المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الحماية الجنائية للبيانات الشخصية المُعالجة إلكترونياً في التشريع الإماراتي

(دراسة تحليلية)

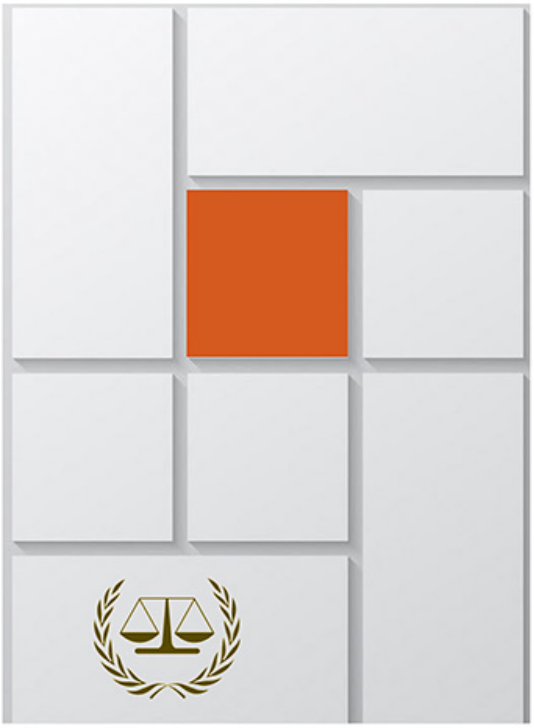
إعداد:
فاطمة خميس حميد النقبي
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الحماية الجنائية للبيانات الشخصية المُعالجة إلكترونياً في التشريع الإماراتي

(دراسة تحليلية)



إعداد:
فاطمة خميس حميد النقبي
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الحماية الجنائية للبيانات الشخصية المُعالجة إلكترونياً في التشريع الإماراتي (دراسة تحليلية)

إعداد:
فاطمة خميس حميد النقبي
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

منشورات المركز العربي للبحوث القانونية والقضائية
العنوان: بيروت -منطقة الأشرفية-شارع بيضون- مقابل فصيلة قوى الأمن الداخلي
الموقع الإلكتروني: www.carjj.org
البريد الإلكتروني: arab.league@carjj.org
تلفون:009611200281 / 009611200283

فاكس: 009611200280

المقدمة

في عصر يتسارع فيه نمو البيانات الرقمية وتقنيات المعلومات بوتيرة غير مسبوقة، أصبحت الحاجة ملحة لوضع إطار قانوني فعّال يضمن حماية البيانات الشخصية ويحد من إساءة استخدامها. التشريع الإماراتي، في هذا السياق، يواجه تحديات جمّة تستدعي التحليل والدراسة للوقوف على مدى قدرته على توفير حماية جنائية كافية للبيانات الشخصية المعالجة إلكترونياً. إن هذه الدراسة تسعى لرصد وتحليل الإطار القانوني الحالي في الإمارات، مع التركيز على الجوانب الجنائية لحماية البيانات الشخصية، بغية تقديم رؤية شاملة تسهم في فهم هذا الموضوع بعمق(1).

إن حماية البيانات الشخصية تتجاوز كونها مسألة قانونية فحسب، فهي تمس أبعاداً متعددة تتعلق بالخصوصية والأمان الرقمي وثقة المستخدمين في النظم الإلكترونية. في الإمارات، حيث تحتل التكنولوجيا مكانة مركزية في الخطط التنموية ورؤية الدولة المستقبلية، يبرز التحدي في كيفية التوفيق بين دعم الابتكار والتحول الرقمي من جهة، وحماية البيانات الشخصية والحفاظ على الخصوصية من جهة أخرى(2).

التشريع الإماراتي، على مر السنين، قد اتخذ خطوات مهمة نحو تعزيز حماية البيانات الشخصية، إلا أن هناك حاجة دائمة للتقييم والتحديث لضمان مواكبته للتطورات التكنولوجية والتحديات الجديدة التي تظهر بشكل مستمر. إن فحص وتحليل الإجراءات الجنائية المتعلقة بحماية البيانات الشخصية في الإمارات يشكل جزءاً أساسياً من هذه الدراسة، بغية تقديم توصيات مدروسة تسهم في تعزيز الحماية الجنائية للبيانات الشخصية وتحقيق التوازن بين مختلف المصالح المعنية(3).

من خلال التحليل العميق والمنهجي، تسعى هذه الدراسة إلى إلقاء الضوء على الجوانب القانونية والتحديات المتعلقة بحماية البيانات الشخصية في الإمارات، وذلك بغية المساهمة في تطوير الإطار القانوني وتعزيز الحماية الجنائية للبيانات الشخصية، ما يشكل خطوة أساسية نحو بناء مجتمع رقمي آمن وموثوق.

أولاً: مشكلة البحث:

تكمن مشكلة هذا البحث في استقصاء مدى كفاءة وفعالية التشريع الإماراتي في توفير حماية جنائية قوية للبيانات الشخصية التي يتم معالجتها إلكترونياً، في ظل الانفجار الهائل للبيانات وتطور تقنيات المعلومات بوتيرة سريعة. تتجلى التحديات في كيفية تحديث الأطر القانونية وتطويرها بما يتماشى مع المستجدات التكنولوجية والمخاطر المتزايدة المتعلقة بإساءة استخدام البيانات الشخصية، وكذلك في ضمان تحقيق التوازن بين حماية الخصوصية ودعم الابتكار والتحول الرقمي. إضافةً إلى ذلك، تبرز التساؤلات حول مدى قدرة الأنظمة الرقابية والإجراءات القانونية المتبعة في الإمارات على التعامل بفعالية مع التحديات المعاصرة المتعلقة بحماية البيانات الشخصية وضمان المساءلة والشفافية في حال حدوث انتهاكات. يستدعي ذلك تحليلاً دقيقاً وعميقاً للتشريعات والسياسات الحالية، بغية تقديم توصيات عملية وفعّالة تسهم في تحسين الإطار القانوني وتعزيز حماية البيانات الشخصية في الإمارات.

ثانياً: أهمية البحث:

يكتسب هذا البحث أهمية بالغة في ظل التحول الرقمي المتسارع والاعتماد المتزايد على تقنيات المعلومات في مختلف مناحي الحياة، مما يجعل موضوع الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً قضية رئيسية تستلزم البحث والتحليل. يسعى البحث إلى تسليط الضوء على التشريعات والأنظمة القائمة في الإمارات العربية المتحدة وتقييم فعاليتها في ضمان حماية البيانات الشخصية، وتحديد الفجوات والتحديات التي قد تعيق تحقيق الحماية الكاملة، وتقديم توصيات عملية لتحسين الإطار القانوني والتنظيمي في هذا المجال. ويمكننا تقسيم هذه الأهمية إلى أهمية نظرية وأهمية تطبيقية، وذلك على النحو التالي:

1- **الأهمية النظرية:** تكمن الأهمية النظرية لهذا البحث في إثراء المعرفة القانونية وتعزيز الفهم النظري حول قضايا حماية البيانات الشخصية في البيئة الرقمية، وذلك من خلال

استقصاء التشريعات والمبادئ القانونية التي تحكم هذا المجال في الإمارات العربية المتحدة. يسعى البحث إلى تحليل الأطر النظرية المتعلقة بحقوق الأفراد في الخصوصية وحماية بياناتهم الشخصية، وكذلك استكشاف الآثار القانونية والأخلاقية المترتبة على معالجة البيانات الشخصية إلكترونياً. يمهد هذا التحليل الطريق لبناء أساس نظري قوي يساهم في تطوير السياسات والتشريعات المستقبلية في هذا المجال.

2- **الأهمية التطبيقية:** تبرز الأهمية التطبيقية لهذا البحث في تقديم حلول عملية وتوصيات قابلة للتنفيذ لتعزيز حماية البيانات الشخصية في الإمارات العربية المتحدة. يسعى البحث إلى تقديم إطار عمل قانوني وتنظيمي محدث يتماشى مع المستجدات التكنولوجية ويعالج التحديات الراهنة في مجال حماية البيانات. يُركز البحث على تحليل الآليات القانونية المتاحة للأفراد للدفاع عن حقوقهم في حال حدوث انتهاكات لخصوصيتهم، ويقدم توجيهات عملية للجهات المعنية والمشرعين لتعزيز الحماية الجنائية للبيانات الشخصية وضمان المساءلة والشفافية.

