International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
Vol. (5), No. (5)
IJLRS
May 2026
الإصدار (5)، العدد (5)

الحماية القانونية لبيانات العامل الشخصية في النظام السعودي

سلمى أبوبكر المحضار
باحثة ماجستير، قسم القانون الخاص، كلية الحقوق، جامعة الملك عبد العزيز، المملكة العربية السعودية
salmaalmehdhar.98@outlook.com

المستخلص

هدفت هذه الدراسة إلى بيان الحماية القانونية لبيانات العامل الشخصية في النظام السعودي، من خلال بيان مفهوم البيانات الشخصية للعامل وحقوقه تجاهها، ومن ثم بيان معايير وضوابط جمع ومعالجة هذه البيانات، و أبرز صور انتهاكها، والآثار القانونية المترتبة على الانتهاك، واعتمدت الدراسة على المنهج التحليلي، وذلك من خلال تحليل نصوص نظام العمل ونظام حماية البيانات الشخصية ذات العلاقة، وتوصلت الدراسة إلى أن المنظم استطاع الموازنة بين حق صاحب العمل في إدارة منشأته ومعرفة بيانات العاملين لديه وبين حق العامل في الخصوصية عبر فرض الضوابط والالتزامات التي تحمي بيانات العامل الشخصية، وأنه يترتب على انتهاك بيانات العامل قيام المسؤولية الجنائية، والمسؤولية الإدارية، بالإضافة لحق العامل في طلب التعويض عن الأضرار المادية والمعنوية التي اصابته نتيجة ذلك، وأوصت الدراسة بفرض دورات تدريبية إلزامية للعاملين الذين تسمح لهم طبيعة عملهم بالتعامل مع البيانات في بيئة العمل حول ضوابط نظام حماية البيانات الشخصية.

الكلمات المفتاحية: نظام العمل، نظام حماية البيانات الشخصية، البيانات الشخصية للعامل، حقوق العامل، صاحب البيانات، المسؤولية القانونية، الحماية القانونية.

Legal Protection of Employees' Personal Data under the Saudi Legal Framework

Salma Abubakr Al-Mehdhar
Master's Researcher, Department of Private Law, Faculty of Law, King Abdulaziz University, Kingdom of Saudi Arabia
salmaalmehdhar.98@outlook.com

Abstract

This study aimed to elucidate the legal protection afforded to employees' personal data under the Saudi legal framework by clarifying the concept of an employee's personal data and the employee's rights in relation thereto, and then by examining the standards and controls governing the collection and processing of such data, the most salient forms of infringement thereof, and the legal consequences arising from such infringement. The study adopted the analytical method through an examination of the relevant provisions of the Saudi Labor Law and the Personal Data Protection Law (PDPL). The study concluded that the regulator has succeeded in striking a balance between the employer's right to manage its establishment and to access the data of its employees, on the one hand, and the employee's right to privacy, on the other, by imposing controls and obligations that safeguard the employee's personal data. It further concluded that infringement of an employee's data gives rise to criminal liability and administrative liability, in addition to the employee's right to claim compensation for the material and moral damages sustained as a result thereof. The study recommended the imposition of mandatory training courses for employees whose functions, by their nature, permit

them to handle data within the workplace, with a view to ensuring compliance with the controls prescribed by the Personal Data Protection Law.

Keywords: Saudi Labor Law, Personal Data Protection Law (PDPL), Employee Personal Data, Employee Rights, Data Subject, Legal Liability, Legal Protection.

المقدمة

بسم الله الرحمن الرحيم، الحمد لله رب العالمين، والصلاة والسلام على سيد المرسلين وخاتم النبيين، وعلى آله وصحبه أجمعين، أما بعد:

يعتبر العمل إحدى ضرورات الحياة، والركيزة الأساسية للنهضة والسبيل لتعمير الأرض، وللعمل مكانة رفيعة في الإسلام، فقد عظّمت الشريعة الإسلامية شأن العمل وحثت عليه، قال الله تعالى في كتابه الكريم: (هُوَ الَّذِي جَعَلَ لَكُمُ الْأَرْضَ ذَلُولًا فَامْشُوا فِي مَنَاكِبِهَا وَكُلُوا مِنْ رِزْقِهِ وَإِلَيْهِ النُّشُورُ). [الملك، آية: 15]، وقال صلى الله عليه وسلم: "ما أكل أحد طعاماً قط خيراً من أن يأكل من عمل يده".

وفي المملكة العربية السعودية التي تعتبر القوى البشرية هي الثروة الحقيقية والمحرك الرئيسي للتنمية المستدامة، نُظم مفهوم العمل في إطار قانوني واضح، حيث أنه لم يترك العلاقة بين العامل وصاحب العمل لتقديرهم المطلق، بل أخضعها لإطار تنظيمي آمر لتحقيق التوازن الاقتصادي والاجتماعي.

وتعد العلاقة العمالية من العلاقات ذات طبيعة قانونية خاصة، وذلك لكونها تقوم على عنصري التبعية والإشراف، إلا أن هذه التبعية لا تعني إهدار حقوق العامل اللصيقة بشخصه، كحقه في الخصوصية وحقه في حماية بياناته الشخصية، ومع التحول الرقمي الذي يشهده العالم بأسره، وتوسع المنشآت والشركات في استخدام التقنيات الحديثة في غالبية المجالات ومن ذلك استعمالها في إدارة الموارد البشرية، أصبحت البيانات الشخصية للعامل معرضة لمخاطر الانتهاك.

مشكلة الدراسة وتساؤلاتها

وتتبلور مشكلة الدراسة في التحدي القانوني المتمثل في حماية البيانات الشخصية للعامل في ظل التحول الرقمي والاعتماد المتزايد على الوسائل التقنية التي قد تجعل بيانات العامل عرضة للانتهاك، وبوجود نظام العمل ومع صدور نظام حماية البيانات الشخصية، ثار التساؤل حول مدى كفاية النصوص الحالية في توفير هذه الحماية.

ودراسة هذا الموضوع تثير التساؤل التالي:

كيف نظّم المنظم السعودي موضوع حماية البيانات الشخصية للعامل؟

ويتفرع عن هذا التساؤل الرئيسي التساؤلات الفرعية التالية:

- ما هو مفهوم البيانات الشخصية للعامل؟
- ما هي الحقوق المترتبة للعامل على بياناته؟
- ما هي ضوابط جمع ومعالجة البيانات؟
- ما هي صور انتهاك البيانات الشخصية للعامل؟
- ما هي الضمانات والجزاءات التي قررها المنظم السعودي لحماية بيانات العامل في حال انتهاكها؟

أهداف الدراسة

تهدف الدراسة إلى:

- تحديد مفهوم البيانات الشخصية للعامل.
- بيان الحقوق المترتبة للعامل على بياناته.

- استنباط المعايير التي فرضها النظام لضمان مشروعية جمع ومعالجة البيانات.
- استعراض صور انتهاك البيانات الشخصية للعامل.
- بيان المسؤولية القانونية والآثار المترتبة على انتهاك البيانات الشخصية للعامل.

أهمية الدراسة

وتنقسم أهمية الدراسة إلى:

- الأهمية العلمية: تكمن أهمية الدراسة في كونها تربط بين نظام العمل ونظام البيانات الشخصية، مما يساهم في إثراء الأدبيات القانونية ذات الصلة بقانون العمل في المملكة؛ نظرًا لقلة الأبحاث في هذا الموضوع.
- الأهمية العملية: تكتسب الدراسة أهميتها العملية من كونها تأتي موضحة حق العامل في حماية بياناته الشخصية خصوصًا في ظل توسع الشركات والمنشآت في استخدام التقنيات الحديثة وتقنيات الذكاء الاصطناعي.

منهج الدراسة

ستعتمد الدراسة على المنهج التحليلي، وذلك من خلال تحليل نصوص نظام العمل ونظام حماية البيانات الشخصية ذات العلاقة، سعيًا لاستنباط الأحكام المحققة لأهداف الدراسة.

حدود الدراسة

- **الحدود الموضوعية**: تقتصر الدراسة على دراسة موضوع حماية البيانات الشخصية للعامل.
- **الحدود المكانية**: يقتصر نطاق الدراسة المكاني على حدود المملكة العربية السعودية.

الدراسات السابقة

- **الدراسة الأولى:** الوادي، آيات محمود حسين، حماية البيانات الشخصية الرقمية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2025م:

تناولت الدراسة موضوع حماية البيانات الشخصية الرقمية في التشريع الأردني، وهدفت إلى بيان مدى حماية البيانات الشخصية الحساسة في ظل قانون حماية البيانات الشخصية الأردني، وذلك من خلال دراسة ماهية البيانات الشخصية الرقمية، ثم دراسة الإطار القانوني لمعالجة البيانات الشخصية، ثم التطرق لموضوع الحماية المدنية للبيانات الشخصية، وتوصلت الباحثة لجملة من النتائج، أبرزها أن الحق في حماية البيانات الشخصية الرقمية هو جزء من الحق في الخصوصية، وأنه يجب أن يكون له إطار قانوني مستقل ووسائل حماية خاصة. كما أوصت الباحثة المشرع الأردني بإعادة صياغة تعريف البيانات الشخصية، لكونه عرف البيانات الشخصية بأنها البيانات أو المعلومات وأن هناك فروقات جوهرية بين المصطلحين.

وتتشابه هذه الدراسة مع دراستنا في تناولها لموضوع حماية البيانات الشخصية، وتختلف عنها في كونها تناولت الموضوع عمومًا في التشريع الأردني، بينما تركز دراستنا على الحماية القانونية للبيانات الشخصية للعامل في النظام السعودي.

- **الدراسة الثانية:** الفارسية، العنود بنت إبراهيم بن عبيد، حقوق صاحب البيانات الشخصية ووسائل حمايتها وفقًا لقانون حماية البيانات الشخصية العماني، رسالة ماجستير، كلية الحقوق، جامعة السلطان قابوس، عمان، 2023م:

تناولت الدراسة موضوع حقوق صاحب البيانات الشخصية ووسائل حمايتها وفقًا لقانون حماية البيانات الشخصية العماني، وهدفت لتسليط الضوء على مضمون حقوق صاحب البيانات الشخصية الواردة في القانون العماني، حيث تكونت الدراسة من مبحث تمهيدي عُني بدراسة ماهية البيانات الشخصية، ومن ثم فصلين رئيسيين، تناول الفصل الأول حقوق صاحب البيانات الشخصية، بينما تناول الثاني موضوع المسؤولية المدنية عن الاعتداء على الحقوق المرتبطة بالبيانات الشخصية، وتوصلت الباحثة لعدد من النتائج والتوصيات، أبرزها أن الحماية القانونية تقتصر على بيانات الشخص الطبيعي الخاضعة للمعالجة فقط وبالتالي يخرج من نطاق الحماية بيانات الشخص الاعتباري والبيانات الشخصية غير المعالجة، بالإضافة لتوصيتها للمشرع العماني بإضافة حق الاطلاع على البيانات الشخصية ضمن حقوق صاحب البيانات الشخصية.

وتتشابه الدراسة مع دراستنا في تناولها لموضوع حماية البيانات الشخصية، وتختلف بتناولها للموضوع عمومًا في القانون العماني، بينما تركز دراستنا على الحماية القانونية للبيانات الشخصية للعامل في النظام السعودي.

- **الدراسة الثالثة:** البروانية، سارة بنت سيف بن أحمد، الحماية الجزائية للبيانات الشخصية -دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة السلطان قابوس، 2022م:

تناولت الدراسة موضوع الحماية الجزائية للبيانات الشخصية، وهدفت الى بيان مفهوم البيانات الشخصية كمحل للحماية الجزائية، بالإضافة لاستعراض الجرائم التي تقع على البيانات الشخصية والعقوبات التي قررها المشرع العماني جزاءً لها، حيث تكونت الدراسة من فصلين، تناول الفصل الأول منها موضوع الحماية الجزائية الموضوعية للبيانات الشخصية، أما الفصل الثاني فقد تناول البحث في الأحكام الإجرائية الخاصة بحماية البيانات الشخصية، وتوصلت الدراسة للعديد من النتائج والتوصيات، أهمها: ان المشرع العماني اعتد بعقوبة الغرامة كعقوبة أصلية بالنسبة للجرائم الواقعة وفقًا لأحكامه ووضع لها حد أقصى بحيث أنها لا تتجاوز خمسمائة ألف ريال عماني، على خلاف القوانين المقارنة التي اتجهت إلى تنويع أدواتها العقابية. كما أوصت الباحثة المشرع العماني بأن لا يكتفي بعقوبة الغرامة في مواجهة الشخص الاعتباري، كون أن هناك عقوبات تحقق ردع أكبر كالمنع من مزاولة النشاط التجاري المرتبط بالاعتداء المرتكب من قبله بشكل مؤقت أو دائم، أو كعقوبة حل الشخص الاعتباري.

وتتشابه هذه الدراسة مع دراستنا في تناول موضوع البيانات الشخصية والحماية المقررة لها، وتختلف في أن دراسة الباحثة تناولت موضوع الجرائم الواقعة على البيانات الشخصية والحماية الجزائية لها عمومًا، بينما ستخصص دراستنا للحديث عن الحماية القانونية للبيانات الشخصية للعامل.

تقسيم الدراسة

وبناءً على ما سبق، ولتحقيق الغرض المرجو من الدراسة، فإن خطة الدراسة تقتضي تقسيمها إلى:

- مطلب تمهيدي: مسوغات جمع بيانات العامل الشخصية
- المبحث الأول: الإطار المفاهيمي للبيانات الشخصية للعامل ومعايير جمعها ومعالجتها:
  - المطلب الأول: مفهوم البيانات الشخصية للعامل وأنواعها.
  - المطلب الثاني: المعايير والمبادئ النظامية لمشروعية جمع ومعالجة بيانات العامل.
- المبحث الثاني: صور انتهاك بيانات العامل والآثار القانونية المترتبة عليها:
  - المطلب الأول: صور انتهاك بيانات العامل الشخصية.
  - المطلب الثاني: الآثار القانونية المترتبة على انتهاك بيانات العامل الشخصية.

المطلب التمهيدي: مسوغات جمع بيانات العامل الشخصية:

قبل الخوض في موضوع الدراسة والحديث عن الحماية القانونية لبيانات العامل الشخصية، وجب التعريف بالعامل، لتحديد النطاق الشخصي لسريان أحكام الحماية التي تتناولها الدراسة، وتوضيح مسوغات جمع بياناته الشخصية بصفته عاملًا تابعًا قانونًا لصاحب العمل.

يعرف قانون العمل على أنه مجموعة القواعد القانونية التي تحكم العلاقات الناشئة عن قيام شخص بالعمل لحساب شخص آخر وتحت إدارته وإشرافه مقابل أجر، أي أنه يجب أن تتوافر عدة شروط في العلاقة العمالية حتى تخضع لنظام العمل، وهي أن تقوم علاقة العمل بين أطراف من أشخاص القانون الخاص، وأن يؤدي العامل عمله مقابل أجر، وأن يكون العامل تابعًا.

وكما هو معلوم، رابطة العمل في صورتها العامة تغطي العمل المستقل والعمل التابع، والعمل المستقل هو العمل الذي ينفرد من يقوم به في تنفيذه وإدارته دون إشراف من أحد، وذلك كعمل الطبيب وعمل المحامي وهذا النوع من العمل يخرج من نطاق

تطبيق نظام العمل، أما العمل التابع، فهو العمل الذي يتم تحت إشراف وتوجيه صاحب العمل، بحيث يكون العامل تابعًا لصاحب العمل تبعية قانونية[1]، والعلاقة الناشئة عن العمل التابع هي العلاقة التي يحكمها نظام العمل، وذلك ما جاء في المادة الخامسة من نظام العمل والتي نصت على: "تسري أحكام هذا النظام على: 1- كل عقد يلتزم بمقتضاه أي شخص بالعمل لمصلحة صاحب عمل وتحت إدارته أو إشرافه مقابل أجر ..."[2].

والتبعية تعد من العناصر المميزة لعقد العمل عن غيره من العقود، ومن العناصر الأساسية التي تجعل العامل خاضعًا لنظام العمل، والتي أكد عليها نظام العمل في مادته الخمسون والتي نصت على: "عقد العمل هو عقد مبرم بين صاحب عمل وعامل، يتعهد الأخير بموجبه أن يعمل تحت إدارة صاحب العمل أو إشرافه مقابل أجر"، ويذهب الرأي الغالب لاعتماد التبعية القانونية كمعيار مُميز لعقد العمل، والتي يقصد بها "القيام بالعمل لحساب صاحب العمل وتحت سلطته وادارته والذي يملك إصدار الأوامر والتوجيهات للعامل ويراقب تنفيذها ويوقع الجزاء التأديبي على العامل إذا أخل بها"[3] وتتبين أهمية عنصر التبعية في دراسة حماية البيانات الشخصية في أن التبعية تخلق نوعًا من الولاية النظامية لصاحب العمل على بيانات العامل الشخصية، و تعطيه السلطة التنظيمية كمسوغ لجمع البيانات، بحيث أن خضوع العمل لإدارة وإشراف صاحب العمل يمنح الأخير حقًا في جمع ومعالجة بعض البيانات الشخصية للعامل، وذلك لتمكين المنشأة من أداء وظائفها، كتسجيل العامل في المؤسسة العامة للتأمينات الاجتماعية، أو إصدار وثائق التأمين وغيرها، وبالمقابل وضع المنظم التزامًا على صاحب العمل بأن لا يستغل أي معلومات شخصية للعامل دون إذنه[4]، وقيّد هذه السلطة بالأغراض المشروعة التي نص عليها نظام العمل ونظام حماية البيانات الشخصية.

وعرّف نظام العمل في مادته الثانية العامل على أنه: "كل شخص طبيعي -ذكرًا أو أنثى- يعمل لمصلحة صاحب عمل وتحت إدارته أو إشرافه مقابل أجر، ولو كان بعيدًا عن ناظرته."[5] ويتبين من التعريف أن لصفة العامل أركان، نحللها من زاوية الحماية المعلوماتية على النحو الآتي:

- **الشخصية الطبيعية**: يقتصر وصف العامل على الشخص الطبيعي، والشخص الطبيعي له حقوق لصيقة بشخصه، ومن ذلك حقه في الخصوصية وحماية بياناته الشخصية وهو حق لصيق بآدميته، فالبيانات التي ندرس حمايتها في هذه الدراسة تشمل اسمه وعنوانه وصوره وبصماته وبياناته الحساسة كبياناته الجنائية أو الائتمانية أو الصحية وغيرها، وهي خصائص بشرية، وبالتالي فإن حماية بياناته هي حماية لكيانه الإنساني.
- **العمل لمصلحة الغير**: وطبيعة العمل لحساب الغير توجب الإفصاح من طرف العامل عن بياناته الشخصية، حيث أنه لا يُتصور أن تقوم منشأة بتشغيل عامل وإتمام إجراءات التوظيف دون الحصول على بيانات تعريفية دقيقة، وبالمقابل يترتب التزام على صاحب العمل بحماية هذه البيانات.
- **الأجر**: ولكون عقود العمل من عقود المعاوضة، فلا يمكن تصور قيام عقد العمل المبرم بين أطرافه دون وجود عنصر الأجر، ومن ناحية البيانات الشخصية، فإن دفع الأجر يوجب على العامل الإفصاح عن بياناته المالية، كحسابه البنكي وغيره.

المبحث الأول: الإطار المفاهيمي للبيانات الشخصية للعامل ومعايير جمعها ومعالجتها

وينقسم هذا المبحث لمطلبين، نوضح المقصود بالبيانات الشخصية للعامل في المطلب الأول، ونحدد معايير ومبادئ جمعها ومعالجتها في المطلب الثاني، على النحو الآتي:

المطلب الأول: مفهوم البيانات الشخصية للعامل:

ولتعريف مفهوم البيانات الشخصية للعامل، نقسم المطلب لفرعين، نوضح المقصود بالبيانات الشخصية عمومًا وأنواعها، ومن ثم نبين مفهوم البيانات الشخصية للعامل، على النحو الآتي:

---

(1) الريس، رزق بن مقبول، والعبد، رضا محمود، شرح أحكام نظام العمل السعودي، مكتبة الشقري، 2017م، ص 36-37.
(2) المادة (5)، نظام العمل، الصادر بالمرسوم الملكي رقم(م/51)، بتاريخ 1426/8/23هـ.
(3) الريس، والعبد، المرجع السابق، ص100.
(4) الدليل الاسترشادي لقواعد أخلاقيات العمل، متاح على:10212021.pdf ، تاريخ الدخول: 20 أبريل 2026م.
(5) المادة (5)، نظام العمل.

الفرع الأول: مفهوم البيانات الشخصية وأنواعها:

يعد مفهوم البيانات الشخصية من المفاهيم التي شهدت تطورًا ملموسًا في الآونة الأخيرة، وذلك نتيجة اتساع نطاق التعاملات، والتطور المتسارع للتكنولوجيا الحديثة، وتزايد المخاوف بشأن المخاطر المرتبطة بها، وذلك ما دفع الدول لتنظيمها وسنّ التشريعات اللازمة لتعزيز الاستخدام الآمن للبيانات الشخصية، وضمان حمايتها من أي تعد أو انتهاك. وفي هذا الفرع نتناول مفهوم البيانات الشخصية ونبين أنواعها.

أولًا: مفهوم البيانات الشخصية:

عرّف المنظم السعودي البيانات الشخصية في المادة الأولى من نظام حماية البيانات الشخصية على أنها: "كل بيان – مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرخص والسجلات، والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي"[6].

ومن التعريف السابق يمكن القول بأن نطاق الحماية يتمثل في بيانات الشخص الطبيعي التي تُمكن من معرفة وتحديد هويته سواءً بطريقة مباشرة عن طريق الاسم او الصورة، أو بطريقة غير مباشرة من خلال ربط البيانات ببيانات أخرى تؤدي لذلك كرقم الهاتف، وبذلك فإن بيانات الشخص الاعتباري تخرج من نطاق الحماية، وذلك يتفق مع تعريف اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي[7] (GDPR) للبيانات الشخصية، وغالبية القوانين المقارنة كالقانون المصري[8]، والقانون الأردني[9] والقانون الاماراتي[10]، والقانون العماني[11]، وعلى خلاف ذلك، فهناك بعض الأنظمة المقارنة التي شملت بيانات الشخص الاعتباري كالقانون الكويتي[12].

ثانيًا: أنواع البيانات الشخصية:

وتصنّف البيانات الشخصية بناءً على طبيعتها إلى بيانات شخصية عادية كالأسماء والعناوين، وبيانات شخصية حساسة، وفرّق المنظم بين الحماية المقررة للأولى عن الحماية المقررة للأخيرة نظرًا لطبيعتها الخاصة، لذلك وجب بيان أنواع البيانات الشخصية، على النحو الآتي:

أ- **البيانات العادية**: وهي البيانات الوارد ذكرها في التعريف، وهي كل معلومة تساهم وتؤدي لتحديد هوية الفرد أو تجعل التعرف عليه ممكنًا، وتتمثل في بيانات الهوية التقليدية كالاسم ورقم الهوية، وفي بيانات التواصل كالعناوين الوطنية وأرقام الهواتف، بالإضافة للمعرفات الرقمية مثل بروتوكول الانترنت (IP address)، ومعرفات الأجهزة، التي تتيح تتبع سلوك الشخص الرقمي وتحديده.

ب- **البيانات الحساسة**: وعرفها المنظم السعودي على أنها: "كل بيان شخصي يتعلق بأصل الفرد العرقي أو أصله الإثني، أو معتقده الديني أو الفكري أو السياسي، وكذلك البيانات الأمنية والجنائية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الصحية، أو البيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما"[13] .

---

[6] مادة (1)، نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19)، بتاريخ 1443/2/9هـ.
[7] اللائحة العامة لحماية البيانات (GDPR)، المادة (4)، 2016م، متاح على: المادة 4 لائحة حماية البيانات العامة – (GDPR) التعريفات - التنظيم العام لحماية البيانات(GDPR) ، تاريخ الدخول: 22 أبريل 2026م.
[8] المادة (1)، قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020م.
[9] المادة (2)، قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023م.
[10] المادة (1)، القانون الاتحادي الاماراتي رقم (45) لسنة 2021م، بشأن حماية البيانات الشخصية.
[11] المادة (1)، المرسوم السلطاني رقم (2022/6) بإصدار قانون حماية البيانات الشخصية، 2022م.
[12] لائحة حماية خصوصية البيانات الكويتية، الهيئة العامة للاتصالات وتقنية المعلومات، 2021م، متاح على: لائحة حماية خصوصية البيانات pdf.، تاريخ الدخول: 22 أبريل 2026م.
[13] المادة (1)، نظام حماية البيانات الشخصية.

وتعد من البيانات الحساسة البيانات الوراثية، وهي البيانات الشخصية المتعلقة بالخصائص الوراثية أو المكتسبة للفرد، والتي تحدد الخصائص الفيسيولوجية أو الصحية له، والناتجة عن تحليل عينة بيولوجية، كتحليل الأحماض النووية أو تحليل أي عينة أخرى تؤدي إلى استخلاص بيانات وراثية[14]، بالإضافة للبيانات الصحية، وهي البيانات الشخصية المتعلقة بحالة الفرد الصحية، سواء الجسدية أو العقلية أو النفسية أو المتعلقة بالخدمات الصحية الخاصة به[15]، وتعد من البيانات الصحية التاريخ الطبي، والتقارير الطبية، وتدخل ضمن البيانات الحساسة أيضًا البيانات التي تفصح عن الأصل العرقي أو المعتقد الديني أو الفكري أو السياسي للفرد، وكذلك البيانات الأمنية أو الجنائية.

وأولت التشريعات البيانات الحساسة اهتمامًا أكبر؛ نظرًا لطبيعتها الخاصة التي تتطلب حماية أشد، فالكشف عنها أو انتهاكها قد يؤدي بأضرار جسيمة بالفرد، والتمييز بين أنواع البيانات يعود لاختلافها عن بعضها من حيث طبيعة البيانات، فالبيانات الحساسة تتعلق بالخصائص والسمات الشخصية العميقة، مثل البيانات الوراثية والبيانات الصحية والبيانات الجنائية التي تتطلب حماية مشددة مقارنةً بالبيانات العادية[16].

ويلاحظ أن تعريف البيانات الحساسة الوارد في النظام لم يشمل البيانات الائتمانية، والتي عرّفها النظام بأنها كل بيان شخصي يتعلق بطلب الفرد للحصول على تمويل، أو حصوله على التمويل، سواء لغرض عائلي أو لغرض شخصي، من جهة ممارسة للتمويل، وبما في ذلك البيانات المتعلقة بقدرته على الحصول على ائتمان أو قدرته على الوفاء به أو متعلقة بتاريخه الائتماني[17]، بالرغم من حساسيتها وبالرغم من أنه أرسى قواعد خاصة بمعالجتها[18].

الفرع الثاني: البيانات الشخصية للعامل:

تعد حماية البيانات الشخصية للعامل من المسائل القانونية المهمة، والتي يجب أخذها بعين الاعتبار ومراعاتها بدقة في بيئة العمل، والبيانات الشخصية للعامل هي كل معلومة تتعلق بشخصه، وتحدد هويته، أو تُمكن من التعرف عليه بشكل مباشر أو غير مباشر، والتي ترتبط ببياناته التاريخية والفكرية، وحالته الصحية، وبياناته الائتمانية، والبيانات التي تستخدم في بيئة العمل لأغراض إجرائية وتنظيمية ومهنية[19].

ونظام العمل في المادة (17)، وضع التزام على صاحب العمل بأن يحتفظ في مكان العمل بالسجلات والكشوف والملفات والبيانات التي بينتها اللائحة[20]، والتي شملت كشف بأسماء العمال، يحتوي على بياناتهم الشخصية، بالإضافة لكشف أجور العمال، وسجل قيد الغرامات، وسجلات الحضور والانصراف، وسجلات الفحوص الطبية إن وجدت[21]، وهذه البيانات بطبيعتها تدخل في مفهوم البيانات الشخصية للعامل، ومنها ما يعد بيانات حساسة، وبالمقابل وضع المنظم التزامًا على صاحب العمل بالمحافظة على سرية هذه البيانات، وبأن لا يستغل أي معلومات شخصية للعامل دون إذنه.

وللعامل بوصفه صاحب بيانات حقوق تجاه بياناته، نظّمها نظام حماية البيانات الشخصية[22] والتي تكفل له حماية بياناته الشخصية، والمتمثلة في:

أ- **الحق في العلم:**

ويقصد به حق العامل بأن يُبلغ بالغرض من جمع بياناته، والمسوغ النظامي لجمعها، ويجب على جهة العمل بوصفها جهة التحكم أن تتخذ التدابير اللازمة لإبلاغ العامل ببيانات التواصل لغرض التواصل المرتبط بحماية البيانات، وبيانات الاتصال بالمسؤول عن حماية البيانات في الجهة، وإبلاغه بالغرض من جمع ومعالجة معلوماته بشكل صريح وواضح، وبمدة الاحتفاظ

---

[14] المادة (1)، نظام حماية البيانات الشخصية.
[15] المادة (1)، نظام حماية البيانات الشخصية.
[16] الخزيمي، وليد عبد الله علي، وبن صغير، مراد، نظرات حول الحماية المدنية للبيانات الشخصية الحساسة للعامل "دراسة في التشريع الإماراتي، مجلة جامعة الشارقة للعلوم القانونية، الإمارات العربية المتحدة، المجلد (22)، العدد (2)، 2024م، ص339.
[17] المادة (1)، نظام حماية البيانات الشخصية.
[18] المادة (24)، نظام حماية البيانات الشخصية.
[19] الخزيمي، الرجع السابق، ص 336.
[20] المادة (17)، نظام العمل.
[21] المادة (5)، اللائحة التنفيذية لنظام العمل، الصادرة بقرار وزير العمل رقم 1/693، بتاريخ 2/29/ 1428هـ.
[22] المادة (4)، نظام حماية البيانات الشخصية.

ببياناته، وعليها توضيح حقوقه له، وكيفية العدول عن موافقته الممنوحة لمعالجة بياناته، بالإضافة لالتزام الجهة ببيان إن كان جمع أي بيان إلزامي أو اختياري[23].

ب- **الحق في الوصول:**

ويقصد به حق العامل بالوصول لبياناته الشخصية المتوفرة لدى جهة التحكم -جهة العمل-، ولكن يجوز لجهة التحكم أن تحدد هذا الحق بتحديد مدد لممارسته، كما يجوز لها تقييد هذا الحق في حال كان التقييد فيه حماية للعامل أو غيره[24]، ويجب عليها تقييد هذا الحق في ، في حال كان وصوله قد يمثل خطراً على الأمن، أو يسيء إلى سمعة المملكة، أو يتعارض مع مصالحها، أو أنه قد يؤثر على علاقات المملكة مع دولة أخرى، أو أنه قد يمنع من كشف جريمة أو يمس حقوق متهم في الحصول على محاكمة عادلة أو يؤثر في سلامة إجراءات جنائية قائمة، أو أنه قد يعرض سلامة فرد أو أفراد للخطر، أو في حال قد يترتب عليه انتهاك خصوصية فرد آخر غيره، أو إن كان وصوله يتعارض مع مصلحة ناقص أو عديم للأهلية[25].

ت- الحق في الحصول:

ويقصد به حق العامل في طلب الحصول على نسخة من بياناته المتوفرة لدى جهة العمل، بصيغة مقروءة وواضحة، على ألا يؤثر ذلك سلبًا على حقوق الغير، وعلى ألا يتضمن الإفصاح بيانات شخصية تحدد هوية شخص آخر[26].

ث- **الحق في طلب التصحيح:**

ويراد به حق العامل في طلب تصحيح بياناته الشخصية لدى جهة العمل في حال عدم صحتها، أو إتمامها، أو تحديثها، ولجهة العمل طلب المستندات أو الوثائق المؤيدة لطلبه متى ما لزم الأمر، على أن تتلفها بعد التحقق منها، وفي حال تصحيح البيانات، وجب على جهة العمل إشعار الجهات التي أُفصح لها عن البيانات سابقًا[27].

ج- **الحق في طلب الإتلاف:**

وهو حق العامل في طلب إتلاف بياناته الشخصية المتوفرة لدى جهة العمل متى ما انتهت الحاجة اليها، وفي هذه الحالة يجب على جهة العمل بوصفها جهة التحكم تنفيذ طلبه، وعليها اتخاذ كافة الإجراءات لإبلاغ الجهات والأشخاص الذين أُفصح لهم عن البيانات وطلب إتلافها[28]، ومع ذلك يجوز للجهة الاحتفاظ بالبيانات إذا تمت إزالة ما يؤدي لمعرفة صاحب البيانات على وجه التحديد[29].

وعلى جهة التحكم عند تلقيها طلب من العامل كصاحب بيانات متعلق بحقوقه أن تنفذ ذلك الطلب خلال (ثلاثين) يوم، إلا إن كان التنفيذ يتطلب جهدًا إضافيًا، فلها تمديد المدة بما لا يزيد عن (ثلاثين) يومًا إضافيًا، بشرط أن تبلغ العامل مسبقًا بالتمديد ومبرراته، وفي حال كان الطلب متكرر بشكل غير مبرر أو كان تنفيذه يتطلب جهد غير عادي، ففي هذه الحالة يحق لجهة التحكم عدم معالجة طلبه، على أن يُبلغ، وأن يكون الرفض مسببًا.[30]

المطلب الثاني: المعايير والمبادئ النظامية لمشروعية جمع ومعالجة بيانات العامل:

في بيئة العمل تمر بيانات العامل بعدة عمليات، تبدأ بجمعها عند التوظيف وإبرام عقد العمل، ثم تخضع هذه البيانات للمعالجة بهدف تحقيق أغراض مشروعة كإدارة العلاقة العمالية وللوفاء بالالتزامات الناشئة عن عقد العمل، ومن هذا المنطلق، أصبح من الضروري وضع ضوابط واضحة لجمع ومعالجة واستخدام هذه البيانات، ولبيان المعايير النظامية للجمع والمعالجة، يتطلب بيان المقصود بالجمع والمعالجة، وذلك على النحو الآتي:

---

[23] المادة (4)، اللائحة التنفيذية لنظام حماية البيانات الشخصية، الصادرة بتاريخ 2/19/ 1445هـ..
[24] المادة (1/9)، نظام حماية البيانات الشخصية.
[25] المادة (2/9)، نظام حماية البيانات الشخصية.
[26] المادة (6)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[27] المادة (7)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[28] المادة (8)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[29] المادة (18)، نظام حماية البيانات الشخصية.
[30] المادة (3)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.

الفرع الأول: ماهية الجمع والمعالجة:

أولًا: الجمع:

ويُقصد بعملية الجمع حصول جهة التحكم على البيانات الشخصية[31]، وفي سياق العمل، فيقصد بجمع البيانات الشخصية للعامل الحصول عليها بأي وسيلة كانت، إما بشكل مباشر من العامل بنفسه عن طريق النماذج الإلكترونية أو الورقية، أو بشكل غير مباشر عبر الجهات الأخرى، وذلك بقصد استعمالها لإتمام إجراءات التوظيف أو لإدارة العلاقة العمالية.

ثانيًا: المعالجة:

ويُقصد بالمعالجة أي عملية أو إجراء يتم على البيانات الشخصية، سواءً كان بوسائل يدوية أو باستخدام تقنيات آلية، ومن ذلك عمليات الجمع والتسجيل والحفظ والفهرسة والتخزين والتعديل والإفصاح والإتلاف والنقل وغيرها[32]، ويعد من سبيل المعالجة حفظ بيانات العامل وتخزينها في الملفات الوظيفية وفي أنظمة الموارد البشرية، واستخدامها في إدارة شؤون العامل كصرف الأجور وتنظيم الحضور والانصراف وتقييم الأداء، بالإضافة لتنظيمها وتحليلها لإعداد التقارير الإدارية، وصولًا لإتلافها عند انتهاء الغرض منها، ويتضح من ذلك أن المعالجة لا تقتصر على إجراء محدد، بل تشمل جميع الإجراءات التي ترد على البيانات الشخصية منذ جمعها وحتى إتلافها.

والمعالجة قد تتم بواسطة جهة العمل بوصفها جهة التحكم، أو بواسطة جهة أخرى تسمى جهة المعالجة، والتي قد تكون جهة عامة، أو أي شخصية ذات صفة طبيعية أو اعتبارية، تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها، وبذلك يمكن القول أن حماية البيانات الشخصية للعامل أثناء المعالجة ترتبط بفئتين من حيث الأشخاص، العامل صاحب البيانات (الدائن بالحماية)، وجهة التحكم أو جهة المعالجة أو مسؤول حماية البيانات[33] (المدين بالحماية)[34].

الفرع الثاني: المعايير والمبادئ النظامية لمشروعية الجمع والمعالجة:

على الرغم من أن عملية الجمع تُعد من صور المعالجة في مفهومها الواسع، إلا أننا نفصل معايير جمع البيانات عن معايير معالجتها، نظرًا لاختلاف المعايير المنظمة لهما، بوصف الجمع المرحلة الأولى في التعامل مع البيانات، وذلك على النحو الآتي:

أولًا: معايير جمع البيانات:

تخضع عملية جمع البيانات الشخصية للعامل لعدة معايير وضوابط تهدف لتنظيم عملية الجمع وضمان مشروعية التعامل مع البيانات، وفي بيئة العمل، تبدأ عملية جمع البيانات الشخصية للعامل من قبل مرحلة ابرام العقد، حيث يتم الحصول على البيانات عندما يقوم العامل بتعبئة النماذج وتقديم المستندات اللازمة، بهدف التحقق من ملائمته للوظيفة.

وأول هذه المعايير جمع البيانات من مصدرها الصحيح، أي من العامل بنفسه أو من الجهات المخولة نظامًا عند الحاجة، وأن يكون الجمع لغرض محدد، أي أن يكون الغرض من جمع البيانات الشخصية ذا علاقة مباشرة بأغراض جهة التحكم كأن يكون مرتبط بإجراءات التوظيف أو بإدارة المواد البشرية.

ومن أهم المعايير أيضًا مبدأ الحد الأدنى من البيانات، أي أن يكون محتوى البيانات مقصورًا على الحد الأدنى اللازم لتحقيق الغرض من جمعها، وان يرتبط ارتباط وثيق ومباشر بالغرض منها، دون طلب معلومات لا ترتبط بطبيعة العمل أو حاجته الفعلية[35].

---

[31] المادة (1)، نظام حماية البيانات الشخصية.
[32] المادة (1)، نظام حماية البيانات الشخصية.
[33] مسؤول حماية البيانات: وهو شخص تعينه جهة التحكم ليكون مسؤولًا عن حماية البيانات الشخصية، قد يكون موظفًا لديها أو متعاقد خارجي، يتولى متابعة تنفيذ أحكام النظام ولوائحه ومراقبة الإجراءات والإشراف عليها داخل الجهة، وغيرها من المهام. / للمزيد حول ذلك، انظر: المادة (32)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[34] للمزيد حول ذلك، انظر: الخزيمي، المرجع السابق، ص340.
[35] المادة (19)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.

ويلي ذلك مبدأ الشفافية، ومقتضاه أن يتم جمع البيانات بعلم العامل وإخطاره بطبيعة البيانات التي يتم جمعها والغرض منها وكيفية استخدامها داخل جهة العمل، بالإضافة لاستخدام الوسائل المشروعة في جمع البيانات، بحيث يتم الحصول على البيانات عبر قنوات نظامية موثوقة، دون استخدام وسائل مظللة.

وبعد إتمام العقد وخلال قيام العلاقة العمالية، قد تستمر عملية الجمع، كالحالات التي تتطلب تحديث المعلومات الشخصية، أو استكمال البيانات الوظيفية، على أن يتم ذلك وفق نفس المعايير وبالقدر اللازم لإدارة العلاقة العمالية دون التوسع غير المبرر في جمع البيانات.

ثانيًا: معايير معالجة البيانات:

في بيئة العمل، تبدأ مرحلة معالجة البيانات الشخصية للعامل منذ لحظة جمعها، حيث أنها تخضع لعدة عمليات وإجراءات كالحفظ والاستخدام والتحديث والمشاركة وغيرها، وهذا الأمر يستلزم التقييد بمعايير تضمن حماية البيانات وتنظيم التعامل معها.

ومن أهم هذه المعايير الحصول على موافقة العامل، فلا تجوز معالجة البيانات الشخصية أو تغيير الغرض من معالجتها إلا بعد موافقة صاحبها إلا في أحوال معينة حددها النظام، والموافقة يصح أن تكون بأي شكل أو وسيلة ملائمة، فقد تكون كتابية، أو شفوية، ويشترط أن تكون صادرة عن إرادة حرة، وأن تبين للعامل أغراض المعالجة، وأن تكون موثقة بوسيلة تتيح التحقق منها مستقبلًا، بالإضافة لأن تكون هناك موافقة مستقلة لكل غرض من أغراض المعالجة[36].

وفي حال كانت البيانات الخاضعة للمعالجة تتضمن بيانات حساسة، فيشترط في الموافقة أن تكون موافقة صريحة[37]، وكذلك هو الحال إن تضمنت بيانات ائتمانية[38]، ويجوز للعامل الرجوع عن موافقته في أي وقت[39].

ويعد أيضًا من أسس المعالجة استخدام البيانات في حدود الغرض الذي جُمعت من أجله، دون التوسع في استعمالها وتوظيفها لأغراض أخرى إلا في أحوال معينة أجازها المنظم[40].

كما يجب عدم الإفصاح عن البيانات أو مشاركتها إلا مع جهة لها مبرر نظامي يقتضي ذلك، ويجب على جهة العمل إن كانت تنيب في المعالجة جهة معالجة أخرى، أن تلتزم باختيار جهة معالجة تقدم ضمانات كافية لحماية البيانات.

ويقترن بذلك ضرورة حماية البيانات وضمان سريتها وآمنها من خلال اتخاذ التدابير الكفيلة بمنع الوصول غير المصرح به أو تسريبها، وتحديد مدة الاحتفاظ بالبيانات، بحيث لا تستمر معالجتها لأكثر من الفترة اللازمة لتحقيق الغرض منها، وصولًا لإتلافها بعد الانتهاء الغرض منها وفق الضوابط التي حددها النظام، بما يحقق الحماية الفعالة لبيانات العامل.

المبحث الثاني: صور انتهاك بيانات العامل والآثار القانونية المترتبة عليها

وبعد التعريف بالبيانات الشخصية للعامل وبيان حقوقه كصاحب بيانات المنصوص عليها في نظام حماية البيانات في المبحث السابق، نقسم هذا المبحث لمطلبين، نستعرض صور انتهاك البيانات الشخصية للعامل في المطلب الأول، ونحدد المسؤولية القانونية المترتبة على انتهاك بيانات العامل الشخصية في المطلب الثاني، على النحو الآتي:

المطلب الأول: صور انتهاك بيانات العامل الشخصية:

تتبين خطورة التهديدات المعلوماتية في حال إساءة استعمالها، وتتعدد أشكال إساءة الاستعمال والاعتداءات التي قد تتعرض لها البيانات الشخصية بشكل عام بزيادة استعمال البيانات الشخصية في جميع جوانب الحياة ومع التطور الذي نعيشه في العصر الحالي والتقنيات المتجددة.

---

[36] المادة (1/11)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[37] الموافقة الصريحة: موافقة تمنح بشكل واضح وصريح من صاحب البيانات الشخصية بأي شكل من الأشكال وتدل على قبوله بمعالجة بياناته الشخصية بحيث لا يمكن تفسيرها بخلاف ذلك، وتكون قابلة للإثبات.
[38] المادة (2/11)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[39] المادة (5)، نظام حماية البيانات الشخصية.
[40] المادة (10)، نظام حماية البيانات الشخصية.

والمراد بالانتهاك التعدي على حق من حقوق صاحب البيانات الشخصية المنصوص عليها في النظام، أو معالجتها بأي صور المعالجة دون استيفاء شروط المعالجة، وبالتالي يتعرض فاعله للمسؤولية المدنية والجزائية بحسب نوع الانتهاك[41]، ويمكن تعريفه بأنه أي ممارسة تخالف المبادئ التي أقرها النظام لمعالجة البيانات، وفي هذا المطلب نهدف لبيان أبرز صور الانتهاك التي قد تتعرض لها بيانات العامل الشخصية.

الفرع الأول: انتهاكات مبادئ الجمع والمعالجة:

وهي التي تقع حين يتم جمع البيانات أو معالجتها دون مسوغ نظامي، أو استخدامها في غير الهدف الذي جمعت من أجله، ومن أبرز صورها:

أولًا: جمع ومعالجة البيانات دون الحصول على موافقة العامل:

والأصل نظامًا هو الحصول على موافقة صاحب البيانات على النحو الموضح في المبحث السابق قبل أي عملية معالجة للبيانات، وعلى سبيل المثال يقع الانتهاك في حال قيام صاحب العمل مثلًا برصد أراء العامل واهتماماته الشخصية دون أخذ موافقته الصريحة والمستقلة.

ثانيًا: انتهاك مبدأ الغرض:

أوجب النظام استخدام البيانات حصرًا للهدف الذي جمعت من أجله، فمثلًا يعد انتهاكًا استخدام المنشأة لأرقام هواتف موظفيها الشخصية لأغراض تخرج عن الغرض الأساسي من جمعها، كتزويد قسم التسويق بها لإرسال رسائل ترويجية لمنتجات المنشأة مثلًا، أو بيعها لجهات خارجية.

ثالثًا: انتهاك مبدأ الحد الأدنى:

ويقتضي هذا المبدأ الاكتفاء بالبيانات الضرورية لتحقيق الغرض منها، فيعد انتهاكًا مثلًا إلزام العامل بتعبئة نماذج تتضمن بيانات شخصية لا صلة لها بطبيعة الوظيفة ولا بالمهام الموكلة إليه، مثل طلب تفاصيل عن حالته المادية والديون الشخصية، أو طلب السجلات الطبية لأفراد عائلته، وهذا يعد تجاوز لمبدأ الضرورة والحد الأدنى. وبالمقابل لا يعد انتهاكًا أن يجمع صاحب العمل فصائل الدم الخاصة بموظفيه العاملين في الوظائف الميدانية التي تتضمن مواجهة بعض المخاطر وذلك للتعامل مع الحوادث بأسرع وقت مع العلم بوجود احتمالي كبير ألا يتم استخدام أي من هذه البيانات خلال فترة عمل هؤلاء الموظفين، ولكن جمعها وحفظها مهم لتقليص الأضرار الناتجة عن الحوادث[42].

رابعًا: انتهاك مبدأ محدودية التخزين:

حظر النظام على جهات التحكم أن تحتفظ بالبيانات بعد انتهاء الغرض من جمعها، وبذلك يعد الاحتفاظ بها انتهاكًا، ومثال ذلك احتفاظ المنشأة بصور وأرقام هويات العاملين الذين انتهت علاقتهم بالمنشأة لسنوات بعد انتهاء العلاقة المالية وتسوية كافة الحقوق دون مبرر نظامي لحفظها.

الفرع الثاني: انتهاكات حقوق صاحب البيانات:

وهي الانتهاكات التي تقع حين تمتنع المنشأة عن تمكين العامل من حقوقه كصاحب بيانات وسلطته على بياناته، حيث أوجب نظام حماية البيانات الشخصية على جهة التحكم الاستجابة لطلبات صاحب البيانات[43]، وبالتالي فإن امتناع المنشأة كجهة تحكم يعد مخالفة لأحكام النظام وانتهاك لحقوق العامل كصاحب البيانات التي كفلها له النظام، وتتمثل صور هذه الانتهاكات فيما يلي:

---

(41) الفارسية، العنود بنت إبراهيم بن عبيد، حقوق صاحب البيانات الشخصية ووسائل حمايتها وفقًا لقانون حماية البيانات الشخصية العماني، رسالة ماجستير، كلية الحقوق، جامعة السلطان قابوس، عمان، 2023م، ص107.

(42) الدليل الاسترشادي لتحديد الحد الأدنى من البيانات الشخصية، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، للمزيد الاطلاع على: MinmumPDGuidelineArabic.pdf ، تاريخ الدخول: 7 مايو 2026م.

(43) المادة (21)، نظام حماية البيانات الشخصية، والتي نصت على: " على جهة التحكم الاستجابة لطلبات صاحب البيانات الشخصية المتعلقة بحقوقه المنصوص عليها في النظام خلال مدة محددة وعبر وسيلة مناسبة تبينهما اللوائح"

أولًا: انتهاك حقه في العلم:

فللعامل الحق في العلم عن جمع بياناته كما ذكرنا سابقًا، فعلى سبيل المثال، يعد انتهاكًا قيام المنشأة بتركيب برمجيات تتبع على أجهزة الموظفين دون علمهم أو توضيح ذلك في سياسة الخصوصية[44] المتعلقة بالمنشأة.

ثانيًا: انتهاك حقه في الوصول:

يتمثل هذا الانتهاك في امتناع المنشأة عن تمكين العامل من الاطلاع على بياناته الشخصية الموجودة لديها، ويقع الانتهاك عندما تضع المنشأة عوائق إجرائية تمنع العامل من الوصول لبياناته، كمنع العامل من الاطلاع على تقييمه السنوي مثلًا.

ثالثًا: انتهاك حقه في الحصول:

ويقع الانتهاك هنا عندما تمتنع المنشأة عن تزويد العامل بنسخة واضحة ومقروءة من بياناته، أو أن تجعل حصوله عليها معقدًا، كأن تطالب برسوم مبالغ فيها مقابل تزويده ببياناته، أو أن تقدمها بصيغة تقنية معقدة يصعب فهمها.

رابعًا: انتهاك حقه في طلب التصحيح:

يجب على المنشأة تعديل أي بيانات غير دقيقة بناء على طلب صاحب البيانات، ويمكن تصور انتهاك هذا الحق في حال تقدم العامل بشهادات أكاديمية جديدة لتحديث مستواه العلمي في أنظمة المنشأة، ورفض المنشأة تعديل هذه البيانات مما يترتب عليه حرمانه من علاوة أو ترقية مستحقة بناء على مؤهله الجديد.

خامسًا: انتهاك حقه في طلب الاتلاف:

يحق للعامل طلب إتلافه بياناته عند انتفاء الحاجة إليها، ويصبح الإتلاف واجبًا على المنشأة كجهة تحكم، ومن صور انتهاك هذا الحق إصرار المنشأة على إبقاء صورة العامل واسمه على موقعها الإلكتروني العام بعد استقالته رغم طلبة الصريح بحذفها رغبة منه في الخصوصية عند انتقاله لجهة منافسة[45].

الفرع الثالث: انتهاكات أمن البيانات:

وهي الانتهاكات التي تقع نتيجة الإخلال بواجبات الحماية والخصوصية، ومن أبرز صورها:

أولًا: التقصير في التدابير الأمنية:

ألزم نظام حماية البيانات الشخصية جهات التحكم باتخاذ التدابير الأمنية اللازمة لحماية البيانات الشخصية، منها تدابير تنظيمية، وتدابير تقنية، وتدابير إدارية[46]، منها:

1. **التدابير التنظيمية:**

وهي الأطر التي تعتمدها المنشأة لتكفل وجود منهجية وآلية منظمة لحماية البيانات، كإيجادها سياسة الخصوصية وهي سياسة داخلية مكتوبة بهدف حماية البيانات الشخصية، تحدد من خلالها كيفية معالجة البيانات، وتوضح فيها الأدوار والمسؤوليات وطرق تقديم الشكاوى والاعتراضات[47].

---

[44] الزم المنظم جهات التحكم أن تعتمد سياسة للخصوصية داخل المنشأة، وذلك وفقًا للمادة (12) من نظام حماية البيانات الشخصية، والتي عُدلت بموجب المرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، لتكون بالنص الآتي: " على جهة التحكم أن تعتمد سياسة للخصوصية، وأن تجعلها متاحة لأصحاب البيانات الشخصية ليطلعوا عليها عند جمع بياناتهم. على أن تشتمل تلك السياسة على تحديد الغرض من جمعها، ومُحتوى البيانات الشخصية المطلوب جمعها، وطريقة جمعها، ووسيلة حفظها، وكيفية معالجتها، وكيفية إتلافها، وحقوق صاحبها فيما يتعلق بها، وكيفية ممارسة هذه الحقوق"، للمزيد الاطلاع على: PrivacyPolicyGuidelineArabic.pdf ، تاريخ الدخول: 7 مايو 2026م.

[45] أصدرت الهيئة السعودية للبيانات والذكاء الاصطناعي دليل استرشادي لإتلاف البيانات الشخصية وإخفاء الهوية والترميز، بهدف دعم الجهات على تطبيق النظام وحفاظًا على خصوصية أصحاب البيانات، للمزيد الاطلاع على: PersonalDataDestructionAnonymizationAndPseudonymisationGuidelineAR.pdf تاريخ الدخول: 8 مايو 2026م.

[46] المادة (19)، نظام حماية البيانات الشخصية، والتي نصت على: " على جهة التحكم اتخاذ ما يلزم من إجراءات ووسائل تنظيمية وإدارية وتقنية تضمن المحافظة على البيانات الشخصية...".

ومن التدابير التنظيمية أيضًا تصنيف البيانات، ويعرف التصنيف بأنه تحليل البيانات بعد جمعها لمجموعات حسب درجة خطورتها[48]، بحيث يتم تصنيف البيانات إلى مستويات وفقًا لطبيعتها، ومستوى حساسيتها[49]، ويتم وفق مبادئ وضوابط حددتها سياسة تصنيف البيانات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي، لتمكين الجهات من توفير الحماية اللازمة لها.

بالإضافة لذلك وبالرغم من أن النظام لم يحدد فترة زمنية محددة للاحتفاظ بالبيانات، ولكن كما ذكرنا سابقًا انه من ضوابط المعالجة تحديد مدة الاحتفاظ بالبيانات واتلافها بعد انتهاء الغرض منها، وتنفيذ ذلك يستوجب تحديد فترات الاستبقاء والاتلاف داخل المنشأة من خلال وضع جدول زمني محدد لحفظ البيانات واتخاذ إجراءات الاتلاف بشكل آمن وامتثالًا للسياسات الصادرة عن الهيئة بعد انتهاء الغرض منها.

2. التدابير التقنية:

ومن التدابير التقنية التحكم في الوصول للبيانات، بتطبيق مبدأ الحد الأدنى من الصلاحيات، بحيث لا يتمكن من الاطلاع على البيانات الخاصة بالعاملين إلا من تتطلب طبيعة عمله ذلك.

بالإضافة لذلك يعد من التدابير الأمنية التقنية الترميز[50]، وإخفاء الهوية[51]، لإخفاء هويات العاملين عند إجراء الدراسات الإحصائية أو التحليلية داخل المنشآت، والبيانات المرمزة تبقى بيانات شخصية خاضعة للحماية، لبقاء إمكانية تحديد هوية صاحبها، بينما البيانات التي جرى إخفاء هوية أصحابها تخرج من نطاق البيانات الشخصية المحمية[52]، ويتم الترميز وإخفاء الهوية بعدة طرق وتقنيات وأساليب، كالتشفير والإخفاء والتعميم وغيرها.

3. التدابير الإدارية:

وهي التدابير المتعلقة بالعنصر البشري الذي يتعامل مع البيانات، ويعد من التدابير الإدارية التوعية والتدريب، بحيث يتم تدريب العاملين الذين تسمح طبيعة مهامهم بالتعامل مع البيانات الشخصية للعاملين في المنشأة على الطرق الآمنة للتعامل مع البيانات.

بالإضافة إلى إضافة شرط عدم الإفصاح لعقود العاملين الذين يتمتعون بصلاحية الوصول للبيانات، وعدم الإفصاح يشمل الأسرار الفنية والتجارية والصناعية وجميع الأسرار المهنية التي تتعلق بالعمل والمنشأة ما دامت سرية[53]، وهذا ما ينطبق على البيانات الشخصية.

ثانيًا: الإفشاء والإفصاح غير النظامي:

ويُقصد به كشف البيانات الشخصية بواسطة الأشخاص المسؤولين عنها[54] ، ويعد هذا الانتهاك من أخطر صور التعدي على خصوصية العامل، ويتحقق بتمكين أي شخص أو جهة غير مصرح لها من الاطلاع على البيانات الشخصية أو الحصول عليها

---

(47) الدليل الاسترشادي لإعداد وتطوير سياسة الخصوصية، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، للمزيد الاطلاع على: PrivacyPolicyGuidelineArabic.pdf تاريخ الدخول: 8 مايو 2026م.

(48) الفارسية، مرجع سابق، ص 117.

(49) سياسات حوكمة البيانات الوطنية، سياسة تصنيف البيانات، الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي، بتاريخ 2020/5/5م، للمزيد الاطلاع على: سياسة وضوابط تصنيف البيانات ، تاريخ الدخول: 8 مايو 2026م.

(50) الترميز: وهو تحويل المعرفات الرئيسية التي تدل على هوية صاحب البيانات الشخصية إلى رموز تجعل من المتعذر تحديد هوية صاحب البيانات الشخصية بشكل مباشر دون استخدام بيانات أو معلومات إضافية، وأن يتم الاحتفاظ بتلك البيانات والمعلومات الإضافية بشكل منفصل ووضع الضوابط الفنية والإدارية اللازمة لضمان عدم ربطها بصاحب البيانات الشخصية بشكل محدد.

(51) إخفاء الهوية: ويقصد به إزالة المعرفات المباشرة وغير المباشرة لصاحب البيانات الشخصية، بطريقة تجعل من المتعذر تحديد هوية صاحبها.

(52) الدليل الاسترشادي لإتلاف البيانات الشخصية وإخفاء الهوية والترميز، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، للمزيد الاطلاع على: PersonalDataDestructionAnonymizationAndPseudonymisationGuidelineAR.pdf ، تاريخ الدخول 8 مايو 2026م.

(53) الدهيمي، علي بن إبراهيم بن عبدالله، التزام العامل بالمحافظة على الأسرار بعد انتهاء عقد العمل وفقاً لأحكام نظام العمل في المملكة العربية السعودية: دراسة مقارنة، مجلة جامعة الملك سعود – الحقوق والعلوم السياسية، المملكة العربية السعودية، المجلد (37)، العدد (2)، 2025م، ص280.

(54) عتوم، علي محمد علي، المسؤولية الجزائية للشخص المعنوي عن انتهاك البيانات الشخصية في ظل تقنيات الذكاء الاصطناعي، رسالة ماجستير، كلية الحقوق، جامعة عمان الأهلية، الأردن، 2024م، ص 37.

سواء تم بطريقة مباشرة أو غير مباشرة، وفي بيئة العمل قد لا يقتصر الإفصاح على بيع البيانات أو تسليمها لجهات خارجية فحسب، بل يشمل الإفشاء الداخلي كأن يتم تداول تقارير العامل الصحية أو بياناته الائتمانية بين عمال آخرون لا تتطلب طبيعة عملهم الاطلاع على هذه المعلومات.

وقد وضع المنظم السعودي ضوابط صارمة حظر بموجبها الإفصاح عن البيانات إلا في حالات محددة، وبناء على ذلك فإن أي إفشاء يتجاوز هذه الحالات يعد انتهاكًا وخطأ موجب للمسؤولية النظامية[55].

ثالثًا: تسرب البيانات وعدم الإبلاغ عنه:

عرّفت اللائحة التنفيذية لنظام حماية البيانات الشخصية تسرب البيانات الشخصية بأنه: "أي حادثة تؤدي إلى الإفصاح عن البيانات الشخصية أو تلفها أو الوصول غير المشروع إليها، سواءً كان ذلك بقصد أو بغير قصد، وبأي وسيلة كانت سواءً آلية أو يدوية"[56]، وأوجب النظام على جهة التحكم إشعار الجهات المختصة عند علمها بحدوث التسرب، وأوجب عليها أن تشعر صاحب البيانات أيضًا إن كان هذا التسرب قد يؤدي للإضرار ببياناته، أو يتعارض مع حقوقه ومصالحه[57].

والتزام المنشأة هنا يعتبر التزام مزدوج، فهي ملزمة بمنع التسرب عبر اتخاذ التدابير السابق ذكرها، ومن جهة أخرى فهي ملزمة بالشفافية في حال وقع التسرب بإشعار الجهات المختصة خلال (72) ساعة من وقت علمها بالحادثة إذا كان من شأنها الإضرار بالبيانات الشخصية، أو بالعامل بوصفه صاحب البيانات، أو كانت تتعارض مع حقوقه ومصالحه، بالإضافة لإبلاغ العامل بذلك[58] .

المطلب الثاني: الآثار القانونية المترتبة على انتهاك بيانات العامل الشخصية:

إن إقرار الالتزامات والتدابير التنظيمية والتقنية لحماية البيانات التي بيّناها في المطلب السابق لا يكون لها قيمة إن لم تقترن بجزاءات رادعة تضمن امتثال المسؤولين بها، وتجبر الضرر الناتج عن الانتهاكات، لذا فإن المنظم السعودي لم يكتف بفرض الالتزامات، بل أرسى ووضع إطار متكامل للمسؤولية القانونية.

وهذا ما سيتم استعراضه في هذا المطلب من خلال ثلاثة فروع، نتناول المسؤولية الجنائية في الفرع الأول، والمسؤولية الإدارية في الفرع الثاني، والمسؤولية المدنية في الفرع الثالث.

الفرع الأول: المسؤولية الجنائية:

تعد السياسة الجنائية من الوسائل التي يعتمد عليها المنظم للحد من الجرائم من خلال تقرير العقوبات والتدابير الاحترازية المناسبة، وتقوم هذه السياسة على مجموعة من المبادئ التي تنظم تحديد العقوبة وتطبيقها وتنفيذها باعتبار ان التجريم وحده لا يحقق الردع ما لم يقترن بجزاء نظامي، وذلك ما اخذ به المنظم السعودي من خلال إقرار عقوبات والمتمثلة في السجن والغرامة أو أحدهما، بالإضافة لمساءلة الأشخاص الاعتباريين عند تحقق السلوك الإجرامي، وبالإضافة لتشديد الجزاء الجنائي في حال العَود[59].

ونُظمت العقوبات الجنائية في النظام السعودي لحماية البيانات الشخصية في المادة (35) من النظام، والتي جاءت مقررة لعقوبات تشمل السجن والغرامة أو أحدهما في حال ثبوت السلوك الإجرامي والمتمثل في الإفصاح عن البيانات الحساسة أو نشرها بطريقة مخالفة لأحكام النظام، واشترط أن يكون ذلك مقترنًا بقصد الإضرار بصاحب البيانات، أو بقصد تحقيق منفعة شخصية[60]، وأسند المنظم الاختصاص بمهمة التحقيق والادعاء أمام المحكمة المختصة في هذه المخالفة للنيابة العامة[61]

---

[55] المادة (15)، نظام حماية البيانات الشخصية.
[56] المادة (1)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[57] المادة (20)، نظام حماية البيانات الشخصية.
[58] المادة (24)، اللائحة التنفيذية لنظام حماية البيانات الشخصية.
[59] الجعيد، صالح عوض منصور، الحماية الجزائية لمعالجة البيانات الشخصية في النظام السعودي (دراسة مقارنة)، مجلة الأندلس للعلوم الإنسانية والاجتماعية، اليمن، المجلد (114)، العدد (12)، 2025م، ص165.
[60] المادة (1/35)، نظام حماية البيانات الشخصية، وعُدلت هذه المادة بموجب المرسوم الملكي رقم (م/148) وتاريخ 5/9/1444هـ، لتكون بالنص الآتي: "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في نظام آخر، يُعاقب بالسجن مدة لا تزيد على (سنتين) وبغرامة لا تزيد على (ثلاثة ملايين)

وبذلك يمكن القول أن المنظم حصر المسؤولية الجنائية لضمان فاعلية الردع في الحالات الأكثر خطورة وهي حالة الإفصاح عن البيانات الحساسة أو نشرها بطريقة تخالف أحكام النظام، واشترط لإيقاع العقوبة توافر الأركان التالية:

1- محل الجناية: أن يقع الانتهاك على بيانات حساسة كالسجلات الطبية أو البيانات الحيوية وغيرها، وهذا ما يضاعف من جسامة الضرر المحتمل وقوعه على صاحب البيانات.

2- الركن المادي: والمتمثل في السلوك الإجرامي ويتحقق بقيام الجاني بالإفصاح عن البيانات الحساسة، أو نشرها بما يخالف ضوابط النظام، ويقصد بالإفصاح تمكين أي شخص من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة كانت ولأي غرض، ويقصد بالنشر بث البيانات الشخصية عبر وسيلة نشر سواءً كانت وسيلة مقروءة أو مسموعة أو مرئية، أو إتاحتها[62].

3- الركن المعنوي: وهو جوهر المسؤولية الجنائية حيث اشترط النظام أن يكون الإفصاح مقترنًا بقصد الإضرار بصاحب البيانات -العامل- أو بقصد تحقيق منفعة شخصية.

وبناء على ذلك، يتضح أن المنظم لا يهدف لتجريم الخطأ التقني المجرد، بل يهدف لمكافحة الاستغلال وسوء الاستعمال للبيانات، وفي سياق العمل فإن هذا الهدف يعزز وجود بيئة عمل آمنة، ويمنع استخدام المعلومات الشخصية كوسيلة للضغط أو الانتقام أو الكسب غير المشروع.

وحدد المنظم الحد الأقصى لعقوبة السجن بحيث لا تزيد المدة عن (سنتين)، والحد الأقصى للغرامة بحيث لا تزيد عن (3ملايين ريال)، وأجاز للمحكمة المختصة مضاعفة عقوبة الغرامة في حال العود وإن ترتب على ذلك تجاوزها للحد الأقصى، على ألا تتجاوز ضعف الحد[63].

بالإضافة إلى أن المنظم أجاز للمحكمة أن تحكم بمصادرة الأموال المتحصلة عن ارتكاب المخالفة -مع مراعاة حقوق الغير حسن النية-[64]، وأجاز لها أن تضمن الحكم الصادر عنها النص على نشر ملخص الحكم بعد اكتسابه صفة القطعية، ويكون ذلك على نفقة المحكوم عليه في صحيفة محلية أو أكثر تصدر في مكان إقامته أو أي وسيلة أخرى مناسبة[65].

الفرع الثاني: المسؤولية الإدارية:

جاءت المادة (36) من نظام حماية البيانات الشخصية كقاعدة عامة لكل مخالفة أخرى لأحكام النظام لم يرد بشأنها نص خاص في المادة (35)، فإن صدر عن أي شخصية ذات صفة طبيعية أو اعتبارية خاصة -مشمولة بأحكام النظام -مخالفة لأي من أحكام النظام أو اللوائح كمعالجة البيانات بطريقة مخالفة، فإنها تُعاقب بالإنذار أو بغرامة لا تزيد على (خمسة ملايين) ريال، وتجوز مضاعفة عقوبة الغرامة في حالة تكرار المخالفة، حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد[66].

ريال، أو بإحدى هاتين العقوبتين؛ كل من أفصح عن بيانات حساسة أو نشرها مخالفاً أحكام النظام إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية".

(61) المادة (2/35)، نظام حماية البيانات الشخصية

(62) المادة (1)، نظام حماية البيانات الشخصية.

(63) المادة (4/35)، نظام حماية البيانات الشخصية، والتي نصت على: "يجوز للمحكمة المختصة مضاعفة عقوبة الغرامة المنصوص عليها في الفقرة (1) من هذه المادة في حالة العود حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد."

(64) المادة (1/38)، نظام حماية البيانات الشخصية.

(65) المادة (2/38)، نظام حماية البيانات الشخصية.

(66) المادة (1/36)، نظام حماية البيانات الشخصية، والتي نصت على: "فيما لم يرد في شأنه نص خاص في المادة (الخامسة والثلاثين) من النظام، ودون إخلال بأيّ عقوبة أشد منصوص عليها في نظام آخر؛ تُعاقَب بالإنذار أو بغرامة لا تزيد على (خمسة ملايين) ريال، كلُّ شخصية ذات صفة طبيعية أو اعتبارية خاصة -مشمولة بأحكام النظام- خالفت أيًّا من أحكام النظام أو اللوائح. وتجوز مضاعفة عقوبة الغرامة في حالة تكرار المخالفة حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد".

وتتولى النظر في المخالفات وإيقاع العقوبات لجان مختصة، وهي لجان النظر في مخالفات أحكام نظام حماية البيانات الشخصية ولوائحه، تكوّن هذه اللجان بقرار من رئيس الجهة المختصة وهي الهيئة السعودية للبيانات والذكاء الاصطناعي، ويكون إيقاع العقوبة بحسب نوع المخالفة المرتكبة ومدى تأثيرها[67].

بالإضافة للعقوبات الواردة في المادة، فإنه يجوز للجنة أن تضمن القرار الصادر منها بتحديد العقوبة بالنص على نشر ملخص القرار، ويكون ذلك على نفقة المخالف في صحيفة محلية أو أكثر تصدر في مكان إقامته أو أي وسيلة أخرى مناسبة، بحسب نوع المخالفة ومدى تأثيرها[68].

الفرع الثالث: المسؤولية المدنية:

المسؤولية المدنية تعد الوسيلة القانونية لحماية الأفراد من الأضرار الناتجة عن أفعال الغير، إذ أنها تلزم المتسبب بالضرر بتعويض المتضرر، وينطبق ذلك على انتهاك البيانات الشخصية للعامل أو إفشائها بشكل غير مشروع مما يوجب مساءلة المتسبب مدنيًا، وفي نظام حماية البيانات الشخصية، ورد في نص المادة (40) أن لمن لحقه ضرر ناتج عن ارتكاب أي مخالفة منصوص عليها في النظام أو اللائحة حق المطالبة أمام المحكمة المختصة بالتعويض عن الضرر المادي أو الضرر المعنوي بما يتناسب مع حجم الضرر[69].

وبإحالة تنظيم المسؤولية المدنية للقواعد العامة في قانون المعاملات المدنية، والتي تنقسم إلى مسؤولية عقدية، ومسؤولية تقصيرية، فإننا نتناولها على النحو الآتي:

1- المسؤولية العقدية:

وكما هو معلوم ينشأ عن عقد العمل التزامات متبادلة بين العامل وصاحب العمل، ومن الالتزامات المفروضة على صاحب العمل احتفاظه بملفات وسجلات العمال والتي تحتوي على بياناتهم، والتزامه بعدم استغلال أي معلومات شخصية للعامل دون إذنه وأن يتخذ كافةً الطرق والتدابير اللازمة للحفاظ عليها، وبذلك إن قام صاحب العمل بمخالفة ذلك بانتهاك بيانات العامل، فإن هذا يوجب عليه قيام المسؤولية العقدية وذلك لتوفر أركانها بالإخلال بالالتزام التعاقدي بالإضافة للضرر المادي أو المعنوي الذي لحق بالعامل.

ولكون التزام صاحب العمل هنا يعد التزام بتحقيق نتيجة، فمتى ما تم الاخلال به وترتب على ذلك حصول ضرر للعامل، انعقدت مسؤولية صاحب العمل، ما لم يثبت أن مصدر الضرر يعود لسبب أجنبي، كخطأ العامل نفسه، أو خطأ الغير، أو بسبب قوة قاهرة.

2- المسؤولية عن الفعل الضار:

لا تنطبق أركان قيام المسؤولية العقدية إن كان المتسبب بالضرر طرف آخر خارج العقد، ولكن بالرغم من ذلك فإن أي تعد على البيانات يوجب المسؤولية عن الفعل الضار، بتوافر الأركان الثلاثة والمتمثلة في الفعل الضار، والضرر، والعلاقة السببية[70].

الخاتمة

تناولت الدراسة موضوع الحماية القانونية لبيانات العامل الشخصية في النظام السعودي، وقد سعت الدراسة إلى بيان الحماية القانونية من خلال تحليل النصوص القانونية ذات العلاقة، وذلك من خلال توضيح المقصود ببيانات العامل الشخصية وبيان حقوقه على بياناته، وأبرز المبادئ والمعايير التي وضعها النظام لضمان مشروعية الجمع والمعالجة، ومن ثم بيان أبرز صور انتهاك البيانات، وأخيرًا بيان الآثار القانونية المترتبة على انتهاك البيانات الشخصية.

---

[67] قواعد عمل لجان النظر في مخالفة أحكام نظام حماية البيانات الشخصية ولوائحه، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، متاح على: CommitteeWorkingRules.pdf ، تاريخ الدخول: 10 مايو 2026م.

[68] المادة (2/38)، نظام حماية البيانات الشخصية.

[69] المادة (40)، نظام حماية البيانات الشخصية.

[70] الخزيمي، مرجع سابق، ص 350-355.

وقد توصلت الدراسة إلى عدد من النتائج والتوصيات، وهي كالتالي:

النتائج:

- أن البيانات الشخصية للعامل هي كل معلومة تتعلق بشخصه، وتحدد هويته، أو تُمكن من التعرف عليه بشكل مباشر أو غير مباشر، والتي ترتبط ببياناته التاريخية والفكرية، وحالته الصحية، وبياناته الائتمانية، والبيانات التي تستخدم في بيئة العمل لأغراض إجرائية وتنظيمية ومهنية.
- للعامل بوصفه صاحب بيانات حقوق تجاه بياناته نظّمها نظام حماية البيانات الشخصية، والمتمثلة في حقه في العلم، وحقه في الوصول، وحقه في الحصول، وحقه في طلب التصحيح، وحقه في طلب الإتلاف.
- حماية البيانات الشخصية للعامل أثناء المعالجة ترتبط بفئتين من حيث الأشخاص، العامل صاحب البيانات (الدائن بالحماية)، وجهة التحكم أو جهة المعالجة أو مسؤول حماية البيانات (المدين بالحماية).
- استطاع المنظم الموازنة بين حق صاحب العمل في إدارة منشأته ومعرفة بيانات العاملين لديه وبين حق العامل في الخصوصية عبر فرض الضوابط والالتزامات التي تحمي بيانات العامل الشخصية.
- من أبرز المعايير والمبادئ التي وضعها النظام لضمان مشروعية الجمع والمعالجة، اشتراط موافقة العامل، ومبدأ الغرض، ومبدأ الحد الأدنى، ومبدأ الشفافية، ومبدأ عدم الإفصاح.
- تتنوع صور انتهاك البيانات الشخصية للعامل بين انتهاكات مبادئ الجمع والمعالجة، وانتهاك حقوق العامل كصاحب بيانات، بالإضافة لانتهاكات تمس آمن البيانات.
- يترتب على انتهاك بيانات العامل قيام المسؤولية الجنائية، والمسؤولية الإدارية، بالإضافة لحق العامل في طلب التعويض عن الأضرار المادية والمعنوية التي اصابته نتيجة ذلك.
- أن المنظم فرّق بين جريمة الإفصاح عن البيانات الحساسة أو نشرها بما يخالف ضوابط النظام، وبين باقي المخالفات لأحكام نظام حماية البيانات الشخصية، من حيث الجزاء، والجهة المختصة بإيقاع العقوبات.
- تبين أن المنظم اعتمد الازدواجية الرقابية فجعل من الهيئة السعودية للبيانات والذكاء الاصطناعي جهة إشرافية وفنية تملك سلطة الجزاء، بينما أبقى الولاية القضائية للمحاكم في المسائل الجنائية والمدنية.

التوصيات:

- توصي الدراسة المنظم بتوسيع نطاق تعريف البيانات الحساسة ليشمل البيانات الائتمانية وذلك نظرا لما يترتب على كشفها أو إساءة استخدامها من أضرار جسيمة تمس استقرار الفرد، ولضمان خضوع التعامل مع هذه البيانات للقيود المشددة والجزاءات المقررة للبيانات الحساسة.
- توصي الدراسة المنظم بفرض التأمين الإلزامي على جهات التحكم ضد مخاطر انتهاك البيانات، وذلك لضمان وجود ملاءة مالية تسمح بتعويض الأفراد المتضررين وحمايةً لجهات التحكم من الغرامات والتعويضات الضخمة التي يقررها النظام.
- توصي الدراسة المنظم بتحديد مدة الاحتفاظ في بيانات العمال بإلزام أصحاب العمل في مدد زمنية محددة لإتلاف بيانات العاملين بعد انتهاء العلاقة التعاقدية وعدم تركها في قاعدة البيانات لمدة طويلة لتقليل مخاطر الانتهاك أو الاستغلال غير المشروع.
- توصي الدراسة المنظم بفرض دورات تدريبية إلزامية لموظفي الموارد البشرية ومن تسمح لهم طبيعة عملهم بالتعامل مع البيانات في بيئة العمل، حول ضوابط نظام حماية البيانات الشخصية لضمان عدم وقوع مخالفات ناتجة عن الجهل بالنظام.
- توصي الدراسة الباحثين بدراسة التقاطع القانوني بين نظام حماية البيانات الشخصية ونظام العمل، نظرًا لندرة الأبحاث في هذا المجال.

قائمة المراجع

1. الجعيد، صالح عوض منصور، الحماية الجزائية لمعالجة البيانات الشخصية في النظام السعودي (دراسة مقارنة)، مجلة الأندلس للعلوم الإنسانية والاجتماعية، صنعاء، المجلد (114)، العدد (12)، 2025م.
2. الخزيمي، وليد عبد الله علي، وبن صغير، مراد، نظرات حول الحماية المدنية للبيانات الشخصية الحساسة للعامل "دراسة في التشريع الإماراتي"، مجلة جامعة الشارقة للعلوم القانونية، الإمارات العربية المتحدة، المجلد (22)، العدد (2)، 2024م.
3. الدليل الاسترشادي لإتلاف البيانات الشخصية وإخفاء الهوية والترميز، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، متاح على:

PersonalDataDestructionAnonymizationAndPseudonymisationGuidelineAR.pdf
4. الدليل الاسترشادي لإعداد وتطوير سياسة الخصوصية، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، متاح على:. PrivacyPolicyGuidelineArabic.pdf
5. الدليل الاسترشادي لتحديد الحد الأدنى من البيانات الشخصية، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، متاح على:.MinmumPDGuidelineArabic.pdf
6. الدليل الاسترشادي لقواعد أخلاقيات العمل، متاح على: pdf10212021.
7. الدهيمي، علي بن إبراهيم بن عبدالله، التزام العامل بالمحافظة على الأسرار بعد انتهاء عقد العمل وفقاً لأحكام نظام العمل في المملكة العربية السعودية: دراسة مقارنة، مجلة جامعة الملك سعود – الحقوق والعلوم السياسية، المملكة العربية السعودية، المجلد (37)، العدد (2)، 2025م.
8. الريس، رزق بن مقبول، والعبد، رضا محمود، شرح أحكام نظام العمل السعودي، مكتبة الشقري، 2017م
9. سياسات حوكمة البيانات الوطنية، سياسة تصنيف البيانات، الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي، بتاريخ 2020/5/5م، متاح على: سياسة وضوابط تصنيف البيانات.
10. عتوم، علي محمد علي، المسؤولية الجزائية للشخص المعنوي عن انتهاك البيانات الشخصية في ظل تقنيات الذكاء الاصطناعي، رسالة ماجستير، كلية الحقوق، جامعة عمان الأهلية، الأردن، 2024م.
11. الفارسية، العنود بنت إبراهيم بن عبيد، حقوق صاحب البيانات الشخصية ووسائل حمايتها وفقًا لقانون حماية البيانات الشخصية العماني، رسالة ماجستير، كلية الحقوق، جامعة السلطان قابوس، عمان، 2023م.
12. القانون الاتحادي الاماراتي رقم (45) لسنة 2021م، بشأن حماية البيانات الشخصية.
13. قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023م.
14. قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020م.
15. القرآن الكريم.
16. قواعد عمل لجان النظر في مخالفة أحكام نظام حماية البيانات الشخصية ولوائحه، الصادر عن الهيئة السعودية للبيانات والذكاء الاصطناعي، متاح على:. CommitteeWorkingRules.pdf
17. اللائحة التنفيذية لنظام العمل، الصادرة بقرار وزير العمل رقم 1/693، بتاريخ 1428/2/29 هـ.
18. اللائحة التنفيذية لنظام حماية البيانات الشخصية، الصادرة بتاريخ 1445/2/19 هـ..
19. اللائحة العامة لحماية البيانات(GDPR) ، 2016م، متاح على: General Data Protection Regulation (GDPR) – Legal Text .

20. لائحة حماية خصوصية البيانات الكويتية، الهيئة العامة للاتصالات وتقنية المعلومات، 2021م، متاح على: لائحة حماية خصوصية البيانات. pdf.

21. المرسوم السلطاني رقم (2022/6) بإصدار قانون حماية البيانات الشخصية، 2022م.

22. نظام العمل، الصادر بالمرسوم الملكي رقم(م/51)، بتاريخ 1426/8/23هـ

23. نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19)، بتاريخ 1443/2/9هـ.