروط المعالجة المنصوص عليه في المادة السابعة من هذا القانون، والتي كان عليه الالتزام بها.

وقد وضع المشرع على المادة الخامسة، بنود المادة السادسة كاستثناء، يقضي بمشروعية المعالجة حتى لو أنها جاءت دون الحصول على الموافقة المسبقة، إلا أنه ومن وجهة نظر الباحثة هذه المادة أثقلت القاعدة القانونية بكثير من الاستثناءات، والتي جردتها من مضمونها، فحتى لو أن الهدف من المعالجة المصلحة العامة، كان على المشرع أن يراعي التوازن، بينها وبين حق صاحب البيانات بحمايتها بوضع قيود أكثر على هذه الاستثناءات، طبعا هذا في حال كان ذلك لا يتم لدواعي أمنية، كالجمع لأغراضٍ إحصائية، أو لأغراض البحث العلمي، و التاريخي، أو لأغراض الرعاية الصحية مثلاً، وخاصة أن المشرع هنا لم يذكر موقفه من نشر هذه البيانات دون موافقة الشخص المعني، فهل هو مصرح بها أم لا، كونها أيضا قد تكون بيانات حساسة؟

أحكام التشريع الأردني بخصوص الموافقة مستقاة من التشريع المقارن، والذي وضحت المادة السابعة منه شروط الموافقة، إلا أن المشرع الأوروبي كان أكثر دقة، في تحديد مصير المعالجة السابقة على سحب الموافقة، وهذا الحق لم يتطرق المشرع الأردني لذكر تفاصيل آليته وما يترتب عليها، وإنما فقط اقتصر على إقراره في المادة الرابعة من التشريع الأردني.

وفي المادة الثامنة من التشريع المقارن قام المشرع بذكر شروط خاصة بموافقة الطفل، وجعل معالجة بياناته قانونية وصحيحة، دون موافقة وليه في حال كان الطفل قد أتم السادسة عشر، وسمح من خلال استثناء في المادة نفسها للدول الأعضاء بالاتحاد الأوروبي بإجراء هذه المعالجة، ودون موافقة الولي أو الوصي لبيانات من هم دون ذلك بشرط ألا يقل سنهم عن ثلاثة عشر سنه.

من وجهة نظر الباحثة، أرى أن المشرع الأردني قد أصاب برفع السن القانوني للطفل، عندما جعل موافقة وليه، أو الوصي عليه شرطا لمعالجة بياناته؛ حتى الثامنة عشر من عمره، كون أهليته لإجراء التصرفات القانونية لا تزال غير كاملة، وكون إدراكه لخطورة مشاركة بياناته، مع جهات غير موثوقة، قد يعرض حياته أو حياة أسرته للخطر.

في المادة التاسعة من التشريع المقارن، ذكر المشرع في البند الأول أن البيانات الشخصية الحساسة، لا يجوز التطرق لمعالجتها، لكنه لم يترك هذا النص على إطلاقه، بل وضع عليه استثناءات في البند الثاني وهذه الاستثناءات تقابل الاستثناءات المذكورة في المادة السادسة/ أ من التشريع الأردني، لكن التشريع الأردني لم يفرق هنا بين نوعية البيانات، كما فعل التشريع المقارن الذي جعلها للحساسة منها فقط نظراً لخصوصيتها.

من وجهة نظر الباحثة، كان على المشرع الأردني أن يولي اهتماما أكثر في للبيانات الحساسة، ويشرع نصوصاً تميزها بالحماية اللازمة للمحافظة على خصوصية أصحابها، فهو في التشريع إجمالا لم يفرق في الحماية بينها وبين الحساسة ولم يميزها عنها، إلا في المادة الثانية، والتي تتضمن التعريف فقط.

8. مبدأ الأمن والتلاؤم:

يقوم هذا المبدأ على أن يتم التأكد من قِبل المسؤول، وقَبل نقل البيانات، من وجود نظام حماية مماثل للذي نص عليه قانون حماية البيانات الشخصية، لدى الجهات التي يُراد نقل البيانات إليها، قبل مشاركة البيانات مع جهات داخلية أو خارجية، وهذا لضمان الحماية للبيانات الشخصية للأفراد، مع العلم أن نقل البيانات قد يكون من قِبل الشخص المعني، كاستعمال لحقه، أو من قِبل مسؤول البيانات. (المادة 15،14،4 من قانون حماية البيانات الشخصية الأردني،2023)

المادة الرابعة والأربعون من GDPR وضح المشرع الأوروبي القواعد العامة لنقل البيانات وكان أكثر صرامة من المشرع الأردني، حيث أنه لم يسمح بنقل بيانات الأفراد الخاضعين قانونيا للاتحاد الأوروبي سواء داخل الإتحاد أو خارجه، حتى لو كانت الشركات التي تعالج بياناتهم وتريد نقلها أجنبية الجنسية، وتقع خارج النطاق الجغرافي للاتحاد، دون التأكد من امتثالها بمستوى من الحماية يتلاءم مع ما يوفره ال (GDPR) لبيانات الأفراد المعنيين، أما إذا كانت بمستوى حماية متلائم مع التشريع فإن عملية النقل تتم بدون إذن بذلك من المفوضية الأوروبية.

ولم يكتفي المشرع الأوروبي بذلك، بل نص في المادة نفسها على ضرورة إجراء فحص ملائمة من قبل المفوضية الأوروبية للتأكد من امتثال المتلقي للقانون، يستند هذا الفحص إلى التأكد من معايير سيادة القانون، ومراعاة الحريات، وحقوق الإنسان، والاستقرار السياسي،

والقضائي، والتزاماتها الدولية خارج دول الإتحاد، لدى البلد المتلقي أو المنظمة الدولية المعنية، قبل إجراء نقل البيانات، كما أن هذا الفحص الدوري تجريه المفوضية بمعدل مرة كل أربع سنوات ع الأقل، وعلى هذا الأساس يمكن للمفوضية أن تقرر تغير، أو تعديل، أو تعليق، قرار التبادل، وهذا ما لم يأت المشرع الأردني على ذكره في التشريع الأردني.

ترى الباحثة أن التشريع الأردني لم يتوسع في شرح عملية نقل البيانات، ولا في آلية هذه العملية، كما فعل التشريع المقارن، كما أنه لم يوضح، إذا ما على المسؤول إخبار الشخص المعني برغبته بنقل بياناته، سواء إلى متلقي داخلي أو خارجي، أو إعلامه فيما إذا كان لدى المتلقي مستوى متكافئ من الحماية التي يوفرها التشريع الأردني أم لا، أما التشريع المقارن أولى عناية كبيرة لهذه العملية كونها ليست فقط تقوم بحماية بيانات الشخص المعني، بل إن مشاركة بيانات مواطني الدولة خارجيا قد يؤثر على الأمن القومي في حال اختراقها، وكون المشرع الأردني أيضا في عملية نقل البيانات لم يفرق بين البيانات الشخصية، والبيانات الحساسة، مما يعني أن المادة الخامسة عشر تنطبق على النوعيين من البيانات، هذا يظهر مدى خطورة مشاركتها مع دول أو منظمات خارجية تقل في مستوى الحماية عن المستوى الذي وفره التشريع الأردني، وبالتالي فإن عملية النقل هذه قد تشكل قاعدة بيانات يستند عليها المتربصون لأمن الدولة، ومثيرو الفتن.

وفي النتيجة ترى الباحثة، أن قانون حماية البيانات الشخصية يتبع بشكل عام المبادئ الأساسية التي حددها GDPR، مع بعض التفاوت في تفاصيل الحقوق والآليات القانونية، ومع ذلك كلا القانونين يركزان على حماية حقوق الأفراد في خصوصية بياناتهم، ويؤكدان على ضرورة الشفافية، والامتثال للمبادئ القانونية المتعلقة بحماية البيانات الشخصية، إن هذه المبادئ تعمل متضافرة متكاملة على تعزيز حماية البيانات الشخصية وبالتالي تعزيز الثقة في المعاملات الإلكترونية والاقتصاد الرقمي.

الفرع الثاني: مقارنة الحقوق التي منحها القانون الأردني للأفراد مع التشريع المقارن

قام المشرع الأردني بالنص في المادة الرابعة من قانون حماية البيانات الشخصية على ثمانية حقوق كفلها للفرد؛ من أجل ضمان حماية بياناته الشخصية، وكانت هذه الحقوق مماثلة للحقوق التي جاء بها التشريع المقارن في مواده من (15–20)، إلا أن هذه الحقوق كانت غير واضحة، وغير محددة كما يجب، وإن الاستثناءات الواردة عليها أدت إلى تفريغ هذه القاعدة العامة من مضمونها مما جعلها حقوقًا مقيدة، وذلك بالتفصيل التالي:

1- حق الوصول:

وقد نصت عليه المادة الرابعة/أ/1 وهي تقابل المادة الخامسة عشر منGDPR، وكلاهما يمنحان الفرد الحق في تقديم طلب للمسؤول للوصول إلى بياناته الشخصية، والاطلاع عليها، إلا أن المشرع الأردني لم يحدد المدة التي على المسؤول أن يجيب فيها طلب الشخص المعني، ولم يذكر المدة التي يجوز فيها للمسؤول الاحتفاظ في بيانات الفرد الشخصية، بعد الانتهاء منها، ولم يحدد ما إذا كان هذا الطلب يستلزم إجراءات معينة، و إنما ذكر في المادة الرابعة/ج أن ممارسة الشخص المعني لجميع حقوقه المذكورة في الفقرة الرابعة/ب تكون مجانية ولا ترتب أي التزام تعاقدي، وهذا يتوافق مع التشريع المقارن، ولكنه قيد ذلك بشرط عدم الإخلال بحقوق المسؤول ، دون ذكر ما هي حقوق المسؤول؟؟؟؟ أو كيف يكون الإخلال بحقوقه؟؟؟؟ وفي حال تم الإخلال كم ستكون الرسوم، هل هي رسوم تتناسب مع مقدار الإخلال أم أنها رسوم محددة بمقدر معين؟؟؟

كما ذكر المشرع الأردني بنفس النص الحق بالعلم إلا أنه وعندما وضح الأمور التي على المسؤول إعلام الشخص المعني بها، لم ينص على إعلامه على نقل بياناته في حال كان مستوى الملائمة لا يتوافق مع ما هو متوفر في التشريع الأردني. (المادة 15من قانون حماية البيانات الشخصية،2023)

نرى أن التشريع الأوروبي كان أكثر تفصيلا، من حيث ذكر تفاصيل حول هذا الطلب كأن يكون برسم يكافئ التكاليف الإدارية لاستخراجه في حال كان المطلوب نسخة ورقية، وأن يقدم المراقب نسخه إلكترونية مجانية في حال تم تقديم الطلب إلكترونيا من الشخص المعني، وأن يكون بصيغة سهلة الوصول ومفهومة، وأن يتم إعلام الفرد بالجهة التي سيتم تزويدها بالبيانات سواء كانت داخلية أو خارجية، وفي حال كانت خارجية إعلامه بالضمانات التي تكفل حماية بياناته لدى الطرف الثالث، وهذا يتناسب مع مبدأ التلاؤم، وأخيرا إخباره بالمعالجة الآلية في حال حدوثها وبالأثر المترتب عليها. (GDPR,Article15)

2-حق سحب الموافقة:

عند الشروع في معالجة بيانات الشخص المعني تطلب بداية منه الموافقة على جمع بياناته، مع ذكر الغرض من جمعها ومعالجتها من قِبل المعالج، وهنا له الحق في الرفض أو الموافقة على ذلك، وبعد إعطاء الموافقة أعطى المشرع الأردني للفرد الحق في تقديم طلب سحبها للمسؤول، ولكنه لم يقم بتوضيح متى يجوز سحب الموافقة؟؟ ولم يحدد متى يكون هذا الطلب مقبولاً أو غير مقبول.

أما التشريع الأوروبي فكان واضحاً وصريحاً في هذا الخصوص، حيث أنه سمح بسحب الموافقة من قِبل الشخص المعني في أي وقت، بشرط ألا يكون هناك مصلحة عامة تفوق في الأهمية على مصلحة مقدم الطلب. (GDPR,2018, Article7)

3- الحق بالتصحيح أو التعديل أو الإضافة أو التحديث للبيانات:

هذا الحق يمكن الشخص المعني بأن يطلب من المسؤول تحديث بياناته وتصحيحها لتكون دقيقة، أو تعديلها، والإضافة عليها لتكون كاملة، وهذا يتوافق مع التشريع الأوروبي، وهنا ينسجم هذا الحق مع مبدأ الدقة الذي يتطلب أن تكون المعلومات صحيحة، ودقيقة، ومحدثة، وكاملة. (المادة4/ب/3 من القانون حماية البيانات الشخصية،2023) (GDPR,2018,Article16)

4- تخصيص المعالجة في نطاق محدد:

وهذا الحق الذي نص عليه المشرع الأردني في المادة الرابعة/ب/4 من قانون حماية البيانات الشخصية هو حق يقتضي من المعالج تحديد نوع البيانات التي يتم جمعها بحسب الهدف من المعالجة، وهذا أيضا حق نص عليه ال GDPR في مادته الخامسة إلا أنه يختلف معه في المضمون، حيث أن حالات تقيد المعالجة في التشريع المقارن وكما ذكرنا في الفصل السابق، أوسع منها في التشريع الأردني، فقد شملت تقيد المعالجة بالمعنى المذكور في التشريع الأردني، إذا كانت المعالجة غير دقيقة، أو تم جمعها بطريقة مخالفة للقانون، وتقيداً آخر لحين الفصل في طلب المحو، وهذا التقيد لم يعرفه المشرع الأردني. (الجعافرة،2022)

ترى الباحثة، إن تقيد المعالجة، يتفق مع مبدأ تقليل البيانات من جهة، ومبدأ الغاية المحددة من جهة أخرى، بحيث لا يتم جمع بيانات إلا الضرورية للمعالجة، والمتعلقة بها، والمحددة وعند الانتهاء من المعالجة لا يسمح بالاحتفاظ في البيانات، لانتهاء الغرض من جمعها، مما يضمن في نهاية الأمر دقة البيانات، وتحديثها بشكل دوري عند الحاجة لها، وعدم جمع ما هو أكثر من اللازم لتحقيق الحماية للبيانات، إلا أنه وفق التشريع الأوروبي أكثر تحقيقاً لهذا المبدأ، وأكثر توافقاً مع المنطق القانوني، فلو مثلا قدم الشخص المعني طلب

لمحو بياناته، فأجدى أن يتم وقف معالجة البيانات لحين الفصل في الطلب مالم تكن المعالجة تتعلق بالمصلحة العامة، أو لأسباب قانونية مثلا .

5- حق المحو:

نص المشرع الأردني على حق المحو أو ما يعرف بحق النسيان في المادة الرابعة/ب/5، وبين تفاصيل وإجراءات هذا الحق في المادة العاشرة من قانون البيانات الشخصية، بأن جعله حق للشخص المعني أو الوحدة التنظيمية، وهنا المسؤول هو من يقوم باتخاذ التدابير اللازمة حال الموافقة على الطلب، ويقدم هذا الطلب عندما لا يكون هناك غرض أساسي للاحتفاظ في البيانات، أو عندما تنتهي المعالجة، أو عندما يسحب الشخص المعني موافقته، أو يعترض على الاحتفاظ بها لعدم وجود أسباب قانونية أو عقدية وهذا يتوافق مع التشريع الأوروبي (الجعافرة،2022)(GDPR,2018, Article 17)

لكن من الجهة التي يقدم الطلب إليها؟ حدد القانون الأردني في المادة الحادية عشر/4 منه أن المراقب هو الشخص المسؤول عن وضع التعليمات الخاصة بشكاوى محو البيانات وإتاحة تقديم الشكاوى للشخص المعني، ولم يذكر المشرع تلقي الشكاوى من بين تلك المهام، وكون هذا القانون موجه للشخص العادي، ويهدف لحماية بياناته، كان من الأفضل أن يقوم المشرع ببسط الإجراءات وجعل العبارات أكثر وضوحاً ويسراً، ولا تحمل إلا معنىً واحداً واضحاً، لتكون أيسر فهما على الشخص العادي، كما فعل التشريع المقارن عندما جعلها من مهام المراقب التي عليه أن يمتثل للطلب فور التحقق توافق أسبابه مع نص القانون.(GDPR, Article 17)

أيضا ترى الباحثة، أن المشرع الأردني ذكر الحالات التي يجوز فيها تقديم الطلب، لكن أغفل بعض الأمور المتعلقة بهذا الحق، وهي مهمة بقدر أهميته، مثل أنه لم يحدد المدة بين تقديم الطلب وإجابته، ولم يحدد ما إذا يمكن للشخص المعني أن يطلب محو بياناته المتعلقة بسجله الجنائي أم لا ؟، كونه اعتبر هذه البيانات من البيانات الحساسة في هذا القانون، لم يذكر المشرع أيضا ما العمل في حال قوبِل الطلب بالرفض من قبل المراقب؟ فهل يحق للشخص تقديم شكوى على الرفض؟ أم هل يحق له طلب قيد المعالجة حتى الانتهاء من النظر في طلب المحو، أسوة بما فعل المشرع الأوروبي حين أعطى الشخص المعني الحق في طلب قيد المعالجة حتى يتم الفصل في طلبه، وفي حال رفض الطلب هل يقدم الرفض معللاً بأسبابه القانونية؟

ولم يوضح المشرع الأردني إذا ما أراد الشخص المعني التظلم من هذا القرار إلى أي جهة يتوجه؟

في التشريعين، لم يتم توضيح مصير أنظمة النسخ الاحتياطي في حال تم قبول طلب محو البيانات، ولا الإجراءات المترتبة على ذلك في حال امتد التنفيذ بالفعل إلى نسخ الاحتياط، ولم تُوَضح نطاق البيانات المطلوب محوها، فهل ينطبق عندما يكون من نشر البيانات هو نفسه الشخص المعني فقط؟ أم يحق طلب محو بيانات منشورة من قبل الغير؟ مما سبق يتبين أن آلية تطبيق الحق وتنفيذه في كلا التشريعين لا تزال مبهمة ويعوزها الكثير من البسط والتوضيح. (مشعل،2017)

كما أن السابعة عشر/2 من التشريع المقارن، نصت على أن لصاحب البيانات الحق في طلب حذف بياناته، في حال كان المراقب هو من قام بنشرها للعامة، ووضحت أن على المراقب القيام بذلك فوراً، وبعد إعلام بقية المراقبين بضرورة حذف كل النسخ والروابط لهذه البيانات، وهذه الحالة لم يتطرق المشرع الى ذكرها أو النص عليها في التشريع الأردني.

المادة (10/ب) من التشريع الأردني والتي نصت على عدم جوز محو البيانات التي ذكرتها المادة (6) من ذات القانون لتصبح بذلك هذه الاستثناءات مطبقة على حالة معالجة البيانات من دون موافقة مسبقة من الشخص المعني، وحالة عدم السماح له أيضا بتقديم طلب لمحوها، استثناءات التشريع المقارن وافقت استثناءات التشريع الأردني إلا أنها أضافت استثناء التعبير عن الرأي والذي ترك المشرع الأردني أمره دون مناقشة هنا(GDPR,Article17/3) .

ومن رأي الباحثة إن هذه الاستثناءات ضرورية لضمان عدم مخالفة النظام العام، أو الآداب العامة مما يؤدي إلى بلبلة في حماية الأمن القومي لكن يتوجب العمل على ضمان التوازن فيما بين الحق في المحو والاستثناءات، وكذلك لابد من تحديد ألية تمكين الشخص المعني من حقه، والجهة الواجب التظلم لها.

6-حق الاعتراض:

هذا الحق يسمح للشخص المعني أن يتقدم بطلب للمسؤول بالاعتراض على جمع بياناته ومعالجتها، لكنه ليس حقاً مطلقا بل وضع عليه المشرع الأردني قيوداً لابد من توفرها حتى يستطيع الشخص المعني أن يستخدمه، لم يذكر المشرع الأردني أنه في حالة قبول الاعتراض على البيانات، كم ستكون مدة قيد المعالجة حتى البث في الطلب؟ وهل سيتم قيد المعالجة، ثم يكون مصير البيانات المحو في حال كان الرد على الطلب إيجابياً؟ في حال تم قيد المعالجة ولكن تبين أنه يجب استئنافها لسببٍ ما فهل سيتم تبليغ صاحب البيانات حال البدء بالمعالجة أو ما هو الإجراء المتخذ في حال رفع القيد عن المعالجة؟ هذه أمور لم يتم التطرق لها، ولم يوضحها المشرع، مما جعل هذا الحق ينقصه التحليل والتفسير.

لم يتحدث المشرع الأردني عن حق الاعتراض على المعالجة الآلية، هو بالأصل لم يتطرق لذكرها في التشريع ككل، مع أنه ومن وجهة نظر الباحثة كان من الأفضل وضع ضوابط وقيود على هذا النوع من المعالجة نظراً لانتشارها، وكثرة ما قد ينجم عنها من جمع، ومعالجة، وتخزين لبيانات قد لا يعرف مصيرها، وكذلك الأمر بالنسبة للتنميط الذي لم يأتِ المشرع الأردني على ذكره.

أما التشريع المقارن، والذي كان أكثر وضوحا وتفسيراً للحق، حيث أنه نص على أن يقدم الطلب إلى المراقب، وإن الاعتراض يكون جائز بأي وقت، وإضافة إلى حق الشخص المعني بالاعتراض على المعالجة غير المشروعة، والغير قانونية، فإنه يمكنه أيضًا الاعتراض على المعالجة الآلية، والتنميط، واستخدام بياناته في البريد الدعائي، وكذلك سمح للشخص المعني أن يتقدم في الاعتراض على معالجة بياناته للأغراض العلمية، أو التاريخية، أو الإحصائية، بشرط أن لا تكون المعالجة لغرض المصلحة العامة، وفرض قيد المعالجة فوراً على المراقب، في حال تبين أن أسباب الاعتراض مشروعة، ومقنعة، كما أنه في وضح كيفية تقديم الطلب، بأن سمح بالاعتراض بشكل آلي بالإضافة إلى الشكل التقليدي، وحدد موعداً للرد على طلب الاعتراض في حال رفضه، بأن تكون بأول تواصل مع الشخص المعني حول هذا الحق، واشترط حينها تسبيب قرار الرفض بصورة مفهومة وواضحة، ومنفصلة عن بقية المعلومات، كما أن المشرع الأوروبي أضفى الشرعية على عملية المعالجة التي تمت قبل الاعتراض، وهذا كله لم يتطرق المشرع الأردني لذكره مما جعل أمر الإجابة عن هذه الاستفسارات مبهمة، وغير واضحة.(GDPR,2018, Article21)

ترى الباحثة أن التشريع المقارن، كان أكثر حرصاً على بسط هذا الحق من كل جوانبه، وأن أفضل ما جاء به، هو أنه مكن الشخص المعني من السيطرة على بياناته، وخاصة حمايتها من المعالجة الآلية، والتنميط الذي قد يؤثر هذا الأخير في الحكم على الفرد، وصورته الاجتماعية.

7- الحق في نقل البيانات:

فرض المشرع الحق للشخص المعني بطلب نقل بياناته، من مسؤول لآخر، وكذلك أعطى الحق للمسؤول بنقل البيانات إلى متلقٍ داخلي أو خارجي ونظم ذلك الحق في المادتين الرابعة، عشر والخامسة عشر، وذلك كما يلي:

1. داخليا: ويكون بين المسؤول وأي شخص آخر، وهذا التبادل اشترط المشرع فيه الموافقة المسبقة، من الشخص المعني قبل القيام بنقل البيانات، وبخلاف ذلك يعد هذا النقل غير قانوني، وبعد أخذ الموافقة يجب التأكد من أن هناك مصلحة مشروعه يحققها النقل لكل من المتلقي والمسؤول، والتأكد من علم صاحب البيانات بالجهة التي نقلت البيانات إليها، وعلمه فيما سوف تستخدم هذه

البيانات، والتأكد من أن لا يكون الغرض من النقل لاستخدامها بالتسويق أو خدمات أخرى دون موافقة صاحب البيانات المسبقة.(المادة 14 من قانون حماية البيانات الشخصية' 2023)

2. خارجيا: اشترط المشرع أن يكون النقل بعد تأكد من أن البيانات المنقولة سوف تتمتع بنفس مستوى الحماية التي كانت موفرة لها داخل المملكة، وهذا يتوافق مع مبدأ التلاؤم.

وباستقراء نصوص المواد السابقة نجد أن المشرع لم يترك هذه القاعدة على إطلاقها، بل وضع عليها العديد من الاستثناءات، التي جعلت نقل البيانات جائزًا إلى جهات خارجية مختلفة، مستثناة من التحقق من مستوى الحماية المتبع لدى المتلقي.

من رأي الباحثة، أن هذه الاستثناءات بالرغم من ضرورةِ تبادل البيانات المتعلقة بها، إلا أنها تشكل خطراً كبيراً على البيانات الشخصية مما قد يعرضها للانتهاك، ويعرض أصحابها لخطر اختراق خصوصيتهم، وما ينجم عن ذلك من تبعات، كان حريٌ بالمشرع أن يبقي على شرط التأكد من ملائمة مستوى الحماية الداخلي مع الخارجي نظراً لحساسية البيانات التي نصت عليها الاستثناءات المذكورة في المادة الخامسة عشر، على غرار التشريع المقارن، والذي لا يسمح بنقل البيانات إلى متلقي خارجي قبل التأكد من أن حماية البيانات فيها تخضع لقيود وضوابط صارمة لضمان حقوق الأفراد.

وهذا الحق نصت عليه المادة العشرون من التشريع المقارن، إلا أنها وضحت آلية نقل هذه البيانات، بأن يكون من خلال طلب يقدم بوسائل آلية إلى المراقب، بشرط أن يكون الهدف من نقل البيانات تفعيل عقد، كما اشترطت أن تكون البيانات التي تم جمعها تستند في جمعها لأساس قانوني ، أو عقد، وهنا أعطى المشرع حق نقل البيانات للشخص المعني دون تدخل من المراقب، إلا في حالة ما إذا كانت عملية المعالجة تتم تنفيذاً للمصلحة العامة، أو ممارسة المراقب لسلطاته، كما فعل المشرع الأردني بأن أعطى للمسؤول الحق بذلك سنداً للاستثناء الوارد في المادة الرابعة عشر/ج، والتي نصت على السماح بنقل المعلومات فيما بين الجهات العامة دون أن يستند ذلك إلى موافقة الشخص المعني، وبغض النظر عن ما جاء في البندين (أ/ب) من ذات.

المشرع الاوروبي، أوكل مهمة تنفيذ الحق إلى المراقب، وجعل واجبه تسهيل عملية نقل البيانات وإيصالها بشكل قابل للقراءة الآلية، والتشغيل البيني، المشرع الأوروبي هدف من هذا الحق أن يجعل الشخص المعني متحكما في بياناته بشكل مطلق، حيث لا يكون المراقب هنا خاضعا للامتثال لأي جهة، بل إنه يكون فقط مقيداً لطلب الشخص المعني، ويتصرف على أساسه.

باستقراء نص المادة الرابعة عشر/ج نجد أنها سلبت روح الحق الذي نصت عليه المادة الرابعة من التشريع الأردني، بأن جعلت الجهات العامة قادرة على تبادل البيانات، حتى لو لم يتوفر علم صاحب البيانات بذلك النقل، أو الغرض منه، ودون الموافقة المسبقة، وفي البند هـ أكد المشرع على أن المسائلة القانونية عن أمن هذه البيانات تكون في مواجهة كل من المعالج والمسؤول، والمتلقي، إلا أن المشرعان الاردني والأوروبي اتفقا على ضرورة التأكد من توافر مستوى حماية مماثلة لدى الشخص المتلقي، في حال نقل البيانات إلى متلقٍ خارجي.(GDPR,2018, Article 20,44-50)

من رأي الباحثة هذه الاستثناءات الكثيرة جردت الحق من مضمونه، كما أن السماح بنقل البيانات إلى الخارج، ودون وجود شرط الحماية الملائمة للحماية التي يوفرها التشريع الأردني للبيانات، ما هو إلا خروج صارخ على الهدف الذي جاء هذا التشريع ساعياً إليه.

8- حق العلم بالإخلال بأمن وسلامة البيانات:

يمكن هذا الحق الشخص المعني من معرفة أن بياناته تم التعدي عليها، أو الوصول إليها، أو تم عليها أي إجراء غير مصرح به بموجب عقد، أو قانون، وبذلك يتمكن من اتخاذ الإجراء القانوني المناسب بحق الشخص المتسبب بالضرر، وقد نصت المادة العشرون من التشريع الأردني، أن على المسؤول تبليغ الشخص المعني بهذا التعدي خلال أربع وعشرون ساعة من اكتشافه، وتوجيهه نحو الإجراءات

الواجب اتخاذها، وكذلك عليه إخبار وحدة حماية البيانات خلال اثنان وسبعون ساعة، وتزويدها بمعلومات حول مصدر الانتهاك، وآليته، وأسماء الأشخاص الذين جرى التعدي على بياناتهم.

أما التشريع المقارن فقد نصت المادة الرابعة والثلاثون منه على ضرورة إبلاغ الشخص المعني بأسرع وقت ممكن، وبشكل واضح وشفاف، وجعل هذا الإبلاغ غير إلزامي في حالات مستثناة، وذلك إذا كانت هناك تدابير فعالة تم اتخاذها لتعطيل أي آثار سلبية للخرق، أو إذا كان الإبلاغ قد يتسبب في تعطيل التحقيقات الأمنية أو القانونية. أما المادة الثالثة والثلاثون فقد توافقت مع التشريع الأردني من حيث أن يتم إعلام الهيئة المشرفة على البيانات خلال اثنان وسبعون ساعة من حدوث الخرق للبيانات، وفي حال التأخر عن هذه المدة لابد من تبرير سبب التأخير.

من رأي الباحثة هذا الحق مفيد للشخص المعني حيث أنه جزء من تأكيد القانون على حقوق الأفراد في حماية بياناتهم الشخصية، ومفيد لأنه يضمن امتثال الشخص المسؤول للقوانين الواردة في هذا التشريع، ولكن مدة الاثنان وسبعون ساعة لإبلاغ الوحدة بالتعدي على البيانات، هي مدة طويلة نسبياً، فقد يكون الانتهاك للبيانات يحمل خطراً كبيراً على خصوصية الشخص المعني، ويتسبب بضرر جسيم، مما يتطلب سرعة في التصرف، وإجراء ما يلزم من تدابير لتخفيف الضرر المحتمل، ولمنع تفاقم التبعات.

وبالنتيجة ترى الباحثة، أن جميع الحقوق المنصوص عليها في المادة الرابعة من التشريع الأردني، بحاجة إلى تبسيط وتوضيح إلى مستوى فهم وإدراك الشخص العادي، ليس القانوني فقط لأنها تمثلُ حقوقاً لأفرادٍ عاديين لا يتوقع منهم أن يقوموا بالبحث عن القصد القانوني للمشرع، لفهم حقوقهم ومعرفة ما عليهم من واجبات، كما أنه حتى العاملين في المجال القانوني من قضاة، ومحامين قد يقعون بحيرة في التأويل، نظراً لعدم حسم الأمور من قِبل المشرع، فكانت هذه المادة تحمل معها كثيراً من الحقوق، وعوزاً للتفسير.

إن هذه المادة من وجهة نظر الباحثة، بحاجة لتعليمات إيضاحية لتنظم الحقوق الواردة فيها بشكل لا يعتريه اللُبس أو الغموض، فهي كما وضحت الباحثة في هذا المطلب كانت مجرد فرض لحقوق دون بيان آلية تمكين الأشخاص من هذه الحقوق، أو بيان كيفية الاعتراض على انتهاكها، وهذا يقف عقبة كبيرة أمام حماية البيانات من جهة، وأمام الموثوقية، والثقة في الاقتصاد الرقمي من جهة أخرى.

في النهاية، نرى أن جميع الحقوق يتم إغفالها، في حال كان الغرض من المعالجة يقع ضمن الاستثناءات الواردة في المادة السادسة من قانون حماية البيانات الشخصية، وتهمل أيضا بالنسبة للتشريع الأوروبي؛ في حال كان لدى المراقب أسباب قانونية أقوى من الأسباب التي يستند إليها الشخص المعني في طلبه.

وفي المجمل، يمكن القول، إن قانون حماية البيانات الشخصية الأردني، يتماشى إلى حد بعيد مع متطلبات GDPR، مع بعض التفاوت في التفاصيل المتعلقة في المهلة الزمنية، آلية الحصول على الحق، وطرق الإبلاغ.

المبحث الثاني: آليات تنفيذ التشريع الأردني مقارنة بالأوروبي

كما أسلفت الباحثة سابقاً أن المشرع يضع القانون، ويراقب الامتثال له، ويرتب العقوبة على المخالفين سواء كانت مدنية أم جزائية بهدف الردع، وضمان الامتثال مستقبلاً، لأجل ذلك فرض المشرع الأردني في كل مؤسسة يكون مجال عملها جمع بيانات الأشخاص الطبيعيين، مسؤولا عن البيانات وحدد واجباته والعقوبات المترتبة عليه في حال مخالفة القانون، وألزمته المادة الحادية عشر من القانون بتعين مراقب يسانده في تطبيق الامتثال للقانون من جهة، وليكون ضابط ارتباط بين وحدة معالجة البيانات في وزارة الاقتصاد الرقمي، والجهات الأمنية والقضائية من جهة أخرى، وكذلك المعالج أو المعالجين في حال تعددهم داخل المؤسسة مسؤولون عن الامتثال للقانون في معالجة البيانات.

فما هي ضوابط الامتثال التي فرضها المشرع الأردني مقارنة (GDPR)؟ وما هي عقوبة عدم الامتثال لأحكام القانون؟

لتوضيح ذلك ارتأت الباحثة تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: أشخاص تنفيذ القانون

وضع المشرع الأردني القواعد القانونية لحماية البيانات الشخصية، ولضمان تطبيق القانون الجديد، بالطريقة المرجوةِ؛ التي تضمن تحقيق أهدافه، أوجد المشرع متأثراً بالتشريع الأوروبي، أشخاصاً طبيعيين واعتباريين لتنفيذ القانون، وأفرد لكل منها مهاماً، ومسؤوليات تضمن العمل بشكل متكامل.

الفرع الأول: أشخاص طبيعيين أو اعتباريين

- **مسؤول حماية البيانات:**

هو الشخص الطبيعي أو الاعتباري، الذي يعيين من قبل الجهة أو الكيان المسؤول عن معالجة البيانات الشخصية، ويكلف بمهمة مراقبة الامتثال لأحكام القانون، والسياسات المتعلقة بحماية البيانات الشخصية، وقد يكون تعينه إلزامياً أو اختياريا حسب حجم ونوع المعالجة. تشمل مهام مسؤول حماية البيانات التأكد من تطبيق معاير الأمان، وحماية البيانات، بالإضافة إلى تقديم المشورة للجهة التي يعمل بها حول كيفية الامتثال للقانون ومتابعة الشكاوى المتعلقة بحماية البيانات، كما يتعين عليه التعاون مع الهيئة المعنية بحماية البيانات و الإشراف على التدابير التي تتخذها الجهة في ما يتعلق بمعالجة البيانات الشخصية، لكن القانون لم يحدد آلية وتفاصيل شكل التفاعل بينه وبين الشخص المعني، وخصوصاً إذا ما كان المسؤول خارج المملكة وفقاً للمادة الثانية من القانون، ومن مسؤولياته التبليغ عن أي إخلال بأمن البيانات، وتدريب الموظفين وتوجيههم إلى الطرق المثلى لتحقيق الامتثال والحماية للبيانات الشخصية، في التشريع الأردني لم يشير بشكل صريح أن يكون مسؤول حماية البيانات مستقلاً عن بقية الأنشطة التجارية أو الإدارية داخل المؤسسة.

في التشريع الأوروبي، يطلق مسمى المتحكم DPO على من يحمل مهام المسؤول وفقاً للتشريع الأردني، ويكون تعين المسؤول إجباريا في المؤسسات الكبيرة التي تعالج بيانات حساسة أو بيانات تتعلق بالأطفال، أو عمليات معالجة واسعة النطاق، وتكون مهمته مراقبة الامتثال للقانون، وتدريب الموظفين، ويعتبر نقطة الاتصال الأساسية مع السلطات الإشرافية مثل المفوضية الأوروبية، والأفراد، ويجب المحافظة على استقلاليته في أداء مهامه، فلا يتعرض لتضارب مصالح، وأن لا يتم توجيهه بشأن كيفية أدائها، فيأخذ قراراته فيما يخص بالامتثال لأحكام ال GDPR بحرية تامة.

من وجهة نظر الباحثة فإن مهام المسؤول، ومسؤولياته تتشابه في كل من قانون حماية البيانات الشخصية الأردني والتشريع الأوروبي من حيث مراقبة الامتثال، وحماية البيانات الشخصية، وتختلف من حيث إلزامية التعين والاستقلالية، كون التشريع المقارن أولى أهمية كبيرة لاستقلالية مسؤول حماية البيانات، وحدد بشكل واضح حالات إلزامية تعينه، وبالنتيجة فإن وظيفة مسؤول حماية البيانات، ضرورية لتعزيز ثقافة الخصوصية في المؤسسات، وحماية حقوق الأفراد في بياناتهم الشخصية.

- **معالج البيانات:**

المعالجة تشمل أي عمليه تتعلق بالبيانات الشخصية مثل الجمع، والتخزين، والتحليل، والتعديل، والإفصاح عن البيانات، ومعالج البيانات وفقا لقانون حماية البيانات هو الشخص الطبيعي، أو الاعتباري، أو الهيئة العامة التي تقوم بمعالجه البيانات الشخصية نيابة عن الجهة المسيطرة على البيانات، يقوم معالج البيانات بتنفيذ عمليات معالجه البيانات، بناء على تعليمات صادرة عن الجهة المسيطرة، مثل: شركة مايكروسفت، أمازون وغيرها.

وقد نصت المادة الثانية عشر من قانون حماية البيانات الشخصية، على مسؤوليات معالج البيانات، وتتمثل في معالجة البيانات وفقا للتعليمات التي وضعها المشرع، وضمان الأمان، حيث أن عليه اتخاذ التدابير اللازمة لحماية البيانات الشخصية من الوصول غير المصرح به، أو التعدي عليها، وكذلك التعاون مع الجهة المسيطرة على البيانات، لضمان الامتثال لأحكام القانون، بما في ذلك مراقبة البيانات وحمايتها، والامتناع عن القيام بأي عمل يؤدي إلى خرق أمني يتعلق بالبيانات الشخصية، بالإضافة إلى مسؤوليته عن محو البيانات بعد الانتهاء من معالجتها، والالتزام بمبادئ المعالجة المشروعة التي نصت عليها المادة السابعة من القانون. (المادة 7 و12 من قانون حماية البيانات الشخصية الأردني)

أما التشريع المقارن فقد وسع مهام المعالج، لتشمل كل ما سبق ذكره لدى التشريع الأردني من مهام، بالإضافة أيضاً إلى مهامٍ لم يتطرق لها المشرع الأردني، كالتبليغ عن أي خروقات أو انتهاك للبيانات الشخصية، فقد نصت على ذلك المادة الثالثة والثلاثين من الGDPR، وجعل في المادة السابعة والثلاثين من مهامه مع المراقب تسمية مسؤول أمن حماية البيانات، وفي المادة الثامنة والثلاثين عليه مهمة التأكد من حيادية مسؤول الحماية وعدم تأثير أي جهة عليه، كما حددت المادة الثانية والثلاثون من التشريع المقارن آلية ضمان سلامة وأمن البيانات التي على المعالج العمل عليها، والتي تتمثل في التشفير، واتخاذ التدابير اللازمة.

وبالنتيجة ترى الباحثة من خلال ما تم عرضه، أن المعالج وفق التشريع الأردني، ما هو إلا تابع للجهة المسيطرة على البيانات، ولا يمكنه اتخاذ قرارات بشأن كيفية، أو لماذا يتم معالجة البيانات، بل يجب أن يلتزم بعمله بما يتوافق مع تعليمات الجهة المسيطرة، وفقا للقانون، والتشريعات التابعة له، كما أن التشريع الأردني كان أكثر مرونة من التشريع المقارن، بأن ترك أمر تحديد آلية حماية البيانات إلى المعالج في المادة الثالثة عشر من قانون حماية البيانات الشخصية، والتي يتبين لنا من استقراء النص أن أمر الحفاظ على سرية البيانات هو مسؤولية مشتركة لكل من المعالج، والمسؤول، وترك تحديد الآلية لهم وجعلهم تحت المساءلة القانونية في حال حدوث إخلال بأمن وسلامة المعلومات .

- **المراقب:**

وهو الشخص الطبيعي يعين من قبل المسؤول الذي يعمل كضابط ارتباط، فيما بين وحدة حماية البيانات والمسؤول، ومهمته مراقبة الامتثال للقانون داخل المؤسسات التي تقوم بجمع البيانات، ويلتزم المسؤول إجباريا بتعين المراقب في الحالات التي نص عليها القانون. (المادة 11 من قانون حماية البيانات الشخصية الأردني)

وباستقراء نص المادة الحادية عشر/ ب من قانون حماية البيانات الشخصية، فأن المراقب يكون مسؤولاً عن مراقبة وتطبيق المسؤول لمعايير حمايه البيانات الشخصية، وضمان امتثال المؤسسات لأحكام قانون حمايه البيانات، وهو المسؤول عن وضع تعليمات الطلبات المتعلقة بحقوق الافراد وشكاويهم وفق ما يقتضيه القانون، كما يترتب عليه التأكد من سلامة أنظمة حماية البيانات، بإجراء تقييماتٍ دورية لعمليات معالجة البيانات الشخصية داخل الجهة المسيطرة، عليه أيضا تدريب وتوعية العاملين في الجهة المسيطرة على السياسات، والإجراءات المتعلقة بحماية البيانات، ورغبة من المشرع الاردني بالمحافظة على المرونة، والتطور في مجال حماية البيانات بما يواكب التقدم التكنولوجي جعل المشرع الأردني البند السابع من المادة الحادية عشر/ ب يتيح للأنظمة، والتعليمات التي ستصدر بموجب هذا القانون، إضافة ما تراه من واجبات، ومهام ضرورية تساهم بحماية البيانات الشخصية.

أما التشريع الأوروبي فالمراقب يكون هو الكيان المسؤول عن اتخاذ القرارات بشان المعالجة، أي الجهة المسيطر نفسها، وليس شخصا معينا لمتابعه الامتثال، فتتوحد وفقاً لل GDPR مهام المراقب والمعالج، –والتي سبق ذكرها– ومنها تعيين ضابط مسؤول وحمايه البيانات DPO لمتابعه الامتثال للقانون، وتقديم الدعم له في تنفيذ مهامه، كما وحددت المادة السابعة والثلاثون البند الخامس الكفاءات

الواجب توافرها في المراقب ليتمكن من أداء مهامه، والتي تتلخص في القدرة على فهم المتطلبات القانونية المتعلقة بحماية البيانات، والخبرة العملية في تطبيق هذه القوانين، والمعرفة التقنية حول كيفية تأمين وحماية البيانات، فضلاً عن مهارة التحليل وإدارة الامتثال.

وبالنتيجة، ترى الباحثة أن في ال GDPR المراقب يشار به إلى الجهة المسيطرة على البيانات الشخصية (Data Controller)، وهي الكيان الذي يحدد أغراض ووسائل المعالجة للبيانات الشخصية، لذلك ووفق التشريع الأوروبي المراقب هو الكيان المسؤول عن اتخاذ القرارات بخصوص جمع البيانات واستخدامها، وهو المسؤول عن ضمان الامتثال لأحكام اللائحة.

وبذلك نستخلص أن هناك فرق بين المراقب ومسؤول حماية البيانات DPO ، وهذا الأخير يكون الشخص المعين لمتابعة تطبيق ال GDPR والامتثال، ولكنه لا يتخذ القرارات حول كيفية أو لماذا يتم جمع البيانات، بينما المراقب في التشريع الأردني، فهو الشخص المكلف داخل الجهة المسيطرة على البيانات، بمهمة مراقبة تطبيق القوانين والإجراءات المتعلقة بحماية البيانات الشخصية، بالإضافة إلى أن من وجهة نظر الباحثة كان يتعين على المشرع الأردني أن يذكر المؤهلات العلمية والعملية المطلوب توافرها في المراقب كما فعل التشريع المقارن، لضمان تعين من يمتلك المعرفة القانونية، والخبرة العملية في مجال حماية البيانات الشخصية.

الفرع الثاني: هيئات رقابية أوجدها القانون

- **وِحدة حماية البيانات الشخصية:**

نصت المادة الثامنة عشر من قانون حماية البيانات الشخصية، على مهام وصلاحيات الوحدة، وباستقراء نص المادة يتبين أن هذه الوحدة هي وحدة مستقلة تم إنشاؤها داخل وزارة الاقتصاد الرقمي، لتقوم بمتابعة الامتثال لأحكام القانون، وتعد حلقة وصل بين الأفراد، والجهات الحكومية، أو الخاصة المعنية بحماية البيانات، والمجلس، وتكون مسؤولة عن تنفيذ السياسات، والإجراءات المتعلقة بحماية البيانات الشخصية في المملكة، أما اختصاصات الوحدة، طبقا لنص المادة فكانت كما يلي:

أ. إصدار التوجيهات والتعليمات المتعلقة بحماية البيانات، ومن ثم إرسالها إلى المجلس.

ب. التعامل مع البلاغات والشكاوى المتعلقة بالانتهاكات الخاصة بالبيانات الشخصية، والتحقيق فيها، وإصدار التوصية المناسبة بشأنها للمجلس

ج. التأكد من التزام الجهات المسيطرة والمعالجين بالقانون.

د. إتباع تعليمات المجلس الخاصة بشأن تنظيم سجل والإشراف عليه، يدون فيه مسؤولو ومعالجو ومراقبو حماية البيانات.

هـ. رفع تقرير يدون فيه الأعمال السنوية للوحدة، ورفعه للمجلس بصفته جهة مسؤولة ومشرفة عليها.

من وجهة نظر الباحثة إن وجود الوحدة هو ضمانة لحقوق الأفراد في الخصوصية، من خلال مراقبة امتثال الكيانات التجارية، أو الهيئات الحكومية للقانون، فهي تعمل على تمكين الأفراد من حقوقهم المنصوص عليها في المادة الرابعة من القانون، إضافة إلى استقبال شكاوى الأفراد، بخصوص الانتهاكات أو التهديدات التي تمس أمن بياناتهم، والمحافظة على السرية التامة بخصوص البيانات التي يطلعون عليها، مما يحقق تطبيق مبدأ المساءلة، كما أن الند الأخير من المادة الثامنة عشر كان ضرورياً من أجل ضمان مرونة القانون، ومواكبته لمستجدات التطور التكنولوجي.

وأيضاً من استقراء نص المادة، يتبين أن المشرع لم يحدد من هم موظفو الوحدة وما هي مؤهلاتهم؟ فلم يذكر المشرع التفاصيل الخاصة بتشكيل هذه الوحدة، أو المؤهلات العلمية والعملية للأفراد العاملين فيها، كما وإنه وفقاً لنص المادة الرابعة والعشرون من هذا القانون، يتبين أنه يمكن أن تتضارب الآراء وتتعارض المصالح بين الوحدة والهيئات الحكومية، وخصوصاً أن الوحدة التي تتلقى تعليماتها وآليات

عملها من مجلس الوزراء، والذي يتكون من وزراء، مسؤولين في وزارتهم عن جمع ومعالجة بيانات الأفراد، فهم يمثلون صفة المسؤول والمعالج عن البيانات وبذات الوقت، عليهم مهام كمجلس حماية بيانات، فكيف ستتمكن الوحدة من مخاصمتهم، وتوجيه الإنذار لهم، وتنسيب الجزاءات، وفرض الغرامات، في حال إخلالهم بأمن وسلامة البيانات؟ وكيف ستقوم بإصدار توصياتها بحيادية، ونزاهة، واستقلالية، في حال ارتكاب أفراد السلطة التنفيذية لمخالفات بحق الأفراد؟

أما بالنسبة للتشريع المقارن فقد نص على إنشاء سلطة إشرافية مستقلة في كل دولة عضوٍ في الإتحاد الأوروبي مثل السلطة الوطنية لحماية البيانات (Data Protection Authority –DPA) مع ضمان الاستقلالية لعمل هذه الهيئة، من خلال منع أعضاء الهيئة عن الازدواجية بالجمع بين وظيفته في الهيئة وأي وظيفة أخرى لا تتوافق مع وظيفتهم، أو وظيفة مدفوعة الأجر، وأن تخصص الدول ميزانية مالية منفصلة وخاصة في الهيئة، وأن تزود الدولة الهيئة بالموارد البشرية، والتقنية والمالية، والمكانية لتمارس عملها باستقلالية وفعالية.(GDPR, Article 51,52)

وحدد الGDPR المهام والصلاحيات لهذه السلطات، حيث يتمتع كل جهاز إشرافي بسلطة مراقبة الامتثال لقانون حماية البيانات الشخصية، بما في ذلك التحقيق والشكاوى، وتتخذ هذه السلطات التدابير القانونية ضد الانتهاكات، مثل إجراء التحقيقات، وفرض الغرامات أو العقوبات الأخرى، وإصدار الإرشادات والتوجيهات المتعلقة بحماية البيانات، وأيضاً التعاون مع السلطات الوطنية في الدول الأخرى لتطبيق القانون، وهذا يتطابق مع مهام ومسؤوليات الوحدة التي أوجدها المشرع الأردني.(GDPR, Article 57,58)

ولها الصلاحية بفرض رسوم تتناسب مع التكلفة الإدارية، أو رفض الطلب المقدم من الشخص المعني في حال الإفراط في تقديم الطلبات، أو في حال الشكاوى الكيدية وهذا ما لم يعالجه المشرع الأردني. (GDPR, Article 57)

تستخلص الباحثة مما سبق، أن التشريع المقارن قدم تفاصيل أكثر، حول الصلاحيات وضمان استقلالية الهيكل التنظيمي للسلطات الإشرافية، والمؤهلات الواجب توافرها لدى كل من أشخاص تنفيذ القانون، مقارنة مع القانون الأردني، كما ويجب العمل في التشريع الأردني على فصل الوحدة تماماً عن الحكومة، لما يحقق ذلك من استقلالية لها في اتخاذ القرارات، وتحقيقاً لمبدأ الحيادية والنزاهة.

- **مجلس حماية البيانات الشخصية:**

أوجد المشرع الأردني مجلس لحماية البيانات، برئاسة وزير الاقتصاد الرقمي والريادة، ويتمتع هذا المجلس بعدد من المهام، والصلاحيات المهمة، التي تساهم في ضمان تطبيق القانون، ومراقبة الامتثال لسياسة حماية البيانات، على أن يتولى المجلس وضع السياسات العامة الخاصة بحماية البيانات الشخصية في المملكة، وتقديم التوجيهات والإرشادات للجهات المسيطرة والمعالجين، وتمثيل المملكة في المحافل المتعلقة بحماية البيانات داخليا وخارجياً، بالإضافة إلى، ذلك يتوجب عليه الاطلاع على التقرير السنوي الخاص بالوحدة، ورفعه إلى مجلس الوزراء بعد إقراره، وأيضا إجراء الدراسات والبحوث المتعلقة بحماية البيانات الشخصية، والتعاون مع الهيئات المحلية والدولية لتحقيق أفضل ممارسات حماية البيانات. (المادة 16و17 من قانون حماية البيانات الشخصية)

و باستقراء نص المادة السابعة عشر/ج؛ والتي منحت المجلس سلطة إصدار التراخيص الخاصة بجمع، ومعالجة، وتخزين، ونقل البيانات، لصالح هيئات مختلفة، والذي يرتبط ارتباطا وثيقا بنص المادة الرابعة والعشرون/أ/1 فإن الباحثة ترى أن هذه التراخيص والتصاريح سوف توسع من نطاق الهيئات المعالجة لبيانات الأفراد، والتي يمكنها أيضا تبادلها بموجب هذه التراخيص على المستويين

الداخلي، والخارجي، مما قد يؤدي إلى احتمالية الإخلال بأمن وسلامة البيانات، نظراً لأن هذه التراخيص تؤدي لكثرة المعالجين في القطاعين العام والخاص، وكون المجلس لم يحدد بعد آلية إصدار هذه التراخيص، ولا الشروط الواجب توافرها في الهيئات لتتمكن من الحصول عليها.

ترى الباحثة وكما أسلفت سابقاً، وتحديداً عند الحديث عن صلاحيات الوحدة، أن المادة السابعة عشر/ه منحت المجلس حق النظر في الشكاوي، سواء المقدمة من الأفراد أو من المسؤول بحق مسؤول آخر، هنا نكرر أيضاً تساؤلنا حول؛ كيفية تحقيق مبدأ العدالة، والنزاهة، والمجلس هو نفسه الخصم والحكم، مستندين في هذا التعبير إلى نص المادة السادسة عشر، الذي وضح تشكيل المجلس من رئيس وأعضاء، فجعل أكثر أعضاء المجلس هم أصلاً معالجين، يديرون هيئات عملها الأساسي جمع، ومعالجة، وتخزين، ونقل البيانات، وهذا لا يضمن الحيادية، والنزاهة، ولا حتى الشفافية، في الحكم واتخاذ القرار بحق الشكاوى المقدمة للمجلس، كما وسيجعل الشخص المعني في متاهة التظلم إلى من هو خصمه أساساً.

وبالعودة إلى التشريع المقارن، نجد أن اللجنة الأوروبية لحماية البيانات European Data Protection (EDPB) ، هي من تتخذ القرارات السياسية الكبرى، تتكون هذه اللجنة من السلطات الوطنية، لحماية البيانات في جميع الدول الاعضاء في الإتحاد الأوروبي، كل دوله عضو في الإتحاد الأوروبي لديها هيئه حمايه بيانات خاصه بها، وهذه الهيئات تجمع في اللجنة، وتتمثل وظيفة هذه اللجنة الأوروبية في أنها تشرف على تنفيذ GDPR ، وتضمن تطبيقه بشكل موحد عبر جميع الدول الاعضاء في الاتحاد الاوروبي، ومن اختصاصاتها إصدار التوجيهات وتفسيرات حول كيفيه تطبيق GDPR، في الحالات المختلفة، وتتولى التنسيق بين السلطات الوطنية لحمايه البيانات، لضمان وجود تطبيق موحد للائحة عبر الإتحاد الأوروبي، وتختلف عن المجلس بنطاقها الجغرافي، حيث أنها هي هيئه تنفيذيه على مستوى الإتحاد الأوروبي ككل، ولها صلاحيات قانونيه في جميع الدول الأعضاء في الإتحاد الأوروبي، وتتمتع بسلطه اتخاذ قرارات تنظيميه، وتنفيذ التنسيق بين الهيئات الوطنية، إلا أن مجلس حماية البيانات، هو جهة محلية تعمل ضمن إطار قانوني محلي يقتصر على المملكة الأردنية الهاشمية، ولا يمتلك السلطة لتنسيق السياسات بين دول متعددة، بل يركز على ضمان الامتثال الوطني لقانون حمايه البيانات الشخصية داخل حدود المملكة الأردنية.(GDPR, Article68,69,70)
بالنتيجة فإن دور اللجنة الأوروبية في الاتحاد الاوروبي يتمتع بسلطه أكبر على مستوى الانتشار الإقليمي، والتنسيق بين الدول الاعضاء، في حين مجلس حماية البيانات الشخصية في الاردن يتعامل وفق الإطار الوطني فقط.

باستقراء نص المادة السابعة عشر/ح من التشريع الأردني، والتي منحت المجلس الحق في إجراء فحص دوري للملائمة على المستوى الخارجي، فهي تماثل المادة الخامسة والأربعون البند الثالث، من التشريع المقارن، والتي منحت المفوضية الأوروبية الحق في تقيم مستوى الحماية، التي توفره الدول أو المنظمات الخارجية عند نقل البيانات لها، وذلك حفاظاً على سرية، وأمن هذه البيانات وتحقيقاً لمبدأ الملائمة، لكن التشريع المقارن حدد مدة إجراء الفحص الدوري كل أربع سنوات على الأقل، وهذا مالم يحدده المشرع الأردني.

من وجهة نظر الباحثة إن على المشرع الأوروبي أصاب بهذا التحديد، مما يضمن التحديث في قوائم الدول، والمنظمات، والهيئات الخارجية المعتمدة، ومكافئة بمستوى الحماية وفي النهاية، تضيف الباحثة، أن القانون الأردني وحفاظا على المرونة التي سعى إليها المشرع الأردني في نصوصه، ما هي إلا ضرورة من ضرورات مواكبة تطور العصر الرقمي، كون القانون لا يزال يحبو، في مجال حماية البيانات الشخصية فقد تظهر مستجداتٌ، وأمور بعد تطبيق القانون تلفت نظر المشرع، أو الوزارة إلى ضرورة شمولها بنطاق حماية القانون.

المطلب الثاني: العقوبات

وفقا للتشريع الأردني، تتدرج العقوبات الإدارية، التي يقضي بها المجلس على الأفراد، والهيئات المخالفين لأحكام هذا القانون، بدأً من الإنذار، وانتهاءً بالغرامة المالية، وذلك بعد أن تصدر الوحدة توصيتها إلى المجلس، بعدم تنفيذ المخالفين لمضمون الإنذار الأولي؛ الذي وجهته خلال المدة المحددة فيه.

باستقراء نصوص المواد الواحدة والعشرون، والثانية والعشرون، من القانون تستنتج الباحثة الملاحظات التالية، بخصوص العقوبة المدنية التي فرضها المشرع على الأفراد، أو مسؤول حماية البيانات عند عدم الامتثال للقانون، أو استخدام البيانات الشخصية بطرق مخالفة للقانون:

- إنه المجلس والوحدة هم نفسهم الأشخاص المعنين بفرض العقوبة وهم نفسهم الأشخاص الذين يمثلون هيئات تعالج وتجمع بيانات الأفراد.
- لم يفرق المشرع في العقوبة من حيث طبيعة البيانات إذا كانت بيانات شخصية أو حساسة.
- لم ينص على عقوبات خاصة بحق الإخلال بأمن بيانات طفل، امرأة، أو شخص لا يتمتع بالأهلية القانونية، كون هذه الشريحة من المجتمع لها خصوصيتها ووضعها الخاص والحساس.
- لم يفرق المشرع في مقدار الغرامة؛ من حيث مدى جسامة الضرر.
- مقدار الغرامة المالية مبلغ قليل جداً قد لا يكون كافياً لردع المخالفين، ومنعهم من تكرار المخالفة.
- اللائحة الأوروبية كانت أكثر صرامة وتشدد مع المخالفين حيث فرضت عشر ملون يورو، أو اثنان بالمئة من إجمالي الإيرادات السنوية– أيهما أكبر– في حالة الضرر الأقل خطورة، وفي حال الانتهاك الجسيم عشرون مليون يورو، أو أربعة بالمئة من الإيرادات السنوية.
- في اللائحة الأوروبية كان هناك أمور يجب الأخذ بها عند فرض الغرامة، فتكون سبباً لتخفيفها، أو تغليظها، وهذا ما لم يناقشه المشرع الأردني. (GDPR, Article 82,83,84)

من وجهة نظر الباحثة، إن المشرع يهدف من العقوبة الضغط على الكيانات أو الأفراد لضمان الامتثال لأحكام القانون، خاصة في حال استمرار المخالفة لفترة طويلة، لكن هذه النتائج السابقة الذكر، قد لا تجعل منها مخالفة رادعة وخصوصاً أن مبلغ الغرامة قليلاً مقارنة بما فرضه التشريع الأوروبي، فمن الأفضل إعادة النظر بالغرامة، لتكون متناسبة مع جسامة الضرر المترتب على المخالفة، وبالتالي تكون رادعة ومانعة من تكرار المخالفة.

الخاتمة:

التشريع الأردني هو تشريع حديث يظهر اهتمام الأردن بحماية البيانات الشخصية، ويمثل خطوة كبيره نحو تعزيز الأمان الرقمي، وحماية الخصوصية، لكن نستخلص هناك جوانب تحتاج إلى تحسين، حيث تمثلت في آلية التنفيذ والرقابة، كذلك هناك بعض الغموض في التشريعات المتعلقة بالنقل الدولي، والحصول على الموافقات أو التراخيص، يمكن أن يشكل تحدياً في التطبيق، خصوصاً في التعامل مع البيانات الحساسة؛ مثل البيانات المالية، وكذلك غموض حول آليه ممارسه الأفراد لحقوقهم، تضمن أيضا القانون؛ أُطراً تنظيمية جيده إلا أن مستوى الوعي العام حول حماية البيانات لا يزال محدوداً في بعض القطاعات مما قد يعيق تطبيق القانون بشكل فعال.

بعد التحليل توصلت الدراسة إلى نتائج عدّة أهمها:

1. لم يأتِ المشرع الأردني على ذكر حق تقيد المعالجة من قبل الشخص المعني كما فعل التشريع المقارن الذي فرضه ضمن أسباب معينه تقتضي وقف المعالجة لفترة محددة، أو تقيدها لغرض معين.
2. أعطى المشرع للشخص المعني الحق في المحو، أو الحق في النسيان – كما يطلق عليه في التشريع المقارن– إلا أنه لم يوضح نوعية البيانات التي يشملها هذا الحق، ولا آلية حصول لفرد على هذا الحق.
3. إن التشريع الأردني لم يكن دقيقاً في بسط آلية تقديم الطلبات لاستفاء الحق أو لتمكين الشخص المعني من هذه الحقوق، كما لم يحدد المدد القانونية للرد على الطلبات المقدمة من الشخص المعني.
4. لم يفرق المشرع الأردني بين البيانات الشخصية والبيانات الحساسة، من حيث المعالجة أو تغليظ العقوبة على الإخلال بأمنها، بالرغم من أن الأخيرة تحتاج لعناية إضافية تتناسب مع طبيعتها.
5. لم يفرد المشرع الأردني نصوصاً خاصة للتعامل مع بيانات تعود لفئات لها خصوصيتها في المجتمع الأردني كالطفل– أقل من 18سنة– أو المرأة، أو بيانات لأشخاص فاقدي الأهلية، ولم يغلظ العقوبة في حال كان الإخلال بأمن البيانات واقعاً عليها.
6. لم يوفر المشرع الأردني إطاراً قانونياً ينظم المعالجة الآلية، أو التنميط، كما فعل التشريع المقارن، كذلك لم يوفر التشريعان أحكاماً خاصة بالذكاء الاصطناعي كنتيجة للتطور التكنولوجي الحاصل.
7. الاستثناءات الواردة في القانون تعتبر جزءاً من مرونته، إلا أن كثرة الاستثناءات على النص التشريعي أدت إلى إفراغ القاعدة من مضمونها، فكان هناك استثناء يقابل كل حق للأفراد، واستثناءات على إذن الموافقة المسبقة، مما يشكك بمدى فعالية تطبيقه في تحقيق التوازن بين حماية البيانات الشخصية، وحماية المصالح الأخرى.
8. الاستثناءات الخاصة بتبادل البيانات داخل وخارج المملكة، تشكل حلاً مرناً، لتلبية احتياجات الأمن القومي، والتعاون التجاري الدولي، لكنها في ذات الوقت تطرح تحديات تتعلق بتطبيق المعايير المناسبة لحماية البيانات.
9. أبرز التحديات التي تواجه تطبيق القانون ستكون بسبب نقص الوعي القانوني لدى الأفراد بحقوقهم وواجباتهم من جهة، ونقص و/ أو تفاوت المعرفة التكنولوجية لدى فئات المجتمع الأردني، ولدى الجهات القضائية كون التشريع لا يزال جديداً من جهة أخرى.
10. ازدواجية مسؤوليات ومصالح الهيئات التي أنشأها المشرع بموجب القانون حيث أن: أ– رئيس المجلس، وأغلب أعضاءه من السلطة تنفيذية، فهناك تداخل في الأدوار والمسؤوليات.

    ب– الوحدة التنظيمية لا تتمتع بالاستقلالية الكاملة في اتخاذ قراراتها.
11. الغرامة التي فرضها المشرع الأردني كعقوبة على الإخلال بأمن البيانات، غير كافية لضمان الامتثال، وتحقيق الردع، وبذات الوقت حماية خصوصية الأفراد ولم تفرق في حال كان الإخلال بأمن بيانات شخصية أو حساسة، أو بيانات تخص فئات لها وضعها الخاص من المجتمع.
12. التراخيص والتصاريح التي نص عليها التشريع الأردني ستضفي المرونة على القانون، وتشجع الابتكار والنمو الاقتصادي، إلا أنها ستؤدي إلى كثرة المعالجين وبالتالي تفتح باباً للاستخدام غير المشروع، وتسريب البيانات أو تعرضها بشكل أكبر للهجمات الإلكترونية.

التوصيات:

ومن خلال هذه الدراسة توصي الباحثة بعدة توصيات، وهي:

1. توصي الباحثة المشرّع الأردني بإعادة النظر بخصوص حق تقيد المعالجة، نظراً لأهميته في تمكين الأفراد من التحكم في كيفية استخدام بياناتهم، مما يعزز الشفافية وحماية الخصوصية، ويضمن التوافق بين التشريع الأردني والتشريع المقارن.
2. توصي الباحثة المشرّع الأردني بتوضيح آلية تمكين الشخص المعني من حقه، وذلك من خلال تحديد إجراءات محددة لتقديم الطلبات، ومتابعة الشكاوى والمدد القانونية التي على الجهة المقدم الطلب إليها الالتزام فيها لتقديم الرد على الطلب، كجعله مثلاً خمسة عشر يوماً من تاريخ رفع الطلب، أو تاريخ قيد الشكوى، قابلة للتمديد وتسبيب التأخير عن المدة المحددة قانونا في حال حدوث ذلك، لضمان الشفافية وسرعة الإجراءات، وكما هو معمول بالتشريع المقارن.
3. توصي الباحثة المشرع بضرورة رفع مستوى العناية بالبيانات الحساسة، وذلك بإفراد نصوص خاصة تضمن الشفافية في معالجتها، وتجعل المعالجة لها مشروطة بالموافقة المسبقة الواضحة والصريحة والمنفصلة عن أي موافقة أخرى، ويُمكِن الأفراد من السحب الطوعي للموافقة متى ما أرادوا.
4. توصي الباحثة المشرّع الأردني بأن يفرد للفئات التالية بالمجتمع (المرأة، الطفل، فاقد الأهلية) نص قانونيا يعزز الحماية لبياناتها الشخصية، والحساسة منها تحديدا وأقترح عليه النص التالي:
   - يجب الحصول على إذن الموافقة المسبقة من الولي أو الوصي القانوني للطفل دون الثامنة عشر، والوصي القانوني لفاقد الأهلية، والمرأة قبل البدء بمعالجة بياناتهم، بشرط أن تكون هذه الموافقة واضحة، مقيدة بالغرض الذي جمعت من أجله، وتكون عملية جمع البيانات لهذه الشريحة من المجتمع، شفافة وواضحة ومحددة، ولا تستخدم لأغراض استغلالية أو تسويقية.
   - مع مراعاة ما ورد بأي قانون آخر من عقوبات أشد، فإن العقوبة في حال حدوث إخلال بأمن بيانات، وخاصة إذا ما تم استخدامها في الذكاء الاصطناعي وبطريقة مخالفة للقانون، هذه الفئة يتم تغليظ العقوبة الواردة في نص المادة 22/أ للضعف
   - يكون لهذه الفئات الحق بمحو بياناتهم فوراً بعد الانتهاء من غرض المعالجة، مع ضمان التنفيذ الأمن.
   - يكون لهذه الفئات الحق في الاعتراض على معالجة بياناتهم الشخصية لأغراض التسويق، والمعالجة الآلية، والتنميط، الذكاء الاصطناعي، وغيرها من الأمور المخالفة لأحكام القانون.
   - شمول هذه الفئات ببرامج التوعية بحقوقهم وكيفية تمكنينهم منها، وكيفية اقتضاءها.
5. توصي الباحثة المشرّع الأردني بأن يفرد نصوصاً قانونية تتعلق بتعزيز حماية البيانات الشخصية، والحساسة من المعالجة الآلية، والتنميط، والذكاء الاصطناعي، مع ضرورة الموازنة بين ما لهذه الأمور من أهمية في الابتكار، والتطور التكنولوجي، ومدى خطورتها وتأثيرها على حياة الأفراد الشخصية، أو المهنية، أو الاجتماعية
6. توصي الباحثة المشرّع الأردني أن يظل المبدأ الأساسي في معالجة البيانات هو حماية خصوصية الأفراد، والمعالجة بشفافية، والعمل على تقليص، وتحديد الاستثناءات ما أمكن، وتعزيز الرقابة الدورية على الهيئات المستثناة، للتأكد من امتثالها للقانون، وضمان الموازنة بين الحقوق الفردية، والمصالح المشروعة.

7. توصي الباحثة المشرّع الأردني، بالعمل على الموازنة بين الاستثناءات المتعلقة بنقل البيانات داخلياً وخارجيا، وحماية خصوصية الأفراد، بياناتهم من الاستغلال الغير مشروع، مع مراعاة الضرورات القانونية والتجارية، والأمن القومي، وأقترح عليه إعادة صياغة نص يراعي ما يلي:
   - النقل الدولي: وضع إطار دولي يتفق مع التشريع المقارن لتحديد المعايير اللازمة لحماية نقل البيانات خارجيا، وإجراء الفحص الدوري لملائمة الحماية كل 4 سنوات على الأقل.
   - النقل الداخلي: تعزيز الرقابة على الشركات والجهات الحكومية لضمان حماية حقوق الأفراد.
   - وفيما يخص البيانات الحساسة اشتراط إذن الموافقة المسبقة من الشخص المعني، في غير الحالات التي تمس الأمن القومي، والمصلحة العامة.
   - وفي النهاية مراجعة الاستثناءات بشكل دوري لضمان عدم استغلالها بشكل مفرط.
8. توصي الباحثة المشرّع الأردني وسنداً للمادة 24 من قانون حماية البيانات الشخصية أن يوعز إلى من يهمه الأمر لدى الجهات والمؤسسات الحكومية المعنية بالتثقيف، أو التعليم، أو التدريب بأن تعمل على:
   - تنظيم حملات توعية موسعه تستهدف جميع فئات المجتمع، بما في ذلك الأفراد، والكيانات التجارية ومؤسسات القطاعين العام والخاص، حول أهمية حماية البيانات الشخصية.
   - تعزيز التدريب والتعليم في مجال حماية البيانات الشخصية داخل المدارس والجامعات، بالإضافة إلى الإعلانات التثقيفية عبر وسائل الإعلام المختلفة على مستوى الأفراد، وعقد دورات، وندوات تثقيفية، وورش عمل حول كيفية الامتثال للقانون على مستوى الهيئات العامة والخاصة
   - تفعيل الرقابة الدورية على الشركات والمؤسسات للتأكد من مدى إلمامها بالجوانب المعرفية للقانون، ومدى امتثالها له، وتوجيهها فوراً عند اقتضاء ذلك.
9. توصي الباحثة المشرّع الأردني بأن يعدل نص المادة 22 من القانون، بحيث يجعل حجم الغرامة متوازنا مع حجم الضرر، المترتب على حجم الإخلال بأمن البيانات، وطبيعتها، والفئة الواقع عليها الضرر، مع مراعاة ألا يكون مقدار الغرامة مرهقاً للأفراد أو غير كافٍ لردع المؤسسات، بما يتفق مع معايير التشريع المقارن، وكذلك ضرورة المراجعة الدورية لحجم الغرامة، لضمان مدى فعاليتها، ومدى توازنها مع المخاطر المترتبة على الإخلال بأمن البيانات.
10. توصي الباحثة المشرّع الأردني بأن يعمل على ضمان استقلالية الوحدة التنظيمية لحماية البيانات بوضع هيكل قانوني وإداري واضح يسمح لها بالعمل بحيادية دون أي تدخل خارجي، والاهتمام بتدريب وتطوير أفرادها لضمان الاستقلال القانوني، مواكبة التطورات والمستجدات، وتأمين مخصصات مالية ترعي أولوياتها وأهدافها، لضمان الاستقلال المالي، وأخيرا وكما جاء بالتشريع المقارن أن تكون آلية التعين فيها على أساس الكفاءة، والشفافية، وتحديد مدة ولاية لأعضائها.
11. توصي الباحثة المشرّع الأردني، وكما هو معمول بالتشريع المقارن، بتعين هيئة مستقلة عن السلطة التنفيذية لتمثل المجلس، لضمان النزاهة، والحياد في اتخاذ القرارات، وأن يتم اختيار أعضائه ضمن مؤهلات قانونية وفنية، محددة بنص القانون، ويكون اختيار هيكلة على أساس الانتخاب، أو اختبارات مهنية محددة مثلا، ويجري الأمر على ذلك بالنسبة الخبراء المذكورين في المادة 6/أ/16 مما يضمن العدالة والشفافية.

12. توصي الباحثة المشرع الأردني، بأن لا يتوسع في منح التراخيص والتصاريح، ويحكمها بشروط صارمة يضمن فيها أمن وسلامة البيانات، وكذلك اشتراط إذن الموافقة المسبقة للشخص المعني وفقا للمادة الخامسة من القانون، وتمكين الشخص المعني من سحب الموافقة بسهولة في الحالات التي أجازها القانون.

المراجع:

اسخيطه، رضوان (2018)، اضاءة على اللائحة الاوروبية لحماية البيانات الشخصية، بلا طبعة، عمان: مكتبة نور خاص–رضوان اسخيطه.

الجعافرة، رويدة حسن، (2022)، قانون حماية البيانات الشخصية في الاردن، المجلة العربية للنشر العلمي، العدد (50)، (Online) Available: www.ajsp.net مستخلص بتاريخ 2024/10/10

سويلم، خالد، محمد، (2022)، الحماية القانونية للبيانات الشخصية الالكترونية "دراسة مقارنة"، المجلة القانونية، المجلد (14)، العدد (6)، (Online) Available: https://jlaw.journals.ekb.eg مستخلص بتاريخ 2024/10/10

عبد الرحمن، دعاء، (2022)، الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي، المجلة القانونية والاقتصادية، المجلد (8)، العدد (0) عدد خاص، (Online) Available: www.jdl.journals.ekb.eg مستخلص بتاريخ 2024/10/10

مشعل، محمد، (2017)، الحق في محو البيانات الشخصية دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الاوروبي GDPR وأحكام المحاكم الاوروبية، مجلة الدراسات القانوني والاقتصاد، المجلد (3)، العدد (2) (Online) Available: www.jdl.journals.ekb.eg مستخلص بتاريخ 2024/10/10

شرقاوي، عبد المنعم (2022)، الوسائل القانونية لحماية معاملات التجارة الإلكترونية في القانون الأردني، مقال منشور على موقع حماة الحق، (Online). متاح على الرابط

www.jordan–lawyer.com مستخلص بتاريخ 2024/10/10

ربيحات، روان (2024)، قانون حماية البيانات الشخصية الأردني خطوة ناقصة للأمام، مقال منشور على منصة دعم السلامة الرقمية Smex (Online)، متاح على الرابط: www.smex.org ومستخلص بتاريخ 2024/10/10

مديرية حماية البيانات الشخصية (2024)، هل نحن بحاجة إلى قانون حماية بيانات شخصية، منشورات موقع وزارة الاقتصاد الرقمي والريادة،(Online) ، متاح على الرابط: https://modee.gov.jo/ مستخلص بتاريخ 2024/10/10.

قانون المعاملات الالكترونية الاردني رقم (15) لسنة (2015).

قانون حماية البينات الشخصية رقم 24 لسنة (2023).

الدستور الاردني لسنة (1956).

GDPR اللائحة العامة الأوروبية (2018)

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد السابع والسبعون
تاريخ الإصدار: 2 – آذار – 2025م
www.ajsp.net

"Legal Protection of Personal Data in Electronic Transactions Under Jordanian Legislation and European Legislation (GDPR) Comparative Stady"

Abstracts:

This study addressed a newly emerging topic, namely Protecting personal data, by addressing the legal provisions related to it according to the Jordanian Personal Data Protection Law and the GDPR.

This study aimed to present the best ways to protect personal data and improve laws in line with comparative legislation, and the importance of the study emerged in clarifying the weaknesses of Jordanian legislation and indicating the extent of its compatibility with the standards of protection provided by comparative legislation, starting from the rights it provides to individuals, the principles on which it is based, the tools for implementing the law and ensuring compliance with it, in order to indicate the adequacy of Jordanian legislation to protect personal data, using the descriptive approach, analytical approach and comparative approach.

One of the most prominent findings of the study was the large number of exceptions to the legislative text, as well as the existence of duplication between the responsibilities and interests of the bodies established by the legislator under the law.

Among the most prominent recommendations are defining exceptions precisely, strengthening periodic monitoring of institutions, educating individuals about their rights, ensuring a balance between protecting individual rights and legitimate interests, and for law enforcement bodies, the recommendation was that they be formed using a mechanism that is clearly defined by law.

Keywords: Personal data protection, Right to erasure, Digital privacy, Sensitive personal data, GDPR ,DPO.