ثالثاً: أهداف البحث:

1- تحديد وتوضيح مفهوم البيانات الشخصية وأنواعها، مع التركيز على التطور التاريخي لحمايتها.

2- تحليل الضوابط القانونية لمعالجة البيانات الشخصية والحماية الجنائية المقدمة في التشريع الإماراتي.

3- استعراض وتقييم التشريعات الخاصة بتجريم الاعتداء على البيانات الشخصية، بما في ذلك الحماية الجنائية للسر المهني.

4- تحليل الحالات التي يمكن فيها معالجة البيانات الشخصية دون الحصول على موافقة صاحبها، وكذلك القواعد المنظمة لنقل ومشاركة البيانات الشخصية عبر الحدود.

5- استكشاف الآليات القانونية لتقديم الشكاوى والتظلمات في حالات انتهاك حماية البيانات الشخصية، وتقييم فعاليتها في ضمان حقوق الأفراد.

رابعاً: منهج البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي في دراسته للحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في التشريع الإماراتي، حيث يسعى إلى توصيف وتحليل الظواهر والأحكام القانونية المتعلقة بحماية البيانات الشخصية، مع العمل على تفسير النصوص التشريعية ذات الصلة. يتبنى البحث منهجاً استقرائياً في تحليل البيانات والمعلومات المتاحة، معتمداً على مجموعة متنوعة من المصادر، بما في ذلك الكتب القانونية، والمقالات العلمية، والتشريعات، والأحكام القضائية،

وغيرها من المواد ذات الصلة. يهدف البحث إلى الكشف عن الفجوات والتحديات في التشريع الحالي، وتقديم توصيات لتعزيز الحماية الجنائية للبيانات الشخصية في الإمارات، مع التأكيد على أهمية التوازن بين حماية الخصوصية والمصلحة العامة. يركز البحث أيضاً على تحليل الإجراءات القانونية المتاحة للأفراد في حال تعرض بياناتهم الشخصية للخطر، ودور الهيئات الرقابية في ضمان الالتزام بالقوانين والتشريعات المعمول بها.

خامساً: هيكل البحث:

مبحث تمهيدي: ماهية البيانات الشخصية.

المطلب الأول: تعريف البيانات الشخصية.

المطلب الثاني: أنواع البيانات الشخصية.

المطلب الثالث: التطور التاريخي لحماية البيانات الشخصية.

الفصل الأول: صور الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً.

المبحث الأول: ضوابط معالجة البيانات الشخصية.

المطلب الأول: حظر جمع البيانات أو معالجتها أو إفشائها إلا بموافقة الشخص المعني.

المطلب الثاني: تقرير بعض الحقوق للشخص المعني بالبيانات على بياناته.

المطلب الثالث: فرض بعض القيود والالتزامات على عمليات جمع البيانات وتحليلها أو معالجتها والاحتفاظ بها.

المبحث الثاني: تجريم الاعتداء على البيانات الشخصية في قانون الجرائم والعقوبات.

المطلب الأول: تجريم الاعتداء على حرمة الحياة الخاصة للأفراد

المطلب الثاني: الحماية الجنائية للسر المهني وتجريم إفشائه

المبحث الثالث: تجريم الاعتداء على البيانات الشخصية في القوانين الخاصة.

المطلب الأول: حماية البيانات الشخصية في المرسوم بالقانون الاتحادي رقم (15) لسنة 2020 في شأن حماية المستهلك.

المطلب الثاني: حماية البيانات الشخصية في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

الفصل الثاني: حالات معالجة البيانات الشخصية.

المبحث الأول: حالات معالجة البيانات الشخصية بدون موافقة صاحبها.

المطلب الأول: أن تكون المعالجة ضرورية لحماية المصلحة العامة.

المطلب الثاني: أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات.

المطلب الثالث: أن تكون المعالجة ضرورية لحماية الصحة العامة.

المبحث الثاني: نقل ومشاركة البيانات الشخصية عبر الحدود.

المطلب الأول: نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال وجود مستوى حماية ملائم.

المطلب الثاني: نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال عدم وجود مستوى حماية ملائم.

المبحث الثالث: تقديم الشكوى والتظلم لضمان حماية البيانات الشخصية.

المطلب الأول: تقديم الشكوى في حالة وجود مخالفة تتعلق بمعالجة البيانات الشخصية

المطلب الثاني: التظلم من قرارات مكتب الإمارات للبيانات.

الخاتمة.

قائمة المراجع.

مبحث تمهيدي

ماهية البيانات الشخصية

تمهيد وتقسيم:

البيانات الشخصية تمثل مجموعة من المعلومات التي تتعلق بالأفراد والتي يمكن استخدامها لتحديد هويتهم، سواء كانت هذه المعلومات مباشرة أو غير مباشرة. وتشمل هذه البيانات مختلف العناصر كالاسم، العنوان، رقم الهاتف، تاريخ الميلاد، بيانات الهوية الوطنية، وغيرها من المعلومات التي يمكن أن ترتبط بشكل خاص بالأفراد. وفي سياق العصر الرقمي والتحول الرقمي الذي نشهده، أصبحت البيانات الشخصية تعالج بشكل إلكتروني بصورة متزايدة، مما يعني تخزينها ومعالجتها ونقلها عبر الأنظمة الإلكترونية وشبكات الإنترنت[4].

تكمن أهمية البيانات الشخصية في كونها تشكل جزءاً أساسياً من الخصوصية الفردية، حيث يعتبر حمايتها حقاً أساسياً للأفراد، وتلعب دوراً حيوياً في الحفاظ على سرية معلوماتهم وحمايتها من التعديات والاستخدامات غير المشروعة. وفي هذا الإطار، يأتي التشريع الإماراتي ليضع مجموعة من القواعد والمعايير القانونية التي تهدف إلى حماية البيانات الشخصية وضمان معالجتها بطريقة آمنة ومشروعة[5].

يتطلب حماية البيانات الشخصية تحديداً دقيقاً لماهيتها وطبيعتها، وكذلك فهم السياق الذي يتم فيه جمعها ومعالجتها. ويشمل ذلك تحديد الأغراض التي يتم من أجلها جمع البيانات، والتدابير الأمنية المتخذة لحمايتها، والحقوق التي يتمتع بها الأفراد فيما يتعلق ببياناتهم الشخصية. ويتطلب أيضاً وضع آليات فعّالة لمراقبة وتدقيق كيفية معالجة البيانات، وضمان التزام الأطراف المعنية بالمعايير والقوانين المعمول بها[6].

وللتعرف على ماهية البيانات الشخصية، سيتم تقسيم هذا المبحث إلى ثلاثة مطالب، وذلك على النحو التالي:

المطلب الأول: تعريف البيانات الشخصية.

المطلب الثاني: أنواع البيانات الشخصية.

المطلب الثالث: التطور التاريخي لحماية البيانات الشخصية.

المطلب الأول

تعريف البيانات الشخصية

البيانات الشخصية في سياق التشريع الإماراتي، وكما هو متعارف عليه في الممارسات القانونية الدولية، تُعرَّف بأنها أي معلومات تتعلق بشخص طبيعي معين يمكن التعرف عليه من خلالها، سواء كان ذلك بشكل مباشر من خلال الاسم أو الرقم الشخصي، أو بشكل غير مباشر من خلال ربطها بعناصر أخرى كالعنوان الجغرافي أو بيانات الاتصال. وتشمل البيانات الشخصية مجموعة واسعة من المعلومات مثل البيانات البيوغرافية، سجلات العمل، البيانات المالية، والمعلومات الصحية. يكمن التحدي في حماية هذه البيانات في كونها تُجمع وتُخزن وتُعالج إلكترونيًا، مما يعرضها لمخاطر التسريب والاستغلال غير المشروع. التشريع الإماراتي، من خلال قوانينه ولوائحه، يسعى إلى إرساء قواعد واضحة ومحددة لضمان حماية البيانات الشخصية، مع التركيز على ضرورة وضع تدابير أمان فعالة وإلزام الجهات المعنية باتباع أفضل الممارسات لضمان سلامة وخصوصية البيانات الشخصية. هذا يتطلب وعياً قانونياً وتقنياً عالياً من الجهات المعنية، واستعداداً للتكيف مع التطورات المستمرة في عالم التكنولوجيا وأمان المعلومات[7].

في دولة الإمارات العربية المتحدة، تم تعريف البيانات الشخصية في المادة (1) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية بأنها: "أي بيانات تتعلق بشخص طبيعي محدد، أو تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر من خلال الربط بين البيانات، من خلال استخدام عناصر التعريف كاسمه، أو صوته، أو رقمه التعريفي، أو المعرف الإلكتروني الخاص به، أو موقعه الجغرافي، أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية، أو الاقتصادية، أو الثقافية، أو الاجتماعية، وتشمل البيانات الشخصية الحساسة والبيانات الحيوية البيومترية"[8].

المادة القانونية المشار إليها هنا تعتبر ركناً أساسياً في تشريع حماية البيانات الشخصية في دولة الإمارات العربية المتحدة، حيث تقدم تعريفاً شاملاً وواضحاً لما يُعتبر "بيانات شخصية". يتم التركيز في هذا التعريف على الارتباط الوثيق بين البيانات والشخص الطبيعي، مما يؤكد على أهمية حماية الخصوصية والحفاظ على السرية[9].

التعريف يستخدم عبارة "أي بيانات"، وهو ما يشير إلى شمولية التعريف وعدم تقييده بنوع معين من البيانات. هذا يعني أن أي معلومات يمكن أن تُستخدم لتحديد هوية الشخص أو التعرف عليه بشكل مباشر أو غير مباشر تقع تحت بند البيانات الشخصية. الإشارة إلى "الشخص الطبيعي" تؤكد أن التعريف يتعلق بالأفراد الحقيقيين وليس الكيانات القانونية[10].

توضح المادة أيضاً كيف يمكن التعرف على الشخص من خلال الربط بين مختلف البيانات، وتُبرز أهمية "عناصر التعريف" مثل الاسم، الصوت، الرقم التعريفي، المعرف الإلكتروني، الموقع الجغرافي وغيرها. هذا يدل على أن عملية حماية البيانات الشخصية لا تتعلق فقط بالمعلومات الأساسية، بل تمتد لتشمل كل ما يمكن أن يُستخدم لتحديد هوية الشخص[11].

الإشارة إلى "البيانات الشخصية الحساسة" و"البيانات الحيوية البيومترية" تعكس الاعتراف بوجود فئات خاصة من البيانات التي تتطلب مستوى أعلى من الحماية نظراً لطبيعتها الحساسة والخاصة. هذا يؤكد على ضرورة اتخاذ تدابير حماية خاصة ومشددة لضمان عدم التعرض للإساءة أو الاستغلال[12].

وترى الباحثة، أن هذه المادة تُعتبر خطوة هامة نحو تعزيز حماية البيانات الشخصية في الإمارات، وتوفير إطار قانوني واضح يُحدد المسؤوليات والالتزامات المتعلقة بحماية هذه البيانات. وهي تُشدد على أهمية توخي الحذر واتخاذ الإجراءات اللازمة لضمان خصوصية الأفراد وحماية معلوماتهم الشخصية.

المطلب الثاني

أنواع البيانات الشخصية

البيانات الشخصية تأخذ أشكالاً وأنواعاً متعددة، ويمكن تصنيفها بناءً على مختلف المعايير والسمات. بشكل عام، يمكن تقسيم البيانات الشخصية إلى فئتين رئيسيتين: البيانات الشخصية العادية والبيانات الشخصية الحساسة. البيانات الشخصية العادية تشمل المعلومات الأساسية مثل الاسم، العنوان، رقم الهاتف، وعنوان البريد الإلكتروني. أما البيانات الشخصية الحساسة، فهي تشمل المعلومات التي يمكن أن تؤدي إلى تمييز أو تفرقة ضد الفرد، مثل البيانات الصحية، المعتقدات الدينية، الانتماء السياسي، والبيانات الجنسية[13].

في الإمارات، يولى اهتمام خاص بحماية البيانات الشخصية، وتحديداً البيانات الشخصية الحساسة، حيث يتطلب القانون توفير مستويات عالية من الحماية واتخاذ تدابير أمان إضافية لضمان سلامة هذه البيانات وحمايتها من الإساءة أو الاستغلال. يشدد التشريع الإماراتي على ضرورة الشفافية والوضوح فيما يتعلق بكيفية جمع البيانات واستخدامها ومشاركتها، ويمنح الأفراد حقوقاً واسعة للوصول إلى بياناتهم الشخصية وتصحيحها وحذفها عند الحاجة[14].

في هذا السياق، يتوجب على الجهات التي تتعامل مع البيانات الشخصية أن تكون على دراية كاملة بأنواع البيانات التي تعالجها، وأن تكون ملتزمة باتخاذ جميع التدابير اللازمة لحماية هذه البيانات

وضمان معالجتها بطريقة قانونية وآمنة. يتطلب ذلك وعياً مستمراً بالتحديات والمخاطر المرتبطة بمعالجة البيانات الشخصية، والاستعداد لمواجهتها بفعالية لضمان حماية خصوصية الأفراد وسلامة معلوماتهم الشخصية[15].

وقد صنف المشرع الاتحادي في دولة الإمارات العربية المتحدة أنواع البيانات الشخصية في المادة (1) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، إلى نوعين من البيانات، وهما:

أولاً: البيانات الشخصية الحساسية:

البيانات الشخصية الحساسة تمثل فئة خاصة من البيانات الشخصية التي تشمل المعلومات الدقيقة والحميمية المتعلقة بالأفراد، والتي يمكن أن تكون لها تأثيرات جوهرية على حياتهم وخصوصيتهم إذا تم التعامل معها بشكل غير لائق. تشمل هذه الفئة من البيانات المعلومات المتعلقة بالصحة البدنية أو العقلية، التوجه الجنسي، الانتماءات الدينية أو العرقية، الآراء السياسية، والسجلات الجنائية. تتطلب هذه البيانات مستوى عالٍ من الحماية نظرًا لحساسيتها والعواقب الخطيرة التي يمكن أن تنجم عن إساءة استخدامها أو تسريبها[16].

في التشريع الإماراتي، يتم التعامل مع البيانات الشخصية الحساسة بمنتهى الجدية، ويتم فرض قيود صارمة على جمعها ومعالجتها ونقلها. يُطلب من الجهات التي تتعامل مع هذه البيانات أن تتخذ تدابير أمان مشددة لضمان حمايتها من التهديدات والخروقات، وأن تضمن أن يتم التعامل معها بشكل قانوني وأخلاقي. كما يُمنح الأفراد حقوق واسعة فيما يتعلق ببياناتهم الشخصية الحساسة، بما في ذلك الحق في الوصول إلى هذه البيانات، وطلب تصحيحها أو حذفها، والحق في الاعتراض على معالجتها في بعض الحالات[17].

يُظهر التشريع الإماراتي بذلك التزامًا قويًا بحماية خصوصية الأفراد وسلامة معلوماتهم الشخصية، خاصة عندما يتعلق الأمر بالبيانات الشخصية الحساسة. يتطلب ذلك وعيًا قانونيًا وتقنيًا عاليًا من الجهات المعنية، واستعدادًا لتحمل المسؤولية في حماية هذه البيانات وضمان معالجتها بطريقة آمنة ومحترمة للخصوصية[18].

تم تعريف البيانات الشخصية الحساسة في المادة (1) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة بأنها: "أي بيانات تكشف بشكلٍ 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 له التي تكشف عن وضعه الصحي"[19].

المادة المشار إليها تقدم تعريفاً دقيقاً ومفصلاً للبيانات الشخصية الحساسة ضمن إطار التشريع الإماراتي لحماية البيانات الشخصية. تهدف هذه المادة إلى تحديد الفئات الخاصة من البيانات التي

تتطلب حماية مُشددة بسبب طبيعتها الحساسة والتي قد تؤثر بشكل كبير على الخصوصية الشخصية[20].

في البداية، تُشير المادة إلى أن البيانات الشخصية الحساسة يمكن أن تكشف عن معلومات خاصة جداً تتعلق بالشخص الطبيعي، بما في ذلك عائلته، أصله العرقي، آرائه السياسية والفلسفية، ومعتقداته الدينية. هذه المعلومات يمكن أن تكون خاصة جداً وحساسة، ولذلك يُعتبر الكشف عنها بدون موافقة الشخص المعني انتهاكاً خطيراً للخصوصية[21].

المادة تتناول أيضاً البيانات المتعلقة بسجل السوابق الجنائية للشخص، وبيانات القياسات الحيوية البيومترية. هذه الأنواع من البيانات يمكن أن تستخدم لتحديد هوية الشخص بدقة عالية، وبالتالي فإن حمايتها ضرورية لمنع التلاعب أو الاستخدام غير اللائق[22].

بالإضافة إلى ذلك، تشير المادة إلى البيانات المتعلقة بالصحة الشخصية، بما في ذلك الحالة الجسدية والنفسية والذهنية والعقلية والبدنية والجينية والجنسية. هذه البيانات شديدة الحساسية ويمكن أن تؤثر بشكل كبير على حياة الشخص ورفاهيته. كما يتم التطرق إلى المعلومات المتعلقة بتوفير خدمات الرعاية الصحية، مما يُشدد على الحاجة إلى حماية المعلومات التي يمكن أن تكشف عن الوضع الصحي للشخص[23].

وترى الباحثة، أن المادة سالفة البيان تُعتبر جزءاً أساسياً من التشريع الإماراتي لحماية البيانات الشخصية، حيث تُوفر تعريفاً واضحاً ومُفصلاً للبيانات الشخصية الحساسة، وتُشدد على الحاجة إلى اتخاذ تدابير حماية مُشددة لضمان عدم الكشف عن هذه البيانات بشكل غير لائق ولحماية خصوصية الأفراد.

ثانياً: البيانات الحيوية البيومترية:

البيانات الحيوية البيومترية تُعد فئة خاصة من البيانات الشخصية، وهي تشير إلى المعلومات المتعلقة بالخصائص الفيزيائية أو السلوكية الفريدة للفرد التي يمكن استخدامها لتعريفه والتحقق من هويته. تشمل هذه الخصائص بصمات الأصابع، البصمة القزحية، التعرف على الوجه، وبصمة الصوت. تُستخدم البيانات البيومترية على نطاق واسع في مجموعة متنوعة من التطبيقات، بما في ذلك الأمان الإلكتروني، التحكم في الوصول، والتعرف على الهوية[24].

في التشريع الإماراتي، يُولى اهتمام كبير لحماية البيانات البيومترية نظرًا لحساسيتها الشديدة والعواقب الخطيرة التي يمكن أن تنجم عن إساءة استخدامها. يتطلب القانون توفير ضمانات قوية لحماية هذه البيانات، بما في ذلك تدابير الأمان التقنية والإدارية الصارمة لمنع الوصول غير المصرح به وضمان سلامة البيانات. كما يُشدد على ضرورة الحصول على موافقة صريحة وواضحة من الأفراد قبل جمع بياناتهم البيومترية، ويُمنح الأفراد حقوق واسعة فيما يتعلق ببياناتهم البيومترية، بما في ذلك الحق في الوصول إليها، تصحيحها، وحذفها[25].

يعكس التشريع الإماراتي بذلك إدراكًا عميقًا للأهمية الخاصة والحساسية البالغة للبيانات البيومترية، ويسعى إلى توفير حماية قانونية قوية لضمان استخدامها بطريقة آمنة ومحترمة لخصوصية الأفراد. يتطلب ذلك التزامًا قويًا من جميع الأطراف المعنية وتطبيقًا دقيقًا للقوانين

والتدابير الوقائية لضمان حماية البيانات البيومترية ومعالجتها بطريقة تحافظ على حقوق وخصوصية الأفراد[26].

تم تعريف البيانات الحيوية البيومترية في المادة (1) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة بأنها: "البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات، والتي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات، مثل صورة الوجه أو بيانات البصمة"[27].

المادة المشار إليها تقدم تعريفًا شاملاً للبيانات الحيوية البيومترية ضمن نطاق حماية البيانات الشخصية في دولة الإمارات العربية المتحدة. هذه الفقرة تهدف إلى توضيح مفهوم البيانات الحيوية البيومترية وتسليط الضوء على أهميتها في عملية التحقق من هوية الأفراد[28].

البيانات الحيوية البيومترية، كما هو موضح في التعريف، هي نوع من البيانات الشخصية الذي يتم إنتاجه من خلال معالجة معينة باستخدام تقنية خاصة. هذه البيانات تتعلق بالخصائص الجسدية، الفسيولوجية أو السلوكية للشخص الذي تخصه البيانات. الغرض الرئيسي من جمع ومعالجة هذه البيانات هو تحديد هوية الشخص بطريقة فريدة ودقيقة[29].

من الأمثلة الشائعة على البيانات الحيوية البيومترية صورة الوجه وبيانات البصمة. هذه الأنواع من البيانات يمكن استخدامها للتحقق من هوية الشخص بسرعة ودقة، وهو ما يجعلها أداة قوية في مجال الأمان الإلكتروني وحماية البيانات[30].

من الجدير بالذكر أن البيانات الحيوية البيومترية تعتبر من البيانات الشخصية الحساسة بسبب طبيعتها الخاصة والتي تتطلب مستوى عالٍ من الحماية. الكشف غير المصرح به أو سوء استخدام هذه البيانات يمكن أن يؤدي إلى انتهاك خصوصية الفرد ويشكل تهديدًا كبيرًا لأمانه الشخصي[31].

وترى الباحثة، أن توضيح وتحديد مفهوم البيانات الحيوية البيومترية في التشريع الإماراتي يُعتبر خطوة مهمة نحو ضمان فهم واضح لطبيعة هذه البيانات وأهمية حمايتها. يساهم هذا التعريف في وضع الأساس لإنشاء إطار قانوني فعال يهدف إلى حماية البيانات الشخصية وتعزيز الثقة في استخدام التكنولوجيا والخدمات الرقمية.

المطلب الثالث

التطور التاريخي لحماية البيانات الشخصية

شهد التطور التاريخي لحماية البيانات الشخصية في الإمارات تغييرات جذرية وتقدمًا ملحوظًا على مدار السنوات، حيث تطور الوعي بأهمية حماية البيانات الشخصية والخصوصية بالتوازي مع التقدم التكنولوجي والرقمنة المتزايدة. في المراحل الأولى، كانت الإمارات تعتمد بشكل أساسي على

القوانين العامة والمبادئ القانونية التقليدية لحماية الخصوصية. ومع ذلك، مع زيادة استخدام الإنترنت والتقنيات الرقمية، أصبح من الواضح أن هناك حاجة ماسة لتحديث التشريعات وإدخال قوانين محددة تتعامل مع حماية البيانات الشخصية[32].

استجابةً لهذه الحاجة، بدأت الإمارات في اتخاذ خطوات جادة نحو تعزيز حماية البيانات الشخصية، وذلك من خلال إصدار قوانين وتشريعات متخصصة تستهدف حماية البيانات الشخصية وضمان التعامل معها بشكل آمن ومحترم للخصوصية. تم تبني مبادئ مثل الشفافية، النزاهة، والموافقة، ووُضعت ضوابط وإجراءات لضمان التزام الجهات العاملة بمعايير الحماية[33].

كما عُززت الحقوق الخاصة بالأفراد فيما يتعلق ببياناتهم الشخصية، مانحةً إياهم المزيد من السيطرة على كيفية جمع واستخدام ومشاركة معلوماتهم الشخصية. وأنشئت هيئات رقابية متخصصة لمراقبة التزام الجهات بالقوانين ولتوفير الدعم والإرشاد بشأن أفضل الممارسات في مجال حماية البيانات[34].

وترى الباحثة، أن التطور التاريخي لحماية البيانات الشخصية في الإمارات يعكس إدراكًا متزايدًا لأهمية هذه القضية والتزامًا قويًا بضمان حماية الخصوصية في عالم متزايد الرقمنة. يتجلى ذلك في الجهود المستمرة لتحديث القوانين وتعزيز الإطار التشريعي، مما يضمن توفير أعلى مستويات الحماية للبيانات الشخصية في الإمارات.

الفصل الأول

صور الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً

تمهيد وتقسيم:

تتميز الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في التشريع الإماراتي بتعدد صورها وشموليتها، حيث تسعى إلى توفير حماية قوية ضد الأنشطة الضارة والاستغلال غير القانوني للبيانات الشخصية. يتضمن التشريع تحديدًا واضحًا للجرائم الإلكترونية المتعلقة بانتهاك الخصوصية وسرقة البيانات، بما في ذلك الوصول غير المصرح به إلى البيانات الشخصية، الاستيلاء على البيانات، وتوزيع البيانات الشخصية بدون موافقة. يتم فرض عقوبات صارمة على هذه الجرائم، بما في ذلك الغرامات المالية الكبيرة والعقوبات السجنية، بغية ردع المخالفين وحماية الأفراد من الانتهاكات[35].

يُشدد التشريع أيضًا على أهمية تطبيق تدابير الأمان التقنية والإدارية لحماية البيانات الشخصية، ويُلزم الجهات المعالجة للبيانات بتبني هذه التدابير لضمان سلامة البيانات وحمايتها من التهديدات الإلكترونية. يتضمن ذلك استخدام التشفير، إجراءات التحقق من الهوية، وغيرها من تقنيات الأمان لحماية البيانات[36].

كما يتم التأكيد على الدور الحيوي للتوعية والتثقيف في مجال الأمان السيبراني، حيث يُشجع التشريع على نشر الوعي بأفضل الممارسات والتدابير الوقائية لحماية البيانات الشخصية. يُعتبر هذا

جزءًا لا يتجزأ من استراتيجية شاملة لحماية البيانات الشخصية وتعزيز الأمان الإلكتروني في المجتمع[37]. بهذه الطريقة، يُقدم التشريع الإماراتي نموذجًا قويًا للحماية الجنائية للبيانات الشخصية، من خلال مزيج من التدابير القانونية الصارمة، التوجيهات الواضحة للجهات المعالجة للبيانات، والتأكيد على أهمية الوعي والتثقيف في مجال الأمان السيبراني.

وللتعرف على صور الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً، سيتم تقسيم هذا الفصل إلى ثلاثة مباحث، وذلك على النحو التالي:

المبحث الأول: ضوابط معالجة البيانات الشخصية.

المبحث الثاني: تجريم الاعتداء على البيانات الشخصية في قانون الجرائم والعقوبات.

المبحث الثالث: تجريم الاعتداء على البيانات الشخصية في القوانين الخاصة.

المبحث الأول

ضوابط معالجة البيانات الشخصية

تمهيد وتقسيم:

تعتبر ضوابط معالجة البيانات الشخصية حجر الزاوية في ضمان الاستخدام الآمن والمسؤول للمعلومات الشخصية، وفي سياق التشريع الإماراتي، يتم التأكيد بشكل كبير على ضرورة وضع إجراءات صارمة ومحددة لحماية البيانات. يجب أن تكون عملية جمع البيانات الشخصية مشروعة وعادلة، وأن تتم بشفافية تامة، بحيث يكون الأشخاص على علم بالغرض من جمع بياناتهم وكيفية استخدامها. كما يجب تحديد نطاق البيانات المجمعة بدقة، بحيث لا يتم جمع سوى البيانات الضرورية لتحقيق الأغراض المحددة. ويتوجب على الجهات المعالجة للبيانات تطبيق تدابير أمان قوية لحماية البيانات من الفقد أو التلف أو الوصول غير المصرح به. يجب أيضًا أن يكون لدى الأشخاص الحق في الوصول إلى بياناتهم الشخصية، وتصحيحها إذا كانت غير دقيقة، وحتى حذفها في بعض الحالات. وتلتزم الجهات المعالجة بضمان المساءلة وتوفير قنوات للشكاوى والتظلمات، لضمان التزامها بأعلى معايير حماية البيانات ومعالجتها بشكل آمن ومسؤول[38].

تم النص على "ضوابط معالجة البيانات الشخصية" في نص المادة (5) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، بقولها: يتم معالجة البيانات الشخصية وفقاً للضوابط الآتية: 1- أن تكون المعالجة بطريقة عادلة وشفافة ومشروعة. 2- أن تكون البيانات الشخصية قد جمعت لغرض محدد وواضح، وألا يتم معالجتها في أي وقت لاحق على نحو يتنافى مع ذلك الغرض، ومع ذلك يجوز معالجتها في حال كان الغرض منها مشابه أو متقارب من الغرض الذي جمعت هذه البيانات من أجله. 3- أن تكون البيانات الشخصية كافية ومقتصرة على ما هو ضروري وفقاً للغرض الذي تمت المعالجة من أجله. 4- أن تكون البيانات الشخصية دقيقة وصحيحة، وأن تخضع للتحديث متى اقتضى الأمر ذلك. 5- أن تتوافر تدابير

وإجراءات لضمان محو أو تصحيح البيانات الشخصية غير الصحيحة. 6- أن تكون البيانات الشخصية محفوظة بشكلٍ آمن بما فيها حمايتها من أي انتهاك أو اختراق أو معالجة غير مشروعة أو غير مصرح بها من خلال وضع واستخدام تدابير وإجراءات تقنية وتنظيمية ملائمة وفق القوانين والتشريعات السارية في هذا الشأن. 7- عدم الاحتفاظ بالبيانات الشخصية بعد استنفاد الغرض من معالجتها، ويجوز الإبقاء عليها في حال تم إخفاء هوية صاحب البيانات باستخدام خاصية "آلية إخفاء الهوية". 8- أية ضوابط أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون"[39].

وللتعرف على ضوابط معالجة البيانات الشخصية، سيتم تقسيم هذا المبحث إلى ثلاثة مطالب، وذلك على النحو التالي:

المطلب الأول: حظر جمع البيانات أو معالجتها أو إفشائها إلا بموافقة الشخص المعني.

المطلب الثاني: تقرير بعض الحقوق للشخص المعني بالبيانات على بياناته.

المطلب الثالث: فرض بعض القيود والالتزامات على عمليات جمع البيانات وتحليلها أو معالجتها والاحتفاظ بها.

المطلب الأول

حظر جمع البيانات أو معالجتها أو إفشائها إلا بموافقة الشخص المعني

يُعد مبدأ حظر جمع البيانات الشخصية أو معالجتها أو إفشائها دون الحصول على موافقة صريحة وواعية من الشخص المعني أحد الركائز الأساسية في إطار حماية البيانات. يسعى هذا المبدأ إلى تعزيز السيطرة الشخصية على المعلومات الحساسة والخاصة، ويضمن أن يكون الأفراد على علم تام بكيفية وأسباب معالجة بياناتهم الشخصية. وفي سياق التشريع الإماراتي، يُعتبر الحصول على الموافقة الواضحة والمستنيرة من الشخص المعني شرطًا أساسيًا قبل الشروع في أي نشاط لمعالجة البيانات[40]، وذلك لضمان أن يكون لدى الأفراد القدرة على التحكم في معلوماتهم الشخصية وحماية خصوصيتهم. يجب أن تكون الموافقة محددة ومستندة إلى معلومات كافية، ويجب أن يكون لدى الأفراد القدرة على سحب موافقتهم في أي وقت، مما يعزز من مبدأ الشفافية والاحترام المتبادل بين الجهات المعالجة للبيانات والأفراد. هذا النهج يسهم في بناء ثقة قوية بين الطرفين ويضمن استخدامًا آمنًا ومسؤولًا للبيانات الشخصية[41].

تم النص على "حظر جمع البيانات أو معالجتها أو إفشائها إلا بموافقة الشخص المعني" في نص المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة

الإمارات العربية المتحدة، بقولها: "يُحظر معالجة البيانات الشخصية دون موافقة صاحبها، وتُستثنى أي من الحالات التالية من هذا الحظر، وتعتبر المعالجة حينها مشروعة: 1- أن تكون المعالجة ضرورة لحماية المصلحة العامة. 2- أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات. 3- أن تكون المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية أو الأمنية. 4- أن تكون المعالجة ضرورية لأغراض الطب المهني أو الوقائي من أجل تقييم قدرة الموظفين على العمل، أو التشخيص الطبي أو تقديم الرعاية الصحية أو الاجتماعية أو العلاج أو خدمات التأمين الصحي أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية وفقاً للتشريعات السارية في الدولة. 5- أن تكون المعالجة ضرورية لحماية الصحة العامة، وتشمل الحماية من الأمراض السارية والأوبئة أو لأغراض ضمان سلامة وجودة الرعاية الصحية والأدوية والعقاقير والأجهزة الطبية، وفقاً للتشريعات السارية في الدولة. 6- أن تكون المعالجة ضرورية لأغراض أرشيفية أو دراسات علمية وتاريخية وإحصائية وفقاً للتشريعات السارية في الدولة. 7- أن تكون المعالجة ضرورية لحماية صاحب البيانات. 8- أن تكون المعالجة ضرورية لأغراض قيام المتحكم أو صاحب البيانات بالتزاماته ومباشرة حقوقه المقررة قانوناً في مجال التوظيف أو الضمان الاجتماعي أو القوانين المعنية بالحماية الاجتماعية وذلك بالقدر الذي يسمح به في تلك القوانين. 9- أن تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه أو لاتخاذ إجراءات بناءً على طلب صاحب البيانات بهدف إبرام عقد أو تعديله أو إنهائه. 10- أن تكون المعالجة ضرورية لتنفيذ التزامات محددة في قوانين أخرى في الدولة على المتحكم. 11- أية حالات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون"[42].

المادة سالفة البيان هي نص محوري ضمن المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة، وتعالج قضية حساسة ومهمة تتعلق بحماية خصوصية الأفراد[43]. تبدأ المادة بتأسيس قاعدة عامة تقوم على ضرورة الحصول على موافقة الشخص المعني قبل معالجة بياناته الشخصية. هذه القاعدة تعكس التزامًا صارمًا بحماية الخصوصية وتؤكد على ضرورة أن يكون للأفراد سيطرة على بياناتهم الشخصية.

ومع ذلك، تدرك المادة أن هناك حالات قد يكون فيها جمع ومعالجة البيانات الشخصية ضروريًا دون الحاجة إلى موافقة صاحب البيانات، ولذلك تقدم المادة قائمة بالاستثناءات التي تعتبر المعالجة فيها مشروعة حتى بدون موافقة صاحب البيانات[44].

تتنوع هذه الاستثناءات لتشمل حالات تتعلق بحماية المصلحة العامة، البيانات الشخصية التي أصبحت معروفة للعامة بفعل من صاحب البيانات، ضرورات قانونية وقضائية، الحاجة للرعاية الطبية والصحية، حماية الصحة العامة، الأرشفة والدراسات العلمية والتاريخية، حماية صاحب البيانات نفسه، والالتزامات القانونية والتعاقدية[45].

هذه الاستثناءات تعكس توازنًا دقيقًا يسعى المشرع لتحقيقه بين حماية خصوصية الأفراد وضرورات الحياة العملية والمصالح العامة. يتطلب تحقيق هذا التوازن فهمًا عميقًا للسياق الذي يتم فيه معالجة البيانات وتقديرًا دقيقًا للمصالح المتعارضة[46].

كما يظهر من النص، فإن المشرع يترك المجال مفتوحًا لإضافة استثناءات أخرى من خلال اللائحة التنفيذية للمرسوم بقانون، مما يوفر مرونة لتحديث وتعديل القواعد القانونية بما يتناسب مع التطورات المستقبلية والحاجات المتغيرة[47].

وترى الباحثة، أن المادة سالفة البيان تشكل حجر الزاوية في نظام حماية البيانات الشخصية في دولة الإمارات العربية المتحدة، وتعبر عن التزام الدولة بحماية خصوصية مواطنيها والمقيمين على أراضيها، مع الأخذ في الاعتبار الحاجة إلى مرونة لضمان استمرارية الأعمال وحماية المصالح العامة.

المطلب الثاني

تقرير بعض الحقوق للشخص المعني بالبيانات على بياناته

يتمتع الشخص المعني بالبيانات بمجموعة من الحقوق الأساسية التي تهدف إلى تعزيز الشفافية وتوفير سيطرة أكبر على بياناته الشخصية، وهذا يشكل جزءاً لا يتجزأ من مفهوم حماية البيانات. من بين هذه الحقوق حق الوصول، حيث يمكن للشخص المعني طلب نسخة من البيانات الشخصية المحفوظة عنه، والتحقق من صحتها والأغراض التي يتم معالجتها من أجلها. يتمتع الفرد أيضًا بحق التصحيح، بحيث يمكنه طلب تصحيح أي بيانات غير دقيقة تتعلق به. وهناك حق الحذف، الذي يُعرف أيضًا بـ "حق النسيان"، حيث يمكن للشخص المعني طلب حذف بياناته الشخصية في ظروف معينة. بالإضافة إلى ذلك، يشمل حق الاعتراض، حيث يمكن للفرد الاعتراض على معالجة بياناته الشخصية لأسباب تتعلق بوضعه الخاص. وأخيرًا، يتمتع الشخص بحق في تقييد المعالجة، بموجبه يمكنه طلب تقييد استخدام بياناته الشخصية في بعض السيناريوهات. هذه الحقوق تُعزز من قدرة الأفراد على السيطرة على بياناتهم وتحقيق مستوى أعلى من الحماية لخصوصيتهم[48].

تم "تقرير بعض الحقوق للشخص المعني بالبيانات على بياناته" في نص المادة (13) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، بقولها: "1- يحق لصاحب البيانات وبناءً على طلب يقدمه إلى المتحكم ومن دون أي مقابل الحصول على المعلومات الآتية: أ- أنواع البيانات الشخصية التابعة له التي يتم معالجتها. ب- أغراض

المعالجة. ج- القرارات المتخذة بناءً على المعالجة المؤتمتة بما فيها التنميط. د- القطاعات أو المنشآت المستهدفة التي سيتم مشاركة بياناته الشخصية معهم من داخل وخارج الدولة. ه- ضوابط ومعايير مدد تخزين وحفظ بياناته الشخصية. و- إجراءات تصحيح أو محو أو تقييد المعالجة والاعتراض على بياناته الشخصية. ز- تدابير الحماية الخاصة بالمعالجة عبر الحدود التي تتم وفقاً للمادتين (22) و(23) من هذا المرسوم بقانون. ح- الإجراءات التي ستتخذ في حال اختراق أو انتهاك بياناته الشخصية، خاصةً إن كان الاختراق أو الانتهاك له خطر مباشر وجسيم على خصوصية وسرية بياناته الشخصية. ط- كيفية تقديم الشكاوى للمكتب. 2- في جميع الأحوال، يجب على المتحكم، وقبل البدء في المعالجة، تزويد صاحب البيانات بالمعلومات المنصوص عليها في الفقرات (ب) و(د) و(ز) من البند (1) من هذه المادة. 3- يجوز للمتحكم رفض طلب صاحب البيانات في الحصول على المعلومات الواردة في البند (1) من هذه المادة، في حال تبين له ما يأتي: أ- أن الطلب لا يتعلق بالمعلومات المُشار إليها في البند (1) من هذه المادة أو كان متكرراً بشكلٍ مبالغ به. ب- أن الطلب يتعارض مع الإجراءات القضائية أو التحقيقات التي تجريها الجهات المختصة. ج- أن الطلب قد يؤثر سلباً على جهود المتحكم في حماية أمن المعلومات. د- أن الطلب يمس بخصوصية وسرية البيانات الشخصية للغير"[49].

تقرير المادة (13) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 في الإمارات العربية المتحدة يأتي ليؤكد على حقوق الأفراد فيما يتعلق بالبيانات الشخصية التي تُجمع وتُعالج إلكترونياً. هذا التشريع يُعد خطوة هامة في تعزيز حماية البيانات والخصوصية في عالم يزداد فيه الاعتماد على التكنولوجيا والبيانات الرقمية[50].

الفقرة الأولى من المادة تقرر أن لصاحب البيانات الحق في الحصول على معلومات مفصلة عن بياناته الشخصية التي يتم معالجتها من قِبل المتحكم بالبيانات، وذلك دون أي مقابل مادي. هذه المعلومات تشمل نوع البيانات الشخصية، الأغراض التي تُعالج من أجلها، القرارات المتخذة بناءً على المعالجة الآلية وغيرها. كما يُمكن لصاحب البيانات معرفة الجهات التي قد تتم مشاركة بياناته معها وضوابط تخزين هذه البيانات[51].

الفقرة الثانية تُلزم المتحكم بالبيانات بإعلام صاحب البيانات بالمعلومات الرئيسية قبل البدء في معالجة بياناته. هذا يضمن أن يكون صاحب البيانات على علم تام بكيفية استخدام بياناته ولأي أغراض[52].

الفقرة الثالثة تتيح للمتحكم بالبيانات الحق في رفض طلب صاحب البيانات في الحصول على المعلومات في حالات معينة. هذه الحالات تشمل الطلبات التي لا تتعلق بالمعلومات المحددة في الفقرة الأولى، أو الطلبات المتكررة بشكل مفرط، أو الطلبات التي قد تتعارض مع الإجراءات القضائية أو التحقيقات الجارية[53].

وترى الباحثة، أن المادة سالفة البيان تُعتبر خطوة مهمة نحو تعزيز حقوق الأفراد وحماية خصوصيتهم في العالم الرقمي. تُوضح المادة الحقوق التي يمتلكها صاحب البيانات وتُحدد الإلتزامات التي يجب على المتحكم بالبيانات الالتزام بها، مما يُساهم في خلق بيئة أكثر أمانًا وشفافية لمعالجة البيانات الشخصية.

المطلب الثالث

فرض بعض القيود والالتزامات على عمليات جمع البيانات وتحليلها أو معالجتها والاحتفاظ بها

إن فرض قيود والتزامات على عمليات جمع البيانات وتحليلها أو معالجتها والاحتفاظ بها يشكل ركيزة أساسية في نظام حماية البيانات، حيث يهدف إلى ضمان معالجة البيانات بطريقة تحترم خصوصية الأفراد وتحمي حقوقهم. يتطلب هذا من الجهات المعنية تطبيق مبادئ البيانات بالحد الأدنى والشفافية، بحيث يتم جمع البيانات لأغراض محددة ومشروعة ولا يتم معالجتها بطريقة تتعارض مع هذه الأغراض[54]. يجب أن يتم الاحتفاظ بالبيانات للمدة الزمنية الضرورية فقط وأن يتم حمايتها من الوصول غير المصرح به أو التلف. الجهات المعالجة للبيانات ملزمة بتنفيذ تدابير أمان قوية وإجراء تقييمات دورية للمخاطر للتأكد من فعالية هذه التدابير. بالإضافة إلى ذلك، يجب أن يكون لدى الأفراد الحق في الوصول إلى بياناتهم الشخصية وتصحيحها أو حذفها في ظروف معينة، ولديهم الحق في المطالبة بتقييد معالجة بياناتهم والاعتراض عليها. هذه القيود والالتزامات تسهم في بناء نظام قوي لحماية البيانات يعزز الثقة ويضمن معالجة المعلومات الشخصية بطريقة مسؤولة وآمنة[55].

تم النص على "حق تقييد معالجة البيانات" في نص المادة (16) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، بقولها: "1- يحق لصاحب البيانات إلزام المتحكم بتقييد وإيقاف المعالجة في أي من الحالات الآتية: أ- اعتراض صاحب البيانات على دقة بياناته الشخصية، وفي هذه الحالة يتم تقييد المعالجة لفترة محددة تسمح للمتحكم التحقق من دقتها. ب- اعتراض صاحب البيانات على معالجة بياناته الشخصية بالمخالفة للأغراض المتفق عليها. ج- أن تكون المعالجة قد تمت بالمخالفة لأحكام هذا المرسوم بقانون والتشريعات السارية. 2- يحق لصاحب البيانات الطلب من المتحكم الاستمرار بالاحتفاظ ببياناته الشخصية لما بعد انتهاء أغراض المعالجة، كون هذه البيانات ضرورية لاستكمال إجراءات متعلقة بالمطالبة بالحقوق والدعاوى القضائية أو الدفاع عنها. 3- على الرغم مما ورد في البند (1) من هذه المادة، للمتحكم المضي في معالجة البيانات الشخصية لصاحب البيانات دون موافقته في أي من الحالات الآتية: أ- إذا كانت المعالجة مقتصرة على تخزين البيانات الشخصية. ب- إذا كانت المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى االقانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية. ج- إذا كانت المعالجة ضرورية لحماية حقوق الغير وفقاً للتشريعات السارية. د- إذا كانت المعالجة ضرورية لحماية المصلحة العامة. 4- وفي جميع الأحوال، يجب على المتحكم في حال قام برفع التقييد المنصوص عليه في هذه المادة، أن يخطر صاحب البيانات بذلك"[56].

تطرح المادة (16) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 الذي يُعنى بحماية البيانات الشخصية في دولة الإمارات العربية المتحدة، موضوع "حق تقييد معالجة البيانات"، متيحة لصاحب البيانات سلطة مطالبة المتحكم بتقييد وإيقاف المعالجة في سيناريوهات معينة[57].

في البند الأول، يُمكن لصاحب البيانات طلب تقييد المعالجة في حالات مثل الشك في دقة البيانات الشخصية، حيث يُتاح للمتحكم فترة زمنية للتحقق من صحة البيانات. كما يُمكن طلب التقييد إذا اعتُرض صاحب البيانات على معالجة بياناته بشكل يتنافى مع الأغراض المتفق عليها أو إذا تمت المعالجة بطريقة تخالف القوانين السارية[58].

البند الثاني يعطي صاحب البيانات الحق في طلب الاحتفاظ ببياناته الشخصية حتى بعد انتهاء فترة المعالجة، إذا كانت هذه البيانات ضرورية لإجراءات قانونية مستقبلية مثل المطالبات القانونية أو الدفاع عن حقوقه[59].

في المقابل، يحدد البند الثالث الظروف التي يُمكن فيها للمتحكم مواصلة معالجة البيانات الشخصية بدون موافقة صاحب البيانات، مثل إذا كانت المعالجة مقتصرة على التخزين فقط أو إذا كانت ضرورية للحماية القانونية لحقوق الغير أو المصلحة العامة. أخيرًا، يُلزم البند الرابع المتحكم بإخطار صاحب البيانات في حال قرر رفع التقييد المفروض على المعالجة[60].

وترى الباحثة، أن هذه المادة تعكس الجهود المبذولة لتعزيز الشفافية والمساءلة في معالجة البيانات الشخصية، وتمنح الأفراد مزيدًا من السيطرة على بياناتهم الشخصية، ما يُسهم في بناء الثقة ويعزز حماية الخصوصية.

المبحث الثاني

تجريم الاعتداء على البيانات الشخصية في قانون الجرائم والعقوبات

تمهيد وتقسيم:

تجريم الاعتداء على البيانات الشخصية يعتبر خطوة حاسمة في تعزيز الحماية القانونية للمعلومات الشخصية، حيث يعتبر ذلك انتهاكًا لخصوصية الأفراد وأمانهم الرقمي. في إطار قانون الجرائم والعقوبات، يمكن أن يشمل تجريم الاعتداء على البيانات الشخصية عدة أفعال، مثل الوصول غير المصرح به إلى البيانات، وسرقة المعلومات الشخصية، وتعديل البيانات دون إذن، والكشف غير القانوني عن المعلومات الشخصية. يعمل تجريم هذه الأفعال على توفير حماية قانونية للبيانات ويعطي الأفراد الثقة في أن معلوماتهم الشخصية آمنة ومحمية. بالإضافة إلى ذلك، يُعد تجريم الاعتداء على البيانات الشخصية أداة رادعة قوية ضد المهاجمين والجناة المحتملين، حيث يمكن أن يؤدي الإدانة إلى فرض عقوبات جنائية، بما في ذلك الغرامات الكبيرة والسجن. يتطلب هذا من الدولة توفير الموارد اللازمة لتحقيق الجرائم ومحاكمة الجناة، وكذلك تحسين البنية التحتية التكنولوجية لحماية البيانات والكشف عن الاختراقات الأمنية. يساهم تجريم الاعتداء على البيانات الشخصية في خلق بيئة رقمية أكثر أمانًا ويعزز من ثقة الأفراد في التعاملات الرقمية واستخدام الخدمات الإلكترونية[61].

وللتعرف على تجريم الاعتداء على البيانات الشخصية في قانون الجرائم والعقوبات، سيتم تقسيم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: تجريم الاعتداء على حرمة الحياة الخاصة للأفراد.

المطلب الثاني: الحماية الجنائية للسر المهني وتجريم إفشائه.

المطلب الأول

تجريم الاعتداء على حرمة الحياة الخاصة للأفراد

تجريم الاعتداء على حرمة الحياة الخاصة للأفراد يُعد إجراءً جوهرياً لحماية الحقوق الأساسية والحفاظ على كرامة الإنسان. الحياة الخاصة تشمل مجالات عديدة من حياة الأفراد، بدءًا من المعلومات الشخصية، والاتصالات، وصولاً إلى الحياة الأسرية والعلاقات الشخصية. عند تجريم الاعتداء على هذه الجوانب، تقوم الدولة بإرسال رسالة واضحة مفادها أن خصوصية الأفراد وحرمتهم الشخصية تُعتبر قيمًا مقدسة وأن الدولة ملتزمة بحمايتها[62].

يشمل تجريم الاعتداء على حرمة الحياة الخاصة فرض عقوبات على أعمال مثل التنصت غير القانوني، والتصوير السري، وانتهاك السرية الشخصية، وسرقة البيانات الشخصية، وغيرها من الأفعال التي تُعتبر تدخلاً في الحياة الخاصة للأفراد. يتطلب ذلك توفير الحماية القانونية الكافية وضمان قيام الأجهزة الأمنية والقضائية بدورها في التحقيق وملاحقة الجناة[63].

بالإضافة إلى ذلك، يساهم تجريم الاعتداء على حرمة الحياة الخاصة في خلق بيئة آمنة تحترم الحريات الشخصية وتعزز من الشعور بالأمان لدى الأفراد، وهو ما يُعد عاملاً أساسيًا في تعزيز الاستقرار الاجتماعي وتحقيق التنمية المستدامة[64].

نصت المادة (431) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات لدولة الإمارات العربية المتحدة، على أنه: "يعاقب بالحبس والغرامة كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه: 1- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف أو أي جهاز آخر. 2- التقط أو نقل بجهاز أياً كان نوعه صورة شخص في مكان خاص. فإذا صدرت الأفعال المشار إليها في الحالتين السابقتين أثناء اجتماع على مسمع أو مرآى من الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضاً. كما يعاقب بذات العقوبة من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة. ويعاقب بالحبس مدة لا تزيد على (7) سبع سنوات وبالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها"[65].

تهتم المادة (431) من قانون الجرائم والعقوبات اتحادي رقم (31) لسنة 2021، في دولة الإمارات العربية المتحدة، بحماية الحرمة الشخصية والعائلية للأفراد، وتحديداً في سياق الاعتداء على خصوصية الاتصالات والمحادثات الشخصية والصور في الأماكن الخاصة، حيث تبدأ المادة بتحديد العقوبات المترتبة على ارتكاب الجرائم المتعلقة بالخصوصية، مشيرة إلى أن الحبس والغرامة هما العقوبتان الأساسيتان لمن يُدان بالاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد. يُشدد النص على أن هذه العقوبات تنطبق في حالات عدم الحصول على الإذن القانوني أو عدم وجود رضاء من الشخص المعتدى على خصوصيته[66].

تُقسم المادة الأفعال المُعاقب عليها إلى قسمين: الأول يتعلق بالاعتداء على خصوصية المحادثات عبر استراق السمع أو تسجيلها أو نقلها، والثاني يتعلق بالتقاط أو نقل صور الأشخاص في أماكن

خاصة دون إذنهم. يُعتبر الرضا مفترضًا في حال حدوث هذه الأفعال أثناء اجتماع يكون فيه الجميع حاضرين وعلى علم بما يحدث[67].

يُضاف إلى ذلك، تُعاقب المادة أيضًا أولئك الذين ينشرون أخبارًا أو صورًا أو تعليقات تتعلق بحياة الأفراد الخاصة أو العائلية، حتى لو كان المحتوى المنشور صحيحًا، مُشددةً على أن الحق في الخصوصية يجب أن يظل محميًا بغض النظر عن صحة المعلومات المُتداولة[68].

تُختتم المادة بالإشارة إلى أن الموظف العام الذي يستخدم سلطة وظيفته لارتكاب أي من الأفعال المذكورة يواجه عقوبة أشد، تصل إلى الحبس لمدة تصل إلى سبع سنوات وغرامة. كما يُلزم النص بمصادرة أي أجهزة أو معدات استُخدمت في ارتكاب الجريمة وإعدام أو محو التسجيلات المتحصلة منها، لضمان عدم استمرار انتهاك خصوصية الأفراد[69].

وترى الباحثة، أن هذه المادة تعكس التزام دولة الإمارات العربية المتحدة بحماية الحرمة الشخصية والخاصة لأفرادها، وتوضح العقوبات الشديدة المترتبة على انتهاك هذه الحقوق.

المطلب الثاني

الحماية الجنائية للسر المهني وتجريم إفشائه

الحماية الجنائية للسر المهني تعتبر جزءاً أساسياً من النظام القانوني لأي دولة، حيث يُعد الحفاظ على السرية المهنية التزاماً أخلاقياً وقانونياً يُلزم الأفراد العاملين في مجالات معينة بحماية المعلومات الحساسة والخاصة التي يتم الكشف عنها أثناء ممارسة مهنتهم. تتضمن الحماية الجنائية للسر المهني تجريم أي أفعال تتعلق بإفشاء المعلومات السرية بشكل غير قانوني، ويمكن أن تشمل هذه الأفعال الإفشاء العمدي للمعلومات السرية، أو الإهمال الذي يؤدي إلى تسرب المعلومات[70].

تُعد هذه الحماية ضرورية للحفاظ على الثقة بين العملاء والمحترفين، سواء كانوا أطباء، محامين، محاسبين، أو أي مهنيين آخرين. الثقة هي الركيزة الأساسية في هذه العلاقات، والحفاظ على سرية المعلومات يعتبر جزءاً لا يتجزأ من بناء والحفاظ على هذه الثقة[71].

تجريم إفشاء السر المهني يعكس إدراك المجتمع لأهمية حماية المعلومات الخاصة، ويساهم في خلق بيئة يشعر فيها الأفراد بالأمان عند مشاركة معلوماتهم الحساسة مع المحترفين. العقوبات المفروضة على إفشاء السر المهني يمكن أن تشمل الغرامات الكبيرة، وفي بعض الحالات، السجن. هذه العقوبات تعمل كرادع قوي ضد أي محاولات لخرق السرية المهنية، وتضمن أن يتحمل الجناة المسؤولية الكاملة عن أفعالهم[72].

نصت المادة (432) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات لدولة الإمارات العربية المتحدة، على أنه: "يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن (20,000) عشرين ألف درهم أو بإحدى هاتين العقوبتين من كان بحكم مهنته أو حرفته أو وضعه أو فنه مستودع سر فأفشاه في غير الأحوال المصرح بها قانوناً أو استعمله لمنفعته الخاصة أو لمنفعة شخص آخر، وذلك ما لم يأذن صاحب الشأن في السر بإفشائه أو استعماله . وتكون العقوبة السجن المؤقت مدة لا تزيد على (5) خمس سنوات إذا كان الجاني موظفاً عاماً أو مكلفاً بخدمة عامة واستودع السر أثناء أو بسبب أو بمناسبة تأدية وظيفته أو خدمته"[73].

تتناول المادة (432) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 في قانون الجرائم والعقوبات الإماراتي، جريمة الإفشاء غير المشروع للأسرار، وهي تعكس التزام الدولة بحماية البيانات والمعلومات الشخصية والسرية للأفراد، خاصةً تلك التي يتم الحصول عليها أو معالجتها في سياق مهني أو رسمي[74].

تنص المادة على أنه يُعاقب بالحبس لمدة لا تقل عن سنة وبغرامة لا تقل عن عشرين ألف درهم، أو بإحدى هاتين العقوبتين، كل من كان بحكم مهنته أو حرفته أو وضعه أو فنه مستودعًا لسر، وقام بإفشائه أو استخدمه لمنفعته الخاصة أو لمنفعة شخص آخر دون إذن صاحب الشأن، وذلك في غير الأحوال التي يصرح بها القانون[75].

تتطرق المادة إلى حالة خاصة تتعلق بالموظفين العامين أو الأشخاص المكلفين بخدمة عامة، حيث تُشدد العقوبة في حالة كان الجاني ينتمي إلى هذه الفئة، وقام بإفشاء السر أو استخدامه لمنفعته الخاصة أو لمنفعة شخص آخر، وذلك أثناء أو بسبب أو بمناسبة تأدية وظيفته أو خدمته. في هذه الحالة، تكون العقوبة السجن المؤقت لمدة تصل إلى خمس سنوات[76].

وترى الباحثة أن المادة سالفة البيان تُظهر اهتمام المشرع الإماراتي بحماية الأسرار والمعلومات الشخصية، وتؤكد على أهمية المحافظة على الثقة في العلاقات المهنية والوظيفية، كما تُعبر عن رفض المجتمع لأي سلوك يتضمن خيانة للأمانة وإفشاء للأسرار بشكل غير مشروع. وبهذا، تُسهم المادة في ترسيخ مبادئ النزاهة والشفافية في المجتمع وتعزيز الثقة بين الأفراد والمؤسسات.

المبحث الثالث

تجريم الاعتداء على البيانات الشخصية في القوانين الخاصة

تمهيد وتقسيم:

تجريم الاعتداء على البيانات الشخصية في القوانين الخاصة يُعتبر خطوة هامة نحو حماية الحق في الخصوصية وضمان أمان المعلومات الشخصