مجلة جامعة الشارقة للعلوم القانونية

اسم المقال: نظرات حول الحماية المدنية للبيانات الشخصية الحساسة للعامل – دراسة في التشريع الإماراتي
اسم الكاتب: وليد عبد الله علي الخزيمي، مراد بن صغير
رابط ثابت: https://political-encyclopedia.org/library/9854
تاريخ الاسترداد: 2026/11/22 18:36 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة – Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الشارقة للعلوم القانونية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة للعلوم القانونية

مجلة علمية محكمة



المجلد 22، العدد 2
ذو الحجة 1446هـ / يونيو 2025م

الترقيم الدولي المعياري للدوريات 2616-6526

https//:doi.org/10.36394/jls.v22.i2.15

نظرات حول الحماية المدنية للبيانات الشخصية الحسّاسة للعامل "دراسة في التشريع الإماراتي"

وليد عبد الله علي الخزيمي[1]

مراد بن صغير[2]

تاريخ الاستلام: 25-08-2024 **تاريخ القبول: 13-12-2024**

ملخص البحث:

تكتسي حماية البيانات الشخصية الحسّاسة لا سيما في مجال العمل، أهمية متزايدة في ظل التحول الرقمي المتسارع وتطور مفهوم الخصوصية واتساع نطاقه. فأصبحت حماية البيانات الشخصية للعامل ضرورة ملحة لحماية خصوصيته وضمان حقوقه في أمن بياناته وسلامتها، في مواجهة خطر انتهاكها أو سوء استغلالها أو تسريبها، مما قد يؤثر سلبا على مساره المهني أو فرص حصوله على عمل أو ترقيته أو غيرها من المخاطر والتحديات القانونية.

يتناول هذا البحث جوانب الحماية القانونية للبيانات الحسّاسة للعامل، التي عمل التشريع الإماراتي على تكريسها من خلال قوانين حديثة جدا، على غرار القانون رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، وكذا القانون رقم 33 لسنة 2021 بشأن تنظيم علاقات العمل المعدل. حيث تتجلّى الإشكالية الرئيسية للبحث في السؤال: ما نطاق الحماية المكرسة للبيانات الحسّاسة للعامل؟ وما ضماناتها المقررة؟ تتناول الدراسة أساس حماية تلك البيانات ونطاقها، وكذا إبراز ضوابط وأحكام تكريسها، إضافة إلى بيان أهم الضمانات والآليات التي أفردها التشريع الإماراتي لتعزيز تلك الحماية. فضلا عن معالجة تدابير إنفاذ القانون وإقرار المسؤولية المدنية حال تضرر العامل نتيجة المساس ببياناته الشخصية الحساسة.

وقد توصلت الدراسة إلى وجوب تقيّد الجهات المعالجة وأصحاب العمل بالشفافية والعدالة والمشروعية والموافقة المستنيرة في جمع ومعالجة البيانات الشخصية الحسّاسة للعمال، باعتبارها ضوابط جوهرية. إضافة إلى ضمان حقوق العمال في سلامة بياناتهم، وأمنها، واستخدامها الموثوق والمشروع. فضلا عن ضرورة إدراج ضمانات عملية إضافية كفيلة بحماية تلك البيانات، وإنفاذ تدابير رقابية وأمنية شاملة مُقترنة بجزاءات قانونية ملائمة حال انتهاكها.

الكلمات الدالة: البيانات الشخصية الحسّاسة، عقد العمل، العمال، المعالجة، الحماية، المسؤولية التعويض.

---

(1) كلية القانون - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

U20105619@sharjah.ac.ae

(2) كلية القانون - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

المقدمة:

نتيجة للتطور المتسارع للتكنولوجيا الحديثة وتقدم نظم المعلومات وتطور أنظمتها التقنية وتشعبها، تتزايد التحديات وتتعاظم المخاوف بشأن المخاطر العملية المرتبطة بأنظمة حماية البيانات وحفظها ومعالجتها. فقد دفع غالب الدول إلى المبادرة بسَنّ تشريعات لتكريس الاستخدام الآمن والمشروع للبيانات الشخصية، وضمان معالجتها بشكل شفاف وعادل، بما يُعزّز الحق في حمايتها من أي تعدٍّ أو انتهاك

وفي ظل النهضة التشريعية التي تعرفها دولة الإمارات العربية المتحدة خلال السنوات الأخيرة، عمدت الدولة إلى تحديث غالب القوانين بما يواكب المستجدات المتلاحقة والظروف والبيئة المتطورة؛ إذ صدر قانون تنظيم علاقات العمل رقم 33 لسنة 2021، والذي عُدِّلّ لاحقا. كما صدر قانون حماية البيانات الشخصية رقم 45 لعام 2021، حرصا على ديمومة المصلحة العامة وحماية حقوق الأفراد، بما فيهم فئة العمال على وجه الخصوص؛ إذ وفّر التشريع الإماراتي غطاء قانونيا للعمال بهدف توفير حماية قانونية متكاملة بما يحفظ حقوقهم ويحقق استقرارهم المهني، لا سيما ما تعلق بجوانب حماية بياناتهم الشخصية

إشكالية البحث: يعالج البحث إشكالية جوهرية ذات بعد أخلاقي، قانوني ومهني، في ظل تزايد استخدام أنظمة الذكاء اصطناعي في مجال العمل والاعتماد على المعالجة الرقمية للبيانات الشخصية. وهو ما كان له بالغ الأثر على حقوق العمال وعقود عملهم؛ إذ تتجلّى إشكالية البحث الرئيسة كالتالي؛ ما حدود الحماية القانونية التي كفلها التشريع للبيانات الشخصية للعمال؟ وما مدى كفاية الضمانات المقررة لتلك الحماية؟

ذلك ما سنسعى للإجابة عنه من خلال بيان المرتكزات والضوابط القانونية التي أنتهجها التشريع الإماراتي في معالجة الموضوع، مع التركيز على معالجة بعض جوانب التعارض بين حق الوصول إلى البيانات الشخصية الحساسة، وحقوق العمال في سرية وحفظ بياناتهم الشخصية والمهنية. مع بيان السبل القانونية المتاحة لإنفاذ القانون وإقرار المسؤولية القانونية حال انتهاك تلك البيانات

أهداف البحث: يهدف البحث إلى الوصول لعدد من الأهداف العلمية والعملية، أبرزها:

- تحديد مفهوم البيانات الشخصية الحساسة للعامل وتمييزها عن غيرها من البيانات الشخصية والبيومترية المشابهة.
- تحليل ومناقشة الضوابط والمعايير المتعلقة بتجميع واستخدام بيانات العامل الشخصية الحسّاسة منها والبيومترية، مع التركيز على نطاق وضوابط استخدامها ومعالجتها.

- تحديد نطاق صلاحيات صاحب العمل في معالجة واستخدام البيانات الشخصية الحسّاسة للعامل، وحدود التزامه بالضوابط والضمانات القانونية المقرّرة في هذا الإطار.
- مناقشة وتقييم الضمانات القانونية والتدابير الإجرائية التي أقرّها التشريع الإماراتي لحماية بيانات العامل الشخصية الحسّاسة، بما يُعزّز سلامة وخصوصية تلك البيانات وضمان عدم انتهاكها.

منهجية البحث: لدراسة موضوع البحث تم توظيف المنهج الوصفي في بيان بعض المفاهيم القانونية والأحكام التنظيمية والإجرائية الخاصة بالبيانات الشخصية الحساسة للعمال. كما تم الاعتماد على المنهج التحليلي من خلال تحليل النصوص القانونية للتشريع الإماراتي ومناقشة الآراء الفقهية والتوجهات القضائية والموازنة والترجيح بينها، بمنهجية تحليلية نقدية قصد بيان حدود وضمانات وآليات حماية البيانات الشخصية الحساسة للعمال، ومعالجة المسؤولية المدنية الناجمة عن انتهاكها

ولبحث الموضوع فقد آثرنا تقسيمه إلى مبحثين: الأول سنوضح من خلاله قواعد تنظيم استخدام البيانات الشخصية الحساسة للعامل، أما المبحث الثاني فسنخصّصه لمعالجة انتهاك البيانات الشخصية الحساسة للعامل

المبحث الأول: الأحكام الناظمة لاستخدام البيانات الشخصية الحساسة للعامل

تقسيم: تعد أحكام وقواعد تنظيم معالجة واستخدام البيانات الشخصية الحساسة للعامل من المسائل القانونية بالغة الأهمية، والتي يجب مراعاتها بدقة واهتمام في بيئة العمل. ذلك أن البيانات الشخصية الحساسة باعتبارها جزء من البيانات الشخصية، إنما ترتبط أساسا بالبيانات التاريخية والمرجعية والفكرية للعامل، وكذا بيانات حالته الصحية، والتي تستخدم لأغراض متعددة قانونية، وإجرائية، وتنظيمية، ومهنية. الأمر الذي يجعل من الضروري، وضع قواعد وضوابط واضحة لمعالجة واستخدام تلك البيانات، سواء بالنسبة لجهات العمل، أو الجهات المخولة بذلك قانونا أو اتفاقا. ضمانا لحماية حقوق العمال في الاستخدام الآمن لبياناتهم الشخصية الحساسة في إطار أخلاقي وقانوني مسؤول. ولتوضيح ذلك نقسم هذا المبحث إلى المطلبين التاليين

المطلب الأول: مفهوم البيانات الشخصية الحساسة

تقسيم: تعد حماية البيانات الشخصية الحساسة أمرًا بالغ الأهمية في تطور العصر الرقمي الحالي؛ إذ أضحى الوصول بسهولة إلى معلومات الأفراد ومشاركتها واستغلالها، وفقا لضوابط تتعلق بتقييد الوصول إليها على الجهات المخولة طبقا للأنظمة التي تتطلبها لأغراض مشروعة. فضلا عن تطوير خطة استجابة واضحة حال اختراق أو انتهاك البيانات الشخصية للأفراد عموما والعمال على وجه الخصوص. ذلك أن العامل بحكم عمله له سجل مهني خاص بمنصب عمله ورتبه ومسيرته المهنية من جانب، كما لديه من جانب آخر بيانات خاصة تتعلق بأصوله العرقية والعائلية ومعتقده وتوجهاته الفكرية والفلسفية والسياسية وغيرها، فضلا عن بيانات تتعلق بحالته الصحية الجسدية والنفسية والعقلية. كلها بيانات تحتاج إلى حماية معززة، مراعاة لمصلحة العامل خلال بحثه عن فرص العمل، أو أثناء أدائه العمل، أو بعد انتهاء علاقة العمل. أمر يدفعنا لضبط تعريف مناسب للبيانات الشخصية الحساسة للعامل وتمييزها عن بياناته الشخصية أو البيومترية (الفرع الأول)، ثم التطرق لنطاق تلك الحماية (الفرع الثاني)

الفرع الأول: تعريف البيانات الشخصية الحساسة وتمييزها عن غيرها

تقسيم: بادرت معظم التشريعات الحديثة إلى تحديد مفهوم دقيق وواضح للبيانات الشخصية، في محاولة لتمييزها عن المفاهيم المشابهة على غرار الخصوصية، والبيانات الحساسة والبيومترية وغيرها من جانب، وضمان حمايتها لأصحابها من جانب آخر. ولتوضيح ذلك نقسم هذا الفرع إلى الغصنين الآتيين

الغصن الاول: تعريف البيانات الشخصية الحسّاسة: عمد المرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، إلى تعريف البيانات الشخصية الحساسة في مادته الأولى بأنها "أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة الشخص الطبيعي أو أصله العرقي أو آرائه السياسية أو الفلسفية أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به، أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحة هذا الشخص وتشمل حالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية التي تكشف عن وضعه الصحي".

يبدو باعتقادنا أن القانون الإماراتي حاول حصر غالب البيانات الشخصية الحساسة، والتي لها جوانب ذات خصوصية وحساسية للفرد، وذلك بالتركيز على أربع جوانب تشكل جوهر البيانات الأساسية الحساسة للشخص وهي: 1. البيانات الخاصة بأصله ومعتقده وفكره، 2. بيانات خاصة بسوابقه الجنائية، 3. بيانات خاصة بقياساته الحيوية البيومترية، 4. بيانات خاصة بحالته الصحية

بمختلف جوانبها وحالاتها. ورغم أنه قد وُفق إلى حد كبير في ذلك، إلا أننا نرى أنه قد شابه القصور بسبب عدم إدراجه للبيانات المالية وكذا البيانات الشخصية للطفل ضمن دائرة البيانات الشخصية الحساسة رغم أهميتها، وهو ما أخذ به التشريع الأمريكي وبعض التشريعات العربية. ولا شك أن البيانات الشخصية الحساسة تُعد أضيق نطاقا من البيانات الشخصية بوجه عام، لاعتبارات ارتباطها المباشر والوثيق كما يرى جانب من الفقه بحقوق الإنسان وحرياته الأساسية، التي تقرها المواثيق الدولية والدساتير الوطنية. (جبور، 2018، ص 81).

وبناء على ما تقدم يمكننا تعريف البيانات الشخصية الحساسة للعامل بأنها جميع البيانات التي تكشف بشكل مباشر أو غير مباشر عن عائلة العامل، أو أصله العرقي، أو آرائه السياسية، أو الفلسفية، أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به، أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحته وحالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية التي تكشف عن وضعه الصحي، أو حتى بياناته المالية.

الغصن الثاني: تمييز البيانات الشخصية الحساسة عن غيرها: تناولت غالب القوانين ثلاث صور للبيانات الشخصية، وهي البيانات الشخصية في صورتها العامة، والبيانات الشخصية الحساسة، والبيانات الحيوية البيومترية. وتتميز البيانات الشخصية الحساسة عن بقية تلك البيانات من عدة أوجه، أبرزها:

1. من حيث المضمون: تتعلق البيانات الشخصية الحسّاسة بالسمات والظروف الشخصية العميقة، مثل الصحة العقلية أو المعلومات الجينية (أقرورو، 2022، ص 134). فهي ترتبط بتقديرنا بالمعلومات والبيانات التي لا يرغب غالب الأشخاص في اطّلاع الغير عليها، نظرا لخصوصيتها وحساسيتها. بينما ترتبط البيانات الحيوية البيومترية بالسمات البيولوجية للفرد (الشعيبي، 2023، ص 104)، مثل البصمة وصورة الوجه والملامح الجسدية والفسيولوجية للشخص. مما يميزها عن الأنواع الأخرى من المعلومات الشخصية التي قد لا تكون في نفس المستوى من القدرة على تحديد الهوية المتأصلة (البقلي، 2021، ص 1030). لذلك يرى البعض أنه يمكن استخدامها كمعرف آلي على الأفراد بناء على خصائصهم البيولوجية والسلوكية (Wayman, and al., 2014). في حين تعبر البيانات الشخصية في صورتها العامة عن مجموع المعلومات والبيانات للتعرف على الشخص باعتبار له مركزا قانونيا، مثل اسمه ورقمه التعريفي وصوته وموقعه الجغرافي وصفاته المتعددة الشكلية، أو الفسيولوجية أو الاقتصادية أو الاجتماعية أو الثقافية. وبهذا يتضح لنا أن كلا من البيانات الشخصية الحساسة والبيانات الحيوية البيو مترية تدخل ضمن البيانات الشخصية.

2. من حيث الحصول على موافقة صاحب البيانات: تقرر غالب التشريعات بما فيها القانون الإماراتي لحماية البيانات بموجب المادة 04 منه، حظر معالجة البيانات الشخصية دون موافقة صاحبها. غير أنه تم استثناء بعض الحالات التي يجوز معالجتها دون حاجة للموافقة، ومنها تلك المتعلقة بالفقرات 4، 8، 9 من ذات المادة، لاعتبارات تتعلق بحماية الصحة العامة للعمال والموظفين، حفظ حقوقهم التعاقدية لا سيما الاجتماعية والمالية منها.

3. من حيث تحديد مسؤول حماية البيانات: أوجبت المادة 10 من قانون حماية البيانات الإماراتي على المتحكم والمعالج معا، بشأن البيانات الشخصية الحساسة دون غيرها، ضرورة تحديد مسؤول لحماية البيانات ممن تتوافر فيه المهارات والدراية الكافية بحماية البيانات الشخصية، وذلك متى كانت المعالجة تتضمن تقييم ممنهج وشامل للبيانات الشخصية الحساسة بما يشمل التنميط والمعالجة المؤتمتة، وكذلك متى كانت المعالجة تنصب على حجم كبير من البيانات الشخصية الحساسة. ولذلك يرى بعض الفقه أنه لا يجوز استخدام البيانات البيومترية والبيانات الحساسة للتجميع والمعالجة الآلية (راشد، 2019، 191).

الفرع الثاني: نطاق حماية البيانات الشخصية الحساسة للعامل

تقسيم: لا أحد يجادل في أن البيانات الشخصية الحساسة للفرد تشكل أحد حقوقه الشخصية الأساسية، والتي يجب حمايتها بشكل قانوني (راشد، 2019، ص 193). أمر يُخوّل العامل الحق في الموافقة على بياناته ومعلوماته الخاصة ومنع الآخرين من إساءة استخدامها، وتعزيز الخصوصية والأمان في بيئة العمل. في ظل تزايد خطر الإفصاح وسوء الاستخدام من قبل الأنظمة الإلكترونية والمواقع وغيرها. ما يستدعي ضرورة تنظيم عمليات معالجة واستخدام وتداول البيانات الشخصية الحسّاسة بطريقة تحافظ على أمنها وسرّيتها (عبد الرحمن، 2015، ص106)

ويتم تحديد نطاق حماية البيانات الشخصية الحسّاسة للعامل من وجهين، من خلال تقسيم هذا الفرع إلى الغصنين التاليين.

الغصن الأول: طبيعة البيانات الحسّاسة ذاتها: طبقا لنص المادة 02 من قانون حماية البيانات الاتحادي، فإن الحماية تنصب على معالجة البيانات الشخصية للعامل مهما كانت كأصل عام، سواء كلها أو جزء منها عن طريق وسائل الأنظمة الإلكترونية أو غيرها من الوسائل. غير أنها استثناء لا تشمل البيانات الشخصية للعامل لدى الجهات الأمنية أو القضائية، وذلك مراعاة لما تقتضيه طبيعة عمل هذين الجهتين وما تهدف إليه من بسط للأمن وتحقيق للعدالة. كما لا ينصرف نطاق الحماية إلى البيانات الشخصية الصحية

التي لديها تشريع ينظم حماية ومعالجة تلك البيانات، على غرار البيانات المتعلقة بنقل وزرع الأعضاء وفقا للقانون الاتحادي رقم 25 لسنة 2023 في شأن نقل وزراع الأعضاء البشرية، وكذلك القانون الاتحادي رقم 8 لسنة 2019 بشأن المنتجات الطبية ومهنة الصيدلة المعدل. ولا شك أن بعض هذه البيانات الحساسة للعامل إنما تفقد امتياز الحماية المشددة التي تتمتع بها، في مقابل قيم أكبر ومصالح أهم؛ كالمصلحة العامة، والصحة العامة، والمصلحة العلمية. (جبور، 2018، ص 83)

ويبدو من وجهة نظرنا أن استثناء بعض البيانات الشخصية من سريان القانون، لا يعني إزالة الحماية عنها، بقدر ما يعكس وعيًا قانونيا بأن بعض الأنواع من البيانات تتطلب معالجة وحماية خاصة نظرًا لطبيعتها الحساسة والمهم.، كما يعزز ذلك الثقة في نظام الحماية ويضمن التوازن بين الخصوصية الفردية واحتياجات المجتمع

الغصن الثاني: آليه معالجة البيانات الحسّاسة: انطلاقا من نص المادة 01 / 4 والمادة 02 / 1 من قانون حماية البيانات الاتحادي، فإن حماية البيانات الشخصية الحساسة للعامل أثناء معالجتها ترتبط بفئتين من حيث الأشخاص، وهما:

1. العامل صاحب البيانات (الدائن بالحماية): وهو بحسب نص المادة 01 من القانون الاتحادي رقم 33 لسنة 2021 بشأن تنظيم علاقات العمل، كل شخص طبيعي مصرح له من الوزارة للعمل لدى إحدى المنشآت المرخصة في الدولة تحت إشراف وتوجيه صاحب العمل، يُقيم في الدولة أو له مقر عمل فيها.
2. المتحكم أو المعالج أو مسؤول حماية البيانات (المدين بالحماية): بحسب نص المادة 01 من قانون حماية البيانات الاتحادي، يلتزم المتحكم أو المعالج سواء كان شخصا اعتباريا (منشأة) أو شخصا طبيعيا، بمعالجة البيانات الشخصية بأي وسيلة إلكترونية، مع ضمان أمنها من خلال مجموعة من التدابير والإجراءات والعمليات التقنية والتنظيمية المحددة، من شأنها الحفاظ على حماية خصوصية وسرية وسلامة ووحدة البيانات الشخصية وتكاملها وتوافرها. كما يلتزم مسؤول حماية البيانات شخصا طبيعيا أم اعتباريا هو الآخر، بالتأكد من مدى امتثال لضوابط واشتراطات وإجراءات وقواعد معالجة حماية البيانات الشخصية، والتأكد من سلامة أنظمتها وإجراءاتها.

يتبين مما سبق أن حماية البيانات الشخصية الحساسة للعامل منوطة بجميع الأطراف ذات الصلة بمعالجة البيانات الشخصية، بما في ذلك الأفراد والكيانات المختلفة، سواء كانوا داخل الدولة أو خارجها. ما يعزّز حماية البيانات الشخصية للعامل بغض النظر عن مكان تواجده أو مكان معالجة بياناته

المطلب الثاني: ضوابط معالجة البيانات الشخصية الحساسة للعامل

تقسيم: إن أحد العناصر الرئيسة التي تمنح المؤسسات ميزة تنافسية هو حجم وجودة البيانات التي تمتلكها، لما لها من قيمة إضافية كبيرة. ففي مجال علاقات العمل يتيح وجود قاعدة بيانات للعمال لأصحاب العمل معرفة طاقة الموارد البشرية المتاحة وحصر القدرة الإنتاجية بشكل دقيق في مكان عملهم. ومن ثم استخدامها لأهداف مشروعة مفيدة للشركة تزيد من نجاحها (أميرهم، 2020، ص 161). غير أن مخاوف كبيرة وتحديات متعددة تثور بشأن الاستخدام الآمن والمعالجة المشروعة للبيانات الشخصية للعامل لا سيما الحساسة منها، سواء أثناء تقديمه للحصول على فرصة عمل من خلال سيرته الذاتية أو سجله الصحي أو مسيرته المهنية السابقة، أو أثناء ممارسته لعمله من خلال حدود المتابعة والمراقبة. لذلك يرى البعض أنه لا يمكن لصاحب العمل معالجة البيانات المتعلقة بالعامل إلا بالحد الأدنى الذي تتعلق فيه هذه البيانات بقدرات العامل على أداء وظيفته، وأن تكون ضرورية لتنفيذ عقد العمل. (Bourdillon, 2017, p 288)

وفي هذا الإطار فقد حظر قانون حماية البيانات الشخصية الإماراتي بموجب المادة 04 أي معالجة للبيانات الشخصية دون موافقة صاحبها. وهذا لا شك يتماشى مع مقتضيات الحماية وتدابير الأمن والسلامة. غير أن المادة أوردت استثناءات على مبدأ موافقة صاحب البيانات، من خلال جملة من الضوابط، منها تلك المعالجة في مجال عقد العمل. وهو ما قد يمنح صاحب العمل مجالا أوسع لاستخدام بيانات العامل أو تجاوزها دون ضوابط. (ريان، 2021، ص 204). وعليه ستتم مناقشة ضوابط معالجة البيانات الشخصية للعامل في الفرعين المواليين.

الفرع الأول: ضوابط المعالجة الخاصة بطبيعة البيانات وأغراضها

لا شك أن مجال حماية البيانات الشخصية يقتضي أن تقتصر المعالجة على الغرض المشروع الذي تم جمع تلك البيانات لأجله. ويهدف هذا المبدأ إلى تضييق وتحديد نطاق المعالجة لضمان تحقيقها للهدف المحدد دون تجاوزه. وفي حالة تغيير أو الانحراف عن تلك الأهداف، يلزم إعلام صاحب البيانات بتلك التغييرات والحصول على موافقته. ذلك أن عدم الامتثال لهذا المبدأ يعد انتهاكًا للقانون. (الخصاونة وآخرون، 2011، ص 14)

وفي إطار استخدام وتداول بيانات العامل، فإنه يُحظر على صاحب العمل تجاوز أغراض علاقة العمل ومتطلباته المشروعة في جمع ومعالجة بيانات العمال (Fanti, 2017, p 233)، من دون الحصول على موافقة صريحة منهم، وفقا لما تقضي به المادتين (04) و(06) من قانون حماية البيانات الشخصية الإماراتي. يُستثنى من ذلك الحالات الواردة على سبيل الحصر في المادة (4)، ومنها:

- المعالجة الضرورية لأغراض الطب المهني أو الوقائي لأجل تقييم قدرة العمال على العمل، أو التشخيص الطبي، أو تقديم الرعاية الصحية، أو الاجتماعية، أو العلاج، أو خدمات التأمين الصحي، أو إدارة أنظمة الرعاية الصحية، أو الاجتماعية.

- المعالجة الضرورية لأغراض قيام المتحكم أو صاحب البيانات بالتزاماته ومباشرة حقوقه المقررة قانونا في مجال التوظيف والعمل أو الضمان الاجتماعي أو القوانين المعنية بالحماية الاجتماعية.

- المعالجة الضرورية لتنفيذ عقد يكون صاحب البيانات طرفا فيه، أو لاتخاذ إجراءات بناء على طلب صاحب البيانات بهدف إبرام عقد، أو تعديله، أو إنهائه.

وما تجدر الإشارة إليه أن هذه الاستثناءات في معالجة بيانات العمال من دون الحصول على موافقتهم ليست مطلقة[1]، بل مقيدة بحالة الضرورة كما هو واضح بصريح المادة 04. كما أن ذلك لا يعفي صاحب العمل باعتقادنا من ضرورة إعلام العمال بمتطلبات ومبررات معالجة بياناتهم الشخصية، وإن كان الأمر لا يتطلب موافقتهم كما ذكرنا. كأن يكون ذلك مدرجا في عقود العمل أو في القانون الأساسي لجهة العمل أو غيره من الآليات التي يتحقق بها علم واطلاع العامل على حالات معالجة بيانته من دون موافقته.

أما عن البيانات الشخصية الحساسة للعامل، فيبدو أن ضوابط حمايتها أكثر دقة وتشديدا من غيرها البيانات الشخصية، لارتباطها بجوانب عرقية وصحية واجتماعية وعائلية خاصة بالعامل (Lempen, 2017, p 271). لذلك نرى عدم أحقية صاحب العمل مالك البيانات أو المتحكم أو المعالج في استخدامها أو تداولها من دون موافقة العامل، لما لها من أثار وتداعيات متعددة على حياته الخاصة وحياة أسرته وعمله ومستقبله المهني.

وقد حددت المادة 05 من قانون حماية البيانات الاتحادي جملة من الضوابط على سبيل المثال، لمعالجة البيانات الشخصية بصفة عامة، ولتوضيح ذلك نقسم هذا الفرع الي أربعة غصون.

الغصن الأول: المعالجة العادلة والشفافة والمشروعة: بحيث تكون معالجة البيانات بطريقة عادلة وشفافة ومشروعة؛ إذ لا يتم جمع البيانات إلا بطريقة مشروعة ولأغراض

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection desdonnées), abrégé ci-après RGPD. Le RGPD est accessible à cette adresse : http://eurlex.europa.eu/legal-content/FR/TXT/

مشروعة (رجب، 2024، ص 437)، ومحددة لصالح العامل المعني بالبيانات أو لصالح الجهة المعالجة، بشكل لا يخالف النظام العام والآداب

الغصن الثاني: المعالجة للضرورة في حدود الغرض المسموح به: ومعنى ذلك أن تكون معالجة بيانات العمال الحساسة لأغراض مهنية بحتة، أو لأغراض تتعلق بحقوق العمال كالضمان الاجتماعي والمعاشات والتعويضات وغيرها. ذلك أن تجميع البيانات أو معالجتها لأغراض تجارية أو ربحية تجعلها غير مشروعة. (التهامي، 2015، ص 406)

الغصن الثالث: الحفاظ على البيانات الشخصية وحمايتها من الانتهاك: من ضوابط المعالجة الأكثر أهمية المحافظة عليها وحمايتها من أي انتهاك، أو اختراق، أو معالجة غير مشروعة، أو غير مرخص بها. وذلك يقتضي اتخاذ تدابير احترازية وإجراءات تنظيمية ملائمة

الغصن الرابع: عدم الاحتفاظ بالبيانات الشخصية بعد استنفاد الغرض من معالجتها: مفاد ذلك ضرورة التخلص من البيانات الشخصية الحساسة للعامل بمجرد استنفاذ الغرض الذي تم جمعها من أجله. وليس هناك من استثناء إلا حالة وحيدة يجوز فيها الإبقاء على تلك البيانات بشرط إخفاء هوية صاحب البيانات باستخدام خاصية "آلية إخفاء الهوية". غير أن القانون الإماراتي لم يحدد مدة محددة للاحتفاظ بتلك البيانات، خلافا للائحة الأوروبية العامة لحماية البيانات التي سمحت بالاحتفاظ بالبيانات لفترة أطول مما هو مخصص لأرشفة المصلحة العامة أو الأغراض العلمية أو البحث التاريخي. (Bourdillon, Knight, 2017, p 293).

غير أننا نرى أن مدة إخفاء هوية العامل والتخلص من بياناته الشخصية لا تقل عن سنتين بعد انتهاء خدمته، وفقا لما ورد في المادة (13) من قانون تنظيم علاقات العمل الإماراتي. ويستند هذا التحديد الزمني إلى عدة مبررات موضوعية وقانونية: أولها حماية حقوق العامل في حال نشوء نزاعات عمالية لاحقة تتطلب الرجوع إلى بياناته وسجلاته، وثانيها تمكين الجهات المختصة من إجراء عمليات التفتيش والرقابة على منشآت العمل خلال مدة معقولة، وثالثها توفير المعلومات اللازمة لتسوية المستحقات المالية والتأمينية للعامل. وبهذا يتضح وجوب احتفاظ صاحب العمل ببيانات العمال باعتبارها ضمن ملفاتهم وسجلاتهم، لمدة لا تقل عن عامين بعد انتهاء علاقة العمل. الأمر الذي يتطلب بتقديرنا تنسيقا وانسجاما أكبر بين قانون حماية البيانات الشخصية وقانون تنظيم علاقات العمل في هذا الخصوص، وذلك لأجل وضع استثناءات وضوابط تسمح لصاحب العمل بحفظ بيانات العامل وكذا استخدام آلية إخفاء البيانات بعد انتهاء علاقة العمل (علي، 2022، ص 1288) بما يكرس حماية أفضل للعامل

الفرع الثاني: ضوابط المعالجة الخاصة بالعامل

لا شك أن وضع معيار للعدالة ومأمونية معالجة البيانات الشخصية الحسّاسة للعامل يمثل تحديا كبيرا، ولكن يمكن فهمه إذا أخذنا في الاعتبار مجال التطبيق والأطراف ذات الصلة وجودة البيانات المراد معالجتها. فتطبيق الإنصاف في معالجة البيانات الشخصية الحساسة للعامل قضية حاسمة في مكان العمل، تؤثر بالتأكيد على مؤسسة وبيئة العمل، والتي بدورها تؤثر على سوق العمل ككل. إذ يجب معاملة العامل بإنصاف وشفافية في عمله، من دون تمييز بسبب جنسه، أو جنسيته أو عرقه أو دينه (Leonelli, S., and al, 2021, p 03).

فمن المهم جدا توحيد أهداف جمع البيانات الشخصية الحساسة للعمال في مجال العمل دون تمييز، وفقا لما أقرته المادة 4 / 1 من قانون تنظيم علاقات العمل الاتحادي، تكريسا لمبدأ تكافؤ الفرص وعدم المساس بالمساواة في الحصول على الوظيفة أو الاستمرار فيها والتمتع بحقوقها. لذلك قد يبدو واضحا انتهاك صاحب العمل للبيانات وضوابط معالجتها، عندما يتم تنفيذ عملية المعالجة بهدف تحديد خلفية فئات معينة من العمال على أساس عرقهم أو جنسياتهم دون فئات أخرى، رغم المساواة في الخبرة والمستوى المهني (Major, 2017, p 302). لذلك يرى البعض أنه يجب أن تضمن سياسة استخدام البيانات الشخصية الحساسة للعامل، عملية المعالجة بطريقة مرئية وحقيقية، شفافة ومشروعة (Flueckiger, 2017, p 09). كما يجب على الشخص الذي يقوم بعملية المعالجة، سواء كان صاحب العمل (المالك) أو المعالج أو المتحكم أو من ينوب عنهم، ضرورة القيام بها بطريقة لا تشكل انتهاكا لبيانات العامل. (القري، 2023، ص 123).

من جهة أخرى وتأكيدا لما ورد في نص المادة 04 من قانون حماية البيانات الشخصية، من حظر معالجة بيانات العامل دون موافقته، فقد بينت المادة 06 الشروط المطلوبة بشأن الموافقة للاعتداد بها، والتي يمكن إجمالها في النقاط التالية:

أ. أن يكون المتحكم قادراً على إثبات موافقة صاحب البيانات في حال كانت المعالجة مبنية على موافقة صاحب البيانات لمعالجة بياناته الشخصية.

ب. أن تكون الموافقة معدة بطريقة واضحة وبسيطة وغير مبهمة وسهلة الوصول إليها سواء كانت كتابية أو إلكترونية.

ج. أن تتضمن الموافقة ما يفيد حق صاحب البيانات بالعدول عنها، وأن يكون إجراء العدول بطريقة سهلة.

2. يجوز لصاحب البيانات الدول في أي وقت عن موافقته على معالجة بياناته الشخصية، ولا يؤثر هذا العدول على قانونية ومشروعية المعالجة المبنية على الموافقة التي أعطيت قبل العدول عنها.

ولا شك أن هذه الشروط تعكس حرص التشريع على توفير حماية قانونية للعامل، وضمان تعامل مسؤول وشفاف في معالجة البيانات الشخصية للعامل من قبل صاحب العمل أو الجهات المخولة بذلك. إذ بموجب هذه الشروط يتم تعزيز الثقة بين الأطراف التي تتولى معالجة البيانات الشخصية، فضلا عن تعزيز حقوق العامل في حماية وضبط التحكم في بياناته الشخصية (Ma Ruoxue, 2023, p 224). أمر لم يقتصر عند حدّ الموافقة فحسب، بل حرص القانون على منح العامل صاحب البيانات حماية إضافية أوسع، وذلك من خلال إقرار حقه في الحصول على المعلومات بشأن بياناته الشخصية التي يتم معالجتها ومن دون أي مقابل، طبقا لما نصت عليه المادة 13 من قانون حماية البيانات الشخصية. وكذلك حقه في العدول عن موافقته في أي وقت وفقا لما ورد في المادة 06 / 2 من ذات القانون، وهو ما يكفل حرية الاختيار والموافقة والمتابعة للبيانات الشخصية، بما يُعزز المرونة والتوازن في العلاقة بين صاحب العمل (المالك) أو المعالج والعامل صاحب البيانات. إضافة إلى الاعتراف للعامل صاحب البيانات بحقه بنقل بياناته الشخصية (المادة 14)، تصحيح أو محو البيانات الشخصية (المادة 15)، تقييد معالجة البيانات الشخصية (المادة 16)، إيقاف المعالجة (المادة 17)، فضلا عن حقه في ضمان أمن معلومات بيانته الشخصية وفقا لما قضت به المادة 20 من ذات القانون

المبحث الثاني: معالجة انتهاك البيانات الشخصية الحسّاسة للعامل

تقسيم: كثيرا ما تتعرض معالجة البيانات الشخصية الحساسة للعامل للانتهاك والاختراق، إما من قبل صاحب العمل أو من الجهات الأخرى ذات العلاقة. ولأجل ذلك تم رصد جملة من الضمانات المقررة لحماية تلك البيانات من جهة (المطلب الأول)، وإقرار المسؤولية المدنية المترتبة عن التعدي عليها من جهة أخرى (المطلب الثاني). ما يستدعي صياغة نظم وإجراءات قانونية كفيلة بإنفاذ ضمانات الحماية، وتيسير حصول العمال على تعويض عادل وشامل حال تضررهم من انتهاك بياناتهم الشخصية الحساسة. ولتوضيح هذا المبحث تم تقسيمه إلى المطلبين التاليين

المطلب الأول: الضمانات المقررة لحماية البيانات الشخصية الحسّاسة للعامل

تقسيم: المتأمل في نصوص قانون حماية البيانات الشخصية الحساسة، يجدها تتراوح بين ضوابط قانونية وقواعد إجرائية، أو ضمانات قانونية عملية لضمان حماية البيانات الشخصية الحساسة للعامل. وسنفرد هذا المطلب من خلال ثلاثة فروع إلى تلك الضمانات التي تضمنها قانون حماية البيانات الشخصية الإماراتي. حيث سنتناول التزامات المتحكم؛

فنسلط الضوء على الإجراءات الواجب اتخاذها من قبل الجهات المتحكمة في جمع ومعالجة البيانات الشخصية الحساسة للعامل. بينما سنستعرض في الفرع الثاني التزامات المعالج؛ فنوضح الخطوات والإجراءات التي يجب اتباعها من قبل الأطراف المعالجة لهذه البيانات. وأخيرًا نلقي الضوء في الفرع الثالث على التزامات مسؤول حماية البيانات؛ إذ نبيّن دوره في تنفيذ السياسات والإجراءات اللازمة لضمان حماية البيانات الشخصية بشكل فعّال

الفرع الأول: التزامات المتحكم

المتحكم بحسب نص المادة 01 من قانون حماية البيانات الشخصية الاتحادي هو المنشأة أو الشخص الطبيعي الذي يقوم بحكم نشاطه بتحديد طريقة وأسلوب ومعايير معالجة البيانات الشخصية والغاية من معالجتها. حيث تلعب الالتزامات المفروضة على المتحكمين دورًا جوهريا وفعّالا في حماية البيانات الشخصية للأفراد وخصوصياتهم (العتيبي، 2015، ص 233). وفي هذا السياق أوردت المادة 07 من قانون حماية البيانات الشخصية الاتحادي جملة من الالتزامات العامة للمتحكم، والتي تشمل جوانب مختلفة أساسية لتعزيز أمن البيانات وسرية المعلومات. إذ يتعيّن بموجبها على المتحكم الامتثال للتدابير التقنية والتنظيمية الكفيلة بتعزيز حماية وأمن البيانات الشخصية ضد الانتهاك أو الاختراق أو الوصول غير المصرح به (Ouannass, 2022). كما يجب أن تتمثل هذه التدابير في التوافق مع طبيعة وأهداف معالجة البيانات مع التقليل من المخاطر المحتملة لسرّية البيانات وخصوصيتها. وبالإضافة إلى ما سبق، يؤكد القانون على ضرورة اتخاذ المتحكم للتدابير المناسبة على مدار دورة المعالجة، بما في ذلك آليات إخفاء البيانات أو محوها أو تعديلها.

كما تلقي المادة 09 من ذات القانون جملة من الالتزامات الضرورية تُثقل كاهل المتحكم، أبرزها المبادرة لإبلاغ مكتب الإمارات للبيانات عن أي انتهاك أو اختراق للبيانات الشخصية للعامل. ولا ريب أن هذا الالتزام يتجاوز مجرد الوعي إلى الكشف الاستباقي، مما يضمن الشفافية والمساءلة في ممارسات معالجة البيانات (Walter, 2017, p 84). ويبدو أن هدف تحديد تفاصيل الانتهاك والإجراءات المتخذة والعواقب المحتملة، هو تيسير التحقيقات الشاملة واتخاذ التدابير الصحيحة. وبالإضافة إلى جملة الالتزامات السابقة، يلتزم المتحكم بإخطار العامل صاحب البيانات، متى كان من شأن الانتهاك مساس بخصوصية وسرية وأمن بياناته. مما يمنح هذا الأخير رؤية واضحة حول طبيعة الانتهاك والتدابير المتخذة لمواجهته، مما يعزز لديه الثقة والشفافية والمسؤولية في معالجة بياناته

من جهة أخرى أوجبت المادة 12 على المتحكم شأنه شأن المعالج كضمانة لحماية بيانات العامل الشخصية، ضرورة توفير السبل كافة لضمان أداء مسؤول حماية البيانات للأدوار والمهام الموكلة إليه والتي سنبينها لاحقا. وفي هذا المقام يتأكد التشديد على ضمان إشراك

مسؤول حماية البيانات وبالشكل المناسب وفي الوقت الملائم في كافة المسائل المرتبطة بحماية البيانات الشخصية للعامل. مع ضمان تزويده كذلك بكافة الموارد اللازمة وتقديم الدعم له لتنفيذ المهام الموكلة إليه. مع الحرص على عدم إنهاء خدماته أو فرض أي جزاء تأديبي لأي سبب يتعلق بتأديته لمهامه. الأمر الذي يقتضي دون شك ضمان المتحكم بعدم تكليف مسؤول حماية البيانات بأي مهام قد ينجم عنها تعارض في المصالح مع المهام الموكلة إليه

وضمن سياق ضمانات حماية البيانات الشخصية الحساسة للعامل، يلتزم المتحكم بتوفير طرق وآليات مناسبة وواضحة لتمكين صاحب البيانات من التواصل معه، وطلب ممارسة أي من حقوقه الواردة في قانون حماية البيانات الشخصية. إذ تشكل قنوات التواصل مسألة جوهرية في عمل المتحكم ومعالجته للبيانات الشخصية (Walter, 2017, p 99). حيث يتوجب عليه في هذا الإطار تكريسا لأمن معلومات البيانات الشخصية للعامل ضرورة وضع واتخاذ إجراءات وتدابير تقنية وتنظيمية ملائمة لضمان تطبيق مستوى أمن المعلومات الذي يتناسب مع المخاطر المحتملة للمعالجة، على غرار تشفير البيانات الشخصية وتطبيق آلية إخفاءها، وكذا تطبيق إجراءات وتدابير لضمان الإبقاء على سرية أنظمة وخدمات المعالجة وسلامتها، مع إمكانية استرجاع البيانات وسرعة وسهولة الوصول إليها، وفقا لما أوردته المادة 20 من قانون حماية البيانات الاتحادي. إضافة إلى التزام المتحكم عند تقييمه لمستوى أمن المعلومات، بضرورة مراعاة حجم المخاطر المصاحبة للمعالجة، وكذا طبيعة المعالجة، ونطاقها، وأغراضها وتكاليفها. وهو ما يتطلب تقييماً وتحسيناً مستمرين للتدابير الوقائية استجابة للتهديدات المتطورة والضروريات التشغيلية

من جانب آخر نلاحظ أن القانون الإماراتي في إطار التقييم الاستباقي لعمليات المعالجة وقبل الشروع في المعالجة، ألزم المتحكم بضرورة أن يُجري تقييما لأثر عمليات المعالجة على حماية البيانات الشخصية للعامل، متى كانت المعالجة ستتم على حجم كبير من البيانات الشخصية الحساسة، أو متى كانت المعالجة تتضمن تقييما ممنهجًا وشاملا للجوانب الشخصية لصاحب البيانات، باعتماد على المعالجة المؤتمتة أو التنميط. وقد قيّدت المادة 21 من قانون حماية البيانات المتحكم بشأن تقييم أثر المعالجة بجملة من القيود والضوابط، بما يتناسب مع حجم المخاطر وطبيعة هذا الإجراء ووقته وأثاره المحتملة

الفرع الثاني: التزامات المعالج

لم يكتفِ قانون حماية البيانات الشخصية الإماراتي في سبيل توفير ضمانات كافية لحماية البيانات الشخصية الحساسة للعامل، بالتزامات المتحكم فحسب. بل عزّز تلك الحماية بإلزام المعالج بالتزامات أخرى، باعتباره المنشأة أو حتى الشخص الطبيعي الذي يعالج البيانات الشخصية نيابة عن المتحكم، وبتوجيه منه ووفقا لتعليماته (Dubois, 2017, 63). حيث أوردت المادة 08 من

قانون حماية البيانات الاتحادي هي الأخرى جملة من الالتزامات العامة للمعالج تكريسا لحماية شفافة ونزيهة للبيانات الشخصية. وما تجدر الإشارة إليه أن المعالج عليه التزامات مزدوجة؛ بعضها تجاه المتحكم من جهة، وغالبها تجاه العامل صاحب البيانات من جهة أخرى.

فالمعالج ملزم بإجراء معالجة البيانات وتنفيذها وفقا لتعليمات المتحكم، في إطار العقود والاتفاقات المبرمة بينهما. كما يلتزم المعالج وفقا للمادة 09 / 3 من ذات القانون، في حال علمه بوجود أي اختراق أو انتهاك للبيانات الشخصية لصاحب البيانات، بضرورة إخطار المتحكم بهذا الاختراق أو الانتهاك فور علمه بذلك. كما ألزمت المادة 10 من القانون نفسه على كل من المتحكم والمعالج وجوبا، ضرورة تعيين مسؤول مؤهل لحماية البيانات، وذلك في ثلاث حالات حصرية أوردتها المادة 11، تتعلق بطريقة المعالجة ونطاقها بشأن البيانات الشخصية الحساسة للعامل، مع التزام كل واحد منهما بتوفير كافة السبل لضمان أداء مسؤول حماية البيانات الأدوار والمهام الموكلة إليه، وفقا لما أوردته المادة 12 من قانون حماية البيانات الاتحادي. غير أن ما أثار التساؤل لدينا؛ هل يملك المعالج تعيين مسؤول لحماية البيانات من تلقاء نفسه؟ أم يكون ذلك بناء على استشارة المتحكم وموافقته؟

لم يرد في قانون حماية البيانات الاتحادي أي توضيح أو تفصيل لذلك، بل إن ظاهر نص الفقرة الأولى من المادة 10، يُوحي بتساوي سلطة المتحكم وسلطة المعالج في تعيين مسؤول حماية البيانات. غير أن ذلك بحسب ما نراه لا يستقيم، ذلك أن عمل المعالج أصلا في المعالجة وتنفيذها إنما يكون وفقا لتعليمات وتوجيهات المتحكم في إطار العقد القائم بينهما. وهو ما يفسر باعتقادنا عدم امتلاك المعالج صلاحية تعيين مسؤول حماية البيانات إلا بموافقة صريحة أو ضمنية من المتحكم.

من جانب آخر يلتزم المعالج تجاه العامل صاحب البيانات طبقا للمادة 08، بتطبيق الإجراءات والتدابير الملائمة لحماية البيانات أثناء مرحلة تصميم أو مباشرة المعالجة، وذلك وفق الغرض والمدة المحددة لها، والتي تم الاتفاق عليها بينه وبين المتحكم. وفي حال تجاوز مدة المعالجة المحددة، يجب عليه إخطار المتحكم لاتخاذ ما يراه مناسبا. كما يتعين عليه محو البيانات بعد انقضاء مدة المعالجة أو تسليمها للمتحكم، وهو ما يترجم التزامه بعدم القيام بأي عمل من شأنه الإفصاح عن البيانات الشخصية أو نتائج المعالجة إلا في إطار القانون (Dupont, 2017, p 204). مع العمل على حماية وتامين عملية المعالجة وتأمين الوسائط والأجهزة المستخدمة في المعالجة.

وإلحاقا بالضمانات السابقة، شدّدت المادة 20 على ضرورة اتخاذ المعالج والمتحكم كافة الإجراءات والتدابير اللازمة لضمان تطبيق مستوى أمن المعلومات بما يتناسب مع المخاطر المرتبطة بالمعالجة وتكاليفها، سواء ما تعلق منها بتشفير البيانات الشخصية وآلية إخفاءها (عبد الرحيم، 2023، ص 36)، أو ضمان سلامتها وسريتها واسترجاعها حال حدوث أي عطل

الفرع الثالث: التزامات مسؤول حماية البيانات

يُعَد مسؤول حماية البيانات الشخصية بمثابة حلقة وصل بين مقدم الخدمة، ومركز حماية البيانات، فهو الشخص المعني بالبيانات، وقد أشارت المادة (10) من قانون حماية البيانات إلى ضرورة تعيين مسؤول حماية البيانات ممن يتمتع بالمهارات والدراية الكافية بحماية البيانات، وذلك في ثلاث حالات واردة على سبيل الحصر، أوردتها الفقرة الأولى. وتعتبر هذه الخطوة أساسية في ضمان الامتثال لقواعد حماية البيانات الشخصية، إذ من المهم أن يتوافق المسؤول المعين مع المعايير المحددة في المادة لضمان فعالية الحماية، لا سيما تلك الحالات التي تتضمن معالجة بيانات شخصية حساسة أو استخدام تقنيات جديدة تشكل خطرًا على خصوصية البيانات، أو تقييم ممنهج وشامل للبيانات الشخصية الحساسة

ويتولى مسؤول حماية البيانات القيام بعدة أدوار أساسية، فيتأكد من مدى امتثال المتحكم أو المعالج بتنفيذ أحكام قانون حماية البيانات ولائحته وكذا تعليمات المكتب، فهو أشبه ما يكون بجهاز رقابي. فيقع على عاتقه التحقق من جودة وصحة الإجراءات المتخذة، وتلقي الشكاوى والطلبات المتعلقة بالبيانات الشخصية، مع تقديم الاستشارات الفنية لتقييم أنظمة الحماية وتوثيق النتائج وتقديم التوصيات اللازمة. لذلك نرى أن مسؤول حماية البيانات يجسّد دور الوسيط باعتباره حلقة وصل بين المتحكم أو المعالج والجهات المختصة. لذلك تتأكّد مسؤوليته عن الحفاظ على سرية المعلومات والبيانات التي يتلقاها تنفيذا لمهامه وصلاحياته.

المطلب الثاني: المسؤولية المدنية عن التعدّي على البيانات الشخصية الحسّاسة للعامل

تقسيم: تعد المسؤولية المدنية أحد الركائز القانونية المهمة التي تُقَام لحماية أفراد المجتمع من الأضرار التي تلحق بهم من غيرهم. فهي كما يُعرّفها البعض بأنها "مجموعة القواعد القانونية التي تلزم كل من سبب ضررا للغير بجبر هذا الضرر، وذلك بتعويض المضرور عما أصابه من ضرر" (العرعاري، 2011، ص 11)

ولا شك أن أي ضرر يلحق بالعامل نتيجة انتهاك بياناته الحساسة أو تداولها على نحو غير مشروع، أو كشف لأسراره، يوجب المسؤولية المدنية للمتسبب في ذلك. ورغم أن قانون حماية البيانات الشخصية، ولا حتى القانون الاتحادي رقم 2 لسنة 2019 بشأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية، لم يوردا نصا ينظم أحكام المسؤولية المدنية، خلافا للمرسوم بقانون اتحادي رقم (46) لسنة 2021 في شأن المعاملات الإلكترونية وخدمات الثقة، الصادر بتاريخ 20 سبتمبر 2021، الذي نص صراحة على مسؤولية مزودي خدمة الثقة عن أي ضرر بسبب الإخلال بالتزاماتهم القانونية. حيث نصت المادة 38 منه على أنه: "يتحمل مزودو خدمة الثقة

المسؤولية المدنية عن أي أضرار تلحق بأي شخص بسبب الإخلال بالالتزامات المنصوص عليها في هذا المرسوم بقانون ولائحته التنفيذية والقرارات الصادرة عن الهيئة"، وهو ما يعني بتقديرنا إحالة تنظيم تلك المسؤولية للقواعد العامة في قانون المعاملات المدنية. وعلى هذا الأساس سنتناول نطاق المسؤولية العقدية عن التعدّي عن البيانات الشخصية الحساسة للعامل (الفرع الأول)، ثم نطاق المسؤولية عن الفعل الضار (الفرع الثاني).

الفرع الأول: نطاق المسؤولية العقدية

يُنشئ عقد العمل التزامات متبادلة بين العامل وصاحب العمل (المتحكم)، إذ يلتزم هذا الأخير بموجب المادة 13 / 1 من قانون علاقات العمل، وكذا المادة 07 / 1 من قانون حماية البيانات الشخصية، بالاحتفاظ بملفات وسجلات العمال وفق الشروط والضوابط والإجراءات المنصوص عليها، وأن يتخذ كافة الإجراءات والتدابير التقنية والتنظيمية الملائمة لحماية وتأمين البيانات الشخصية والحفاظ على سريتها وخصوصيتها، وضمان عدم اختراقها (عميمر، 2020، ص444). ومن ثم فإن أي انتهاك لبيانات العامل الحسّاسة تسبّب فيها صاحب العمل، على غرار اختراق كلمات المرور الخاصة به، أو الاطلاع على بريده الإلكتروني من دون موافقة، أو التنصت على مكالماته واتصالاته، أو حتى الكشف عن بعض بياناته أو كلها لجهات غير مرخص لها بذلك، من شأنه أن يوجب مسؤوليته العقدية. ذلك أن أركان انعقادها متوافرة، فالإخلال بالالتزام التعاقدي بحفظ البيانات وحمايتها قائم، والضرر الذي أصاب العامل حاصل سواء كان ماديا أو معنويا

من جانب آخر نعتقد وخلافا لما يراه البعض (الخصاونة وآخرون، 2011، ص 15)، أن التزام صاحب العمل بحماية البيانات الشخصية الحساسة للعامل هو التزام بتحقيق نتيجة، مفاده عدم التعدّي أو انتهاك تلك البيانات، وألا يتم استخدامها أو تداولها إلا وفقا لمتطلبات العمل أو ما تقتضيه الإجراءات والتدابير القانونية. ومن ثم متى تم الإخلال بتلك الالتزامات وترتب حصول ضرر عنها للعامل، انعقدت مسؤولية صاحب العمل ما لم يثبت أن مصدر الضرر يعود لسبب أجنبي كخطأ العامل المضرور نفسه، أو خطأ الغير كالمعالج، أو المتحكم، أو غيرهما، أو بسبب قوة قاهرة لا يمكن دفعها.

وتجدر الإشارة إلى أن المسؤولية العقدية قد تتحول إلى مسؤولية عن الفعل الضار في حال ارتكب المتحكم غشاً أو خطأً جسيماً في تعامله مع البيانات الشخصية الحساسة للعامل. وهذا ما يمكن استنباطه من نص المادة (383) من قانون المعاملات المدنية الإماراتي التي تنص على أنه: "إذا كان المطلوب من المدين هو المحافظة على الشيء أو القيام بإدارته أو توخي الحيطة في تنفيذ التزامه فإنه يكون قد وفى بالالتزام إذا بذل في تنفيذه من العناية كل ما يبذله الشخص العادي ولو لم يتحقق الغرض المقصود هذا ما لم ينص القانون أو

الاتفاق على غير ذلك. وفي جميع الأحوال يبقى المدين مسئولاً عما يأتيه من غش أو خطأ جسيم". فالغش أو الخطأ الجسيم في معالجة البيانات الحسّاسة للعامل يخرج عن نطاق الالتزامات التعاقدية العادية ويرقى إلى مستوى الفعل الضار الذي يستوجب التعويض

ويتعزز هذا التوجه بما ورد في المادة (4) من قانون حماية البيانات الشخصية الإماراتي رقم 45 لسنة 2021، والتي تنص على أنه: "يُحظر معالجة البيانات الشخصية دون موافقة صاحبها، .....". فإذا تعمد المتحكم مخالفة هذا الحظر القانوني وأساء استخدام البيانات الشخصية الحسّاسة للعامل لتحقيق منافع شخصية، فإن مسؤوليته تتجاوز نطاق المسؤولية العقدية لتصبح مسؤولية عن فعل ضار، نظراً لجسامة الفعل وخروجه عن مقتضيات حسن النية في تنفيذ العقد (الخصاونة وآخرون، 2011، ص 16)

الفرع الثاني: نطاق المسؤولية عن الفعل الضار

تقسيم: تتطلب حماية البيانات الشخصية للعمال إمكانيات تقنية ومالية كبيرة، ما يجعل تلك البيانات محل تداول لدى جهات أخرى يلجأ إليها صاحب العمل بموجب نص القانون أو بموجب اتفاق، بغرض معالجتها وحمايتها. وفي كل الأحوال فإن أي تعدٍّ على هذه البيانات يوجب المسؤولية عن الفعل الضار لكل من لم يرتبط بعقد مع العامل، كالمعالج ومسؤول حماية البيانات ومزودي خدمة الإنترنت أو الاتصالات أو غيرهم، على اعتبار أن مصدر التزامهم هو نص القانون. كما قد يكون انتهاك البيانات من أشخاص أو جهات أخرى في شكل عمليات قرصنة لاختراق البيانات واستغلالها بصورة غير مشروعة

ولا شك أن انتهاك البيانات الحسّاسة للعامل يشكل عملا غير مشروع يوجب انعقاد المسؤولية عن الفعل الضار حال حصول ضرر للعامل، طبقا لنص المادة 282 من قانون المعاملات المدنية الاتحادي. وهو ما يعني ضرورة توافر أركانها الثلاث على التفصيل التالي.

الغصن الأول: فعل الإضرار: يعبّر الإضرار عن تجاوز الحد الواجب الوقوف عنده، أو الإخفاق في الوصول إلى الحد الواجب في الفعل أو الامتناع عنه، مما ينجم عنه حدوث الضرر (سرحان، 2010، ص 18). (زهرة، 2002، ص 85).

ويتحقق فعل الإضرار في مجال البيانات الشخصية الحساسة للعامل إما بالمباشرة أو بالتسبب، وفقاً لما نصت عليه المادة (283) من قانون المعاملات المدنية الإماراتي بأن: "يكون الإضرار بالمباشرة أو التسبب"

1. الإضرار بالمباشرة: يتحقق عندما يكون الفعل المؤدي للضرر متصلاً مباشرة بالنتيجة دون وساطة، وهو ما أكدته المادة (284) من قانون المعاملات المدنية بقولها: "إذا كان بالمباشرة لزم الضمان ولا شرط له". ومثال ذلك قيام صاحب

العمل أو شخص ما أو أي جهة أخرى باختراق البيانات أو تداولها أو كشف أسرار العمال وبياناتهم الحسّاسة على نحو غير مشروع بصورة مباشرة دون تدخل أي عنصر أو عامل آخر. أو قيام المتحكم بنشر البيانات الصحية الحسّاسة للعامل مباشرة على منصة إلكترونية. أو تعمد المعالج إرسال البيانات المالية للعامل إلى طرف ثالث غير مصرح له. ففي هذه الحالات يكون المباشر ضامناً للضرر بغض النظر عن توافر التعدي أو التعمد (العبيدي، 2018، ص 321).

2. الإضرار بالتسبب: يتحقق عندما يتداخل أو يشترك أكثر من سبب في حدوث الضرر، وهو ما نصت عليه الفقرة الثانية من المادة (283) من قانون المعاملات المدنية: "وإذا وقع بالتسبب فيشترط التعدي أو التعمد أو أن يكون الفعل مفضياً إلى الضرر". ومن أمثلته في مجال البيانات الشخصية؛ إهمال المتحكم في تأمين نظام حماية البيانات مما يسهل اختراقها. أو عدم تحديث برامج الحماية للأنظمة التي تحوي بيانات العمال الحسّاسة (الشرقاوي، 2019، ص 156). أو لم يتم تشفير البيانات والمعلومات الصحية أو المالية للعامل عند إرسالها أو تداولها، وغيرها من الحالات التي يتم من خلالها إلحاق الضرر بالعمال بالتسبّب نتيجة التعدّي أو التعمّد أو الإفضاء المؤدي للضرر غالبا.

3. اجتماع المباشر مع المتسبب: وفقاً للقاعدة العامة في المادة (284) من قانون المعاملات المدنية: "إذا اجتمع المباشر والمتسبب يضاف الحكم إلى المباشر". ومثال ذلك اشتراك المتحكم (متسبب) مع المعالج (مباشر) في تسريب بيانات العمال الحساسة لتحقيق منفعة مالية (الزرقا، 2004، ص 178).

ويمكن القول أن تحديد المسؤولية في مجال البيانات الشخصية الحساسة للعمال يتطلب تحليلاً دقيقاً لطبيعة الفعل الضار وظروف ارتكابه، مع الأخذ في الاعتبار الطبيعة الخاصة للبيانات محل الحماية وأثر الضرر الواقع على العامل

الغصن الثاني: الضرر: الضرر هو كل ما يمكن أن يؤثر سلبا على حقوق الفرد أو مصالحه المشروعة المتعلقة بالمال أو الجسم أو العرض والشرف (عبد الله، 1995، ص 71). والضرر شرط أساسي لانعقاد المسؤولية العقدية أو اللاعقدية أو الموضوعية، ذلك أن فعل الإضرار بغض النظر عن خطورته وجسامته، لا يلزم مرتكبه بالضمان ما لم يترتب عنه إلحاق ضرر بالغير. (الزحيلي، 1998، ص 23)، (سليم، 2007، ص 05)

وجدير بالإشارة أن الأضرار التي تصيب العمال نتيجة انتهاك بياناتهم الشخصية الحساسة قد تأخذ عدة صور وأشكال. فالكشف عن مثل هذه البيانات والمعلومات يمكن أن يؤدي إلى أشكال من التمييز والتحيّز (Lempen, 2017, P 274). فقد يدفع ذلك مثلا

الشركات وأصحاب العمل إلى الاهتمام أكثر بالعمال الذين يتمتعون بصحة جيدة ولهم قدرة على الإنتاج مع انخفاض تكاليفهم الطبية (Lequillerier, 2017, p 19)، أو ممن لهم خلفية إيديولوجية أو ثقافة. كما قد تتخذ شركات العمل الأخرى أو المؤسسات المالية المقرضة أو حتى أصحاب العقارات وشركات التأمين على الحياة وغيرها، قرارات برفض طلبات العمال أو التمييز بينها، بناء على ما تم كشفه وتداوله من بيانات ومعلومات

ويشترط في الضرر الناتج عن انتهاك البيانات الشخصية الحسّاسة للعامل عدة ضوابط أساسية، تشكل صورا للضرر القابل للتعويض وفقاً لقواعد قانون المعاملات المدنية الإمارات، نوجزها فيما يلي:

1. الضرر المحقق: تنص المادة (282) من قانون المعاملات المدنية الإماراتي على مبدأ عام مفاده أن "كل إضرار بالغير يلزم فاعله بضمان الضرر". كما تنص المادة (292) على أن "يقدر الضمان في جميع الأحوال بقدر ما لحق المضرور من ضرر وما فاته من كسب بشرط أن يكون ذلك نتيجة طبيعية للفعل الضار". ويشمل هذا في مجال انتهاك البيانات الشخصية الآثار المباشرة مثل الخسائر المادية والمعنوية التي تلحق بالعامل نتيجة تسريب بياناته الحساسة.

2. الضرر المباشر: وفقا لمضمون المادة (283) من قانون المعاملات المدنية، فإن الضرر المباشر هو ما يتصل بالفعل الضار دون وسائط. (الزحيلي، 2003، ص78).

3. الضرر الحال والضرر المستقبلي: تطبيقاً لنص المادة (292) من قانون المعاملات المدنية، يشترط في الضرر أن يكون محققاً، سواء كان حالاً أو مستقبلياً. وهو ما يعني أن الضرر المستقبلي يستوجب التعويض متى كان مؤكد الوقوع. (زهرة، 2002، ص 215).

4. نطاق التعويض: بناء على نص المادة (389) من قانون المعاملات المدنية، يتبين إذا لم يكن التعويض مقدراً في القانون أو في العقد، يُقدره القاضي بما يساوي الضرر الواقع فعلاً حين وقوعه. وهو ما يعني أن تقدير التعويض يشمل ما لحق المضرور من خسارة وما فاته من كسب. (سرحان، 2019، ص 143).

5. علاقة السببية: يُعد إثبات علاقة السببية أصعب أركان المسؤولية المدنية على المضرور، وأكثرها تعقيدا بسبب أنها تجمع بين الركنيين السابقين. ذلك أن العامل المضرور بسبب انتهاك بياناته أو إفشاء أسراره يتحمل في الأصل تبعة إثبات علاقة السببية بأن الضرر الحاصل له إنما كان بفعل المسؤول المباشر أو المتسبّب. ولما كان من الصعب التأكيد بشكل قاطع أن فعلًا معينًا هو السبب الفعلي للضرر، كان اللجوء إلى فكرة قرينة السببية كوسيلة لإثبات ذلك. فإذا كان الفعل الذي ينسب إلى المسؤول وهو صاحب العمل (المتحكم) أو المعالج أو مسؤول حماية البيانات أو جهة أخرى، قادرًا على إحداث الضرر بشكل معتاد، فإن القرينة تكون كافية لإثبات وجود علاقة السببية بينهما لصالح المضرور. فيتعيّن أنداك على المسؤول أن يواجه هذه القرائن بإثبات أن الضرر نشأ عن سبب خارجي لا علاقة له به. (حبيب، 2003، ص 241).

وبناء عليه يحق لمن قام بمعالجة البيانات أن يثبت أن الضرر الذي أصاب العام لم ينجم عن فعله، بل كان ناشئًا عن فعل الغير أو حتى عن فعل المضرور نفسه (عبد الله، 1995، ص 85)، كما لو قام العامل نفسه بكشف بياناته الشخصية الحساسة لجهة أخرى. وفي تقديرنا فإن علاقة السببية تمثل عاملاً أساسيًا لتحديد مدى الضمان وتكوين الالتزام، حيث يجب على من قام بمعالجة البيانات أن يقاوم القرائن التي تثبت وجود علاقة السببية بين معالجته والضرر الناجم. فإذا أثبت وجود سبب أجنبي لنفي العلاقة السببية، يكون حينئذ قد نجح دفع المسؤولية كليًا أو جزئيًا عن الضرر الناتج عن معالجة البيانات. ولا شك باعتقادنا أن استناد القانون إلى وجود سبب أجنبي يأتي للحفاظ على مبدأ العدالة وتحقيق التوازن المطلوب في تحمل المسؤولية.

وتتميز رابطة السببية في إطار المسؤولية عن الضرر الناشئ عن انتهاك البيانات الشخصية الحسّاسة للعامل في القانون الإماراتي بخصوصية مهمة، إذ تختلف أحكامها باختلاف نوع الإضرار، سواء كان بالمباشرة أو بالتسبب أو باجتماع كليهما كما أشرنا. وبناء عليه فإن مسؤولية المعالج (المباشر) عن انتهاك البيانات تختلف عن مسؤولية المتحكم (المتسبب)، حيث يكفي في الأولى مجرد وقوع الضرر لقيام المسؤولية. بينما يشترط في الثانية التعدي أو التعمد. كما أن السبب الأجنبي يؤثر في رابطة السببية بحسب طبيعة الإضرار، فقد نصت المادة (287) على أنه "إذا أثبت الشخص أن الضرر قد نشأ عن سبب أجنبي لا يد له فيه كآفة سماوية، أو حادث فجائي، أو قوة قاهرة، أو فعل الغير، أو فعل المتضرر كان غير ملزم بالضمان ما لم يقضِ القانون أو الاتفاق بغير ذلك". ولا شك أن هذا التمييز في أحكام السببية يعود لتأثر القانون الإماراتي بالفقه الإسلامي الذي يميز بين المباشرة والتسبب في الإضرار. (سرحان، 2010، ص 187)

الفرع الثالث: تعويض العامل عن أضرار انتهاك بياناته الشخصية الحسّاسة

يعد التعويض الوسيلة القانونية المثلى لجبر الضرر وتخفيف آثاره، فهو الجزاء القانوني لانعقاد المسؤولية المدنية عن أضرار انتهاك البيانات الشخصية الحساسة للعامل، تطبيقا للقواعد العامة الواردة في المواد (299)، (300)، (293) من قانون المعاملات المدنية الاتحادي. غير أن تعويض الأضرار الناجمة عن التعدّي على البيانات الشخصية الحساسة ذو طبيعة خاصة ومعقدة، نظرا لما تنطوي عليه حماية البيانات ومعالجتها وتداولها من أخطار وتحديات تتعلق أساسا بأمنها وحمايتها. يؤكد ذلك تعدّد الجهات التي تتعامل مع هذه البيانات، فضلا حالات الاختراق والقرصنة والاستخدام غير المشروع لتلك البيانات من جهات خارجية أخرى

ولا شك أن تقدير التعويض يكون في الأصل بناء على جسامة الضرر الحاصل متى تسبّب فيه المسؤول منفردا كالمتحكم أو المعالج أو الغير. غير أنه في حالة اشتراك أكثر من معالج أو شخص أو جهة في إحداث الضرر، انعقدت مسؤوليتهم بالتضامن وفقا لنص المادة 08 / 10 من قانون حماية البيانات الشخصية. ومن ثم تُقدَّرُ قيمة التعويض بناءً على معيار ذو شقين وهما؛ مدى الضرر، وجسامة الخطأ. ذلك أن معيار الضرر يحدد قيمة التعويض المستحق للعامل المتضرر، أما معيار الخطأ فيحدد نصيب كل مسؤول في مقدار التعويض. وحينئذ يُلزم به القاضي متى تمكن من تحديد نسبة خطأ كل واحد منهم بدقة، أما إذا لم يتبيّن ذلك فيلجأ إلى توزيع مقدار التعويض بينهم بالتساوي

ورغم أن قانون حماية البيانات الشخصية الاتحادي لم يتطرق لفكرة التعويض لا من قبيل الإشارة ولا من باب التفصيل، إلا أنه قد أدرج آلية جديدة تتناسب مع طبيعة البيانات الشخصية وإجراءات حمايتها وضمان سلامتها، تتمثل في تقديم الشكوى. حيث نصت المادة 24 من ذات القانون على أنه يحق لصاحب البيانات أن يقدم شكوى إلى مكتب الإمارات للبيانات متى تضرر، أو كان لديه اعتقاد بمعالجة غير مشروعة من المتحكم أو المعالج، أو أي مخالفة لأحكام القانون. حيث يتولى المكتب استلام الشكوى والتحقق منها بالتنسيق مع المتحكم والمعالج، ومن ثم توقيع الجزاءات الإدارية حال ثبوت مخالفة المتحكم (صاحب العمل) أو المعالج لأحكام القانون. وهو ما يُفسح المجال أمام العامل المتضرر للمطالبة بالتعويض.

وجدير بالإشارة أنه رغم الوعي بأهمية البيانات الشخصية الحسّاسة للعامل، وتأكيد القانون على المخاطر المحدقة بعدم حمايتها أو عدم اتخاذ ما يلزم لحفظها وعدم اختراقها، إلا أنه لم يورد أي نص قانوني بشأن إلزامية التأمين على عاتق المتحكم أو المعالج عن تلك المخاطر. ولا شك أن ذلك يشكل باعتقادنا قصور واضح وغير مبرر.

ذلك أن حجم المخاطر المرتبطة بالبيانات الشخصية للعامل لا سيما الحسّاسة منها، لا تقل أهمية وقيمة بحسب ما نراه عن أخطار حوادث المرور أو الحوادث الطبية أو غيرها مما ألزم بشأنها القانون بالتأمين الإجباري. وهو ما نوصي بتداركه وضرورة تنظيم أحكامه

الخاتمة:

لا يزال موضوع حماية البيانات الشخصية يشغل بال الهيئات التشريعية والدوائر التنظيمية، ويُثير اهتمام الفقهاء والقانونيين والمختصين. وقد تم في هذا البحث معالجة موضوعٍ لا يقل أهمية وإثارة قانونية ومعرفية، يتمثل في حماية البيانات الشخصية الحساسة للعامل. وبعد التطرق لمختلف جوانبه القانونية بالتحليل والمناقشة، تم التوصل إلى مجموعة من النتائج والتوصيات نوردها فيما يلي

أولا- النتائج:

- التأكيد على ضرورة التقيّد بالضوابط القانونية والشروط التنظيمية في حفظ وتخزين أو معالجة أو تداول البيانات الشخصية الحسّاسة للعامل، سواء ما تعلق منها بتلك المرتبطة بطبيعة البيانات في حد ذاتها، أو تلك المرتبطة بالعامل نفسه.

- قصور نصوص قانون تنظيم علاقات العمل في تكريس وتنظيم حماية البيانات الشخصية للعامل لا سيما الحسّاسة منها، بما يكمّل ويدعم الأحكام العامة الواردة في قانون حماية البيانات الشخصية.

- تقتضي متطلبات المصلحة العامة وفقا للمادة 02 من قانون حماية البيانات الشخصية، استثناء البيانات لدى الجهات الأمنية والقضائية من نطاق الحماية، مما قد يؤثر على خصوصية العامل وضمان حماية بياناته دون ضوابط محددة.

- يهدف التشريع الإماراتي إلى حماية حقوق العامل وضمان عدم استغلال بياناته الشخصية دون مبرر مشروع، من خلال تقييد معالجة البيانات بشرط الضرورة وإلزام جهة العمل بإعلام العامل بحدود وأسباب معالجة بياناته، مما يعزز مبدأ الشفافية والمشروعية.

- على الرغم من القيود الموجودة، لا يزال هناك مجال لتحديد فترة واضحة للاحتفاظ بالبيانات الشخصية الحساسة بعد انتهاء علاقة العمل، بما يحقق التوازن بين حماية حقوق العامل والمصالح الأخرى.

- خصّص قانون حماية البيانات الشخصية الاتحادي جملة من الضمانات القانونية والإجرائية، تشمل واجبات المتحكم والمعالج ومسؤول حماية البيانات، بما يضمن اتخاذ تدابير تقنية وتنظيمية وإبلاغ الجهات المعنية في حالة اختراق البيانات، مما يعزز الشفافية والمساءلة.

- تقع على عاتق صاحب العمل (المتحكم) مسؤولية تعاقدية لحماية بيانات العامل الشخصية، ويعتبر هذا الالتزام جزءًا من تنفيذ عقد العمل. ما يعني أن أي انتهاك للبيانات بسبب غش أو خطأ جسيم من قبل المتحكم، من شأنه أن يُحوّل المسؤولية إلى مسؤولية عن الفعل الضار عن الأضرار الناجمة.

ثانيا- التوصيات:

- إضافة فقرة جديدة للمادة الأولى من المرسوم بقانون اتحادي رقم 45 لسنة 2021 تنص على "تُعتبر من البيانات الشخصية الحساسة كذلك البيانات المالية للشخص الطبيعي بما فيها المعلومات المصرفية والائتمانية والضريبية، وكافة البيانات الشخصية المتعلقة بالأطفال العاملين دون سن الثامنة عشرة".

- نوصي بإدخال تعديل على قانون حماية البيانات الشخصية الاتحادي؛ ليشمل نصاً يُلزم صاحب العمل بتحديد فترة زمنية معينة للاحتفاظ بالبيانات الشخصية الحساسة للعامل بعد انتهاء علاقة العمل، مع استثناء يتيح الإبقاء على هذه البيانات لأغراض الضرورة في النزاعات القانونية أو الإدارية. شريطة إخفاء هوية العامل.

- ضرورة إدراج نصوص قانونية تكرّس حماية البيانات الشخصية الحسّاسة للعامل ضمن قانون تنظيم علاقات العمل، بما يحقق الانسجام والتكامل التشريعي بينه وبين قانون حماية البيانات الشخصية. وهو ما من شأنه أن يعزّز حماية أفضل للعامل ويحفظ حقوقهم، ويساعد القضاء في حل المنازعات العمالية المحتملة.

- توعية أصحاب العمل بأهمية اتخاذ التدابير الفنية والتنظيمية اللازمة لحماية البيانات الحسّاسة وتدريب الموظفين على التعامل الآمن والسليم مع هذه البيانات. مع ضرورة تفعيل الرقابة القانونية بشكل دوري ومستمر على عمليات معالجة البيانات الشخصية الحسّاسة، لضمان سلامتها وأمنها وتجنب أي انتهاكات أو اختراقات محتملة.

- إدراج نصوص قانونية تنظم أحكام المسؤولية المدنية بشكل صريح وواضح عقدية كانت أو لا عقدية، من حيث أساسها ونطاقها، بما يتناسب مع إقرار الحق في التعويض العادل والشامل للضرر.

قائمة المصادر والمراجع:

أولا- المراجع باللغة العربية:

أقرورو، سميرة (2022). الحماية القانونية للمعطيات الشخصية الحساسة: المعطيات الجينية أنموذجا: دراسة مقارنة. مجلة القانون والأعمال، 86.

أميرهم ، جيهان عادل (2020). أثر تحليل البيانات الضخمة "Big Data" على الأداء المالي والتشغيلي في منظمات الأعمال: دراسة تطبيقية. مجلة البحوث المالية والتجارية، 2.

البقلي، أيمن مصطفى أحمد (2021). حماية الخصوصية المعلوماتية لمستخدمي الإنترنت في مواجهة متطلبات التجارة الإلكترونية. المجلة القانونية، 9(4).

حبيب، عادل جبري (2003). المفهوم القانوني لرابطة السببية وانعكاساته في توزيع عبء المسئولية المدنية: دراسة مقارنة بأحكام الفقه الإسلامي. دار الفكر الجامعي.

الخصاونة، علاء الدين و الكساسبة، فراس ودرادكة، لافي محمد (2011). الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية. مجلة جامعة الشارقة للعلوم الشرعية والقانونية، 8(2).

راشد، طارق جمعة السيد (2019). الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي: دراسة مقارنة. مجلة القانون والاقتصاد.

ريان، إيمان أحمد (2021). الحماية التشريعية للحق في خصوصية البيانات في العصر الرقمي. مجلة الشريعة والقانون، 3(36).

الزحيلي، وهبة (1998). نظرية الضمان. دار الفكر.

زهرة، محمد المرسى (2002). المصادر غير الإرادية للالتزام في قانون المعاملات المدنية لدولة الإمارات العربية المتحدة: الفعل الضار والفعل النافع. مطبوعات جامعة الإمارات.

سرحان، عدنان (2010). المصادر غير الإرادية للالتزام الحق الشخصي الفعل الضار - الفعل النافع القانون: في قانون المعاملات المدنية الإماراتي وفقا لأصوله من الفقه الإسلامي: دراسة معززة بأحدث توجهات القضاء الإماراتي. مكتبة الجامعة.

سليم، محمد محيي الدين (2007). نطاق الضرر المرتد. دار المطبوعات الجامعية.

الشعيبى، فؤاد (2023). الحماية المدنية للبيانات الشخصية من المعالجة غير المشروعة في ضوء مرسوم القانون الاتحادي الإماراتي رقم 2021/45 بشأن حماية البيانات الشخصية. مجلة الدراسات القضائية، 13(24).

عبد الرحمن، محمود (2015). التطورات الحديثة لمفهوم الحق في الخصوصية: الحق في الخصوصية المعلوماتية. مجلة كلية القانون الكويتية العالمية، 3(9).

عبد الرحيم ، الحسين الزقيم محمد (2023). تسلل وسائل التكنولوجيا إلى دفاتر وأسرار الحياة الخاصة بالعامل. مجلة الفقه والقانون، 130.

عبد الله، عمر السيد أحمد (1995). مسؤولية الشخص عن فعله في قانون المعاملات المدنية الإماراتي مقارنا بالقانون المصري. دار النهضة العربية.

علي، نزيه محمد (2022). دور التشريعات والقوانين الوطنية والدولية الحاكمة لحماية امن المعلومات. المجلة

المصرية لبحوث الأعلام، 80.

عميمر، عبد القادر (2020). تأثير تكنولوجيا المعلومات على الحق في الحياة الخاصة. مجلة حوليات جامعة الجزائر 1، 34(1).

العتيبي، صالح ناصر (2015). الحق في الخصوصية في مواجهة التشريعات الوطنية: حماية حياة العامل الخاصة في قانون العمل الكويتي. مجلة كلية القانون الكويتية العالمية، 3(9).

العرعاري، عبد القادر (2011). مصادر الالتزام - المسؤولية المدنية(ط3). دار الأمان.

القانون الاتحادي رقم 25 لسنة 2023 في شأن نقل وزراع الأعضاء البشرية.

القانون الاتحادي رقم 8 لسنة 2019 بشأن المنتجات الطبية ومهنة الصيدلة المعدل.

القري، عبد الباسط (2023). حماية البيانات البيومترية السمعية البصرية في البيئة الرقمية: دراسة تحليلية للقانون الجزائري 18/7 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، 3(1).

المرسوم بقانون اتحادي رقم (33) لسنة 2021 بشأن تنظيم علاقات العمل.

المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

المرسوم بقانون اتحادي رقم (46) لسنة 2021 في شأن المعاملات الإلكترونية وخدمات الثقة.

الترجمة الصوتية لمصادر ومراجع اللغة العربية: Romanized Arabic References:

ʾaqrwrw sumayrata (2022). alḥimāyatu alqānawniyyatu lil-muʿṭayāti al-shakhṣiyyati alḥassāsati almuʿṭayātu al-jīniyyati unmūdhajan dirāsatun muqārinatun mijallatu alqānūni wa-l-ʾāʿmāli 86.

ʾamīruhum jayyahin ʿādil (2020). ʾatharu taḥlīli albayānāti al-ḍakhmati "Big Data" ʿalā alʾadāʾi almāliyyi wa-l-tashghīliyyi fī munaẓẓimāti alʾaʿmāli dirāsatun taṭbīqiyyatun mijallatu albuḥūthi almāliyyati wa-l-tijāriyyati 2.

albaqliyyu ʾaymanu muṣṭafā ʾaḥmada (2021). ḥimāyatu alkhuṣūṣiyyati almiʿliwwamiātya limussittakhdimy alʾintarniti fī mūājahati mutaṭallabāti al-tijārati alʾilktrūniyyati almajallatu alqānawniyyatu 9(4).

ḥabībun ʿādil jabrī (2003). almafhūmu alqaʾanwiniyyu lirābiṭati al-sababiyyati waʾanʿikāsuāthu fī tawzīʿi ʿabʾi almasʾiūliyyati almadaniyyati dirāsatun muqāranatun biʾaḥkāmi alfiqhi alʾislāmiyyi dāru alfikri aljāmiʿiyyi

alkhaṣāwunatu ʿalāʾu al-dīni w alkusāsibatu firāsun wadarādakatu lāfī muḥammad (2011). alḥimāyatu alqānawniyyatu lil-khuṣūṣiyyati wa-l-bayānāti al-shakhṣiyyati fī niṭāqi almaʿliwimmitya mijallatu jāmiʿati al-shāriqati lil-ʿulūmi al-sharʿiyyati wa-l-qqianwinnayi 8(2).

rāshidun ṭāriqu jumuʿati al-sayyidi (2019). alḥimāyatu alqānawniyyatu likhuṣūṣiyyati albayānāti al-shakhṣiyyati fī alʿaṣri al-raqmiyyi dirāsatun muqāranatun mijallatu alqānūni wa-l-iāqtiṣādi

rayyānu ʾīmānu ʾaḥmada (2021). alḥimāyatu al-tashrīʿiyyatu lil-ḥaqqi fī khuṣūṣiyyati albayānāti fī alʿaṣri al-raqmiyyi mijallatu al-sharīʿati wa-l-qānūni 3(36).

al-zuḥayliyyu wahibatu (1998). naẓariyyati al-ḍamāni dāru alfikri

zahratu muḥammadu almarsā (2002). almaṣādiru ghayru alʾirādiyyati lil-iāltizāmi fī qānūni almuʿāmalāti almadaniyyati lidawlati alʾimārāti alʿarabiyyati almuttaḥidati alfiʿla al-ḍārru wa-l-fiʿlu al-nāfiʿu maṭbūʿātu jāmiʿati alʾimārāti

sirḥānu ʿadnāna (2010). almaṣādiru ghayru alʾirādiyyati lil-iāltizāmi alḥaqqu al-shakhṣiyyu alfiʿlu al-ḍārru - alfiʿlu al-nāfiʿu alqānūnu fī qānūni almuʿāmalāti almadaniyyati alʾimāarittī wafqan liʾuṣūlihi mina alfiqhi alʾislāmiyyi dirāsatun muʿazzazatun biʾaḥdathi tawajjuhāti alqaḍāʾi alʾimāarittī maktabatu aljāmiʿati

sulaymun muḥammadu muḥyī al-dīni (2007). niṭāqu al-ḍarari almurtaddi dāru almaṭbūʿāti aljāmiʿiyyatu

al-shuʿaybā fuʾuādun (2023). alḥimāyatu almadaniyyatu lil-byāniāt al-shakhṣiyyati mina almuʿālajati ghayri almashrūʿati fī ḍawʾi marsūmi alqānūni alitaḥiddī alʾimāarittī raqmi 2021/45 bishaʾani ḥimāyati albayānāti al-shakhṣiyyati mijallatu al-dirāsāti alqaḍāʾiyyati 13(24).

ʿabdu al-Raḥmāni maḥmūdin (2015). al-taṭawwurātu alḥadīthatu limafhūmi alḥaqqi fī alkhuṣūṣiyyati alḥaqqu fī alkhuṣūṣiyyati almiʿliwwamiātya mijallatu kulliyyati alqānūni alkawītiyyatu alʿālamiyyatu 3(9).

ʿabdu al-raḥīmi alḥusayni al-zaqīmi muḥammad (2023). taslulu wasāʾilu al-tiknūlūjyā ʾilā dafātiri waʾasrāri alḥayāti alkhāṣṣati bi-l-ʿāmili mijallatu alfiqhi wa-l-qānūni 130.

ʿabd Allāhi ʿumara al-sayyidi ʾaḥmadu (1995). masʾūliyyatu al-shakhṣi ʿan fiʿlihi fī qānūni almuʿāmalāti almadaniyyati al-ʾimāarittī muqārinan bi-l-qqiānawni almiṣriyyi dāru al-nahḍati alʿarabiyyati

ʿaliyyun nazīh muḥammad (2022). dawru al-tashrīʿāti wa-l-qawānīni alwaṭaniyyati wa-l-diwalyi#ta alḥākimati liḥimāyati amni almaʿlūmāti almajallatu almiṣriyyatu libuḥūthi alʾaʿlāmi 80.

ʿumaymirun ʿabdu alqādiri (2020). taʾathīru tiknūlūjyā almaʿlūmāti ʿalā alḥaqqi fī alḥayāti alkhāṣṣati mijallatu ḥawliyyāti jāmiʿati aljazāʾiri 1، 34(1).

alʿutaybiyyu ṣāliḥu nāṣirin (2015). alḥaqqu fī alkhuṣūṣiyyati fī mūājahati al-tashrīʿāti alwaṭaniyyati ḥimāyatu ḥayāti alʿāmili alkhāṣṣati fī qānūni alʿamali alkiwaytiyyi mijallatu kulliyyati alqānūni alkawītiyyatu alʿālamiyyati 3(9).

alʿarʿāriyyu ʿabdu alqādiri (2011). maṣādiru aliāltizāmi - al-masʾūliyyatu almadaniyya#iṭ dāru alʾamāni

alqānūnu alitaḥidduy rqmu 25 lsna 2023 fī shaʾani naqli wazirāʿi alʾaʿḍāʾi albashariyyati

alqānūnu alitaḥidduy rqmu 8 lsna 2019 bisha'ani almuntajāti al-ṭibbiyyati wamihnati al-ṣiyadlati almu'addali

alqurriyyi 'abdu albāsiṭi (2023). ḥimāyatu albayānāti albayū'imtiryyati al-sam'iyyati albaṣariyyati fī albī'iati al-raqmiyyati dirāsatun taḥlīliyyatun lil-qānūni al-jazā'iriyyi 18/7 almuta'alliqu biḥimāyati al'ashkhāṣi al-ṭabī'iyyīna fī majāli mu'ālajati almu'ṭayāti dhāti al-ṭāba'i al-shakhṣiyyi almajallatu al'arabiyyatu al-dawliyyatu litakaniwwaliwjyā alma'lūmāti wa-l-bayānāti 3(1).

al-marsūmu biqānūnin atḥiāadyi rqmu (33) lsna 2021 bisha'ani tanẓīmi 'alāqāti al-'amali

al-marsūmu biqānūnin atḥiāadyi raqmu (45) lisanati 2021 bisha'ani ḥimāyati albayānāti al-shakhṣiyyati

almarsūmu biqānūnin atḥiāadyi raqmu (46) lasinti 2021 fī sha'ani almu'āmalāti al'ilikitrūniyyati wakhadamāti al-thiqati

ثانيا- المراجع باللغة الأجنبية:

Bourdillon- Stalla, S. & Knight, A. (2017). Anonymous data v. personal data - a false debate: an EU perspective on anonymization, pseudonymization and personal data: Wisconsin International Law Journal, 34(2), 284-322.

Dubois, C. (2017). Protection des données personnelles : contexte international et avant-projet de réforme du conseil fédéral. Livre La protection des données dans les relations de travail. Centre d'étude des relations de travail, Schulthess Éditions Romandes.

Fanti, S. (2017). Protection des données informatiques. Livre La protection des données dans les relations de travail, Centre d'étude des relations de travail, Schulthess Éditions Romandes.

Flueckiger, C. (2017). Principes généraux de la protection des données et communications transfrontières dans le cadre des relations de travail. Livre La protection des données dans les relations de travail, Centre d'étude des relations de travail, Schulthess Éditions Romandes.

Lempen, K. (2017). Protection des données informatiques, Livre La protection des données dans les relations de travail. Centre d'étude des relations de travail, Schulthess Éditions Romandes.

Leonelli, S. & Lovell, B. & Flemingm, L. & Wheeler, B. & Williams, H. (2021). From Fair Data to Fair Data Use: Methodological Data Fairness in Health-Related Social Media Research. Big Data and Society, 8 (1), 1-9.

Lequillerier, C. (2017). L'impact de l'intelligence artificielle sur la relation de soin. Journal de Droit de la Santé et de l'Assurance Maladie, 17, 14-20.

Major, M. (2017). Le droit d'accès de l'employé à son dossier personnel. Livre La protection des données dans les relations de travail, Centre d'étude des relations de travail, Schulthess Éditions Romandes.

Ma, R. (2023). Legislative Conception for the Special Protection of Biometric Information: A Study Based on Extraterritorial Experience. Proceedings of the International Conference on Social Psychology and Humanity StudiesDOI: 10.54254/2753-7048/10/20230195. https://www.researchgate.net/publication/373922175.

Ouannass, A. (2022). The Impact of the UAE's New Data Protection Law on Labor Law. https://www.roedl.com/insights/uae-data-protection-law-labor-law.

Sylvie Dupont, A. (2017). La protection des données confiées aux assureurs. Livre La protection des données dans les relations de travail, Centre d'étude des relations de travail, Schulthess Éditions Romandes.

Walter Philippe, J. (2017). Accès aux documents officiels contenant des données personnelles et droit à la protection des données. Livre La protection des données dans les relations de travail, Centre d'étude des relations de travail, Schulthess Éditions Romandes.

Wayman, J. & McIver, R. & Waggett, P. & Clarke, S. & Mizoguchi, M. & Busch, C. & Delvaux, N. & Zudenkov, A. (2014). Vocabulary harmonisation for biometrics: The development of ISO/IEC 2382 Part 37. Biometrics, IET. 3. 1-8. 10.1049/iet-bmt.2013.0003.

Views on the Civil Protection of Sensitive Personal Data of Workers "A Study in the UAE Legislation"

Walid Abdullah Matar Al-Khuzaimi(1)
Mourad Benseghir(2)

Abstract:

Protecting sensitive personal data, especially in the workplace, has become increasingly important in light of the rapid digital transformation, the evolving concept of privacy, and its expanding scope. Protecting the workers' personal data has become an urgent necessity to protect their privacy and guarantee their rights to the security and integrity of their data, in the face of the risks of violation, misuse, or leakage, which may negatively affect their career path, job opportunities, promotions, or lead to other legal risks and challenges.

This research deals with the legal protection of sensitive data of workers, which the UAE legislation sought to enshrine through very recent laws, such as Law No. 45 of 2021 regarding the protection of personal data, as well as Law No. 33 of 2021 regarding the regulation of labor relations as amended. The main issue of the research revolves around the question: What is the scope of protection dedicated to the sensitive data of workers? What are its established guarantees?

The study addresses the basis and scope of protecting this data, highlighting the regulations and provisions for its enshrinement, in addition to stating the most important guarantees and mechanisms provided by the UAE legislation to enhance this protection. It also addresses the law enforcement measures and the establishment of civil liability in case the worker's sensitive personal data is harmed.

The research concludes that processing entities and employers must adhere to transparency, fairness, legality, and informed consent when collecting and processing the workers' sensitive personal data, as essential safeguards. In addition to ensuring workers' rights to the safety and security of their data and its reliable and legitimate use. It also calls for the inclusion of additional practical guarantees to protect such data, as well as the enforcement of comprehensive security measures coupled with appropriate legal penalties in case of violations.

Keywords: sensitive personal data, employment contract, workers, processing, protection, liability, compensation.

(1) College of Law - University of Sharjah (Sharjah - U.A.E)
U20105619@sharjah.ac.ae

(2) (2)College of Law - University of Sharjah (Sharjah - U.A.E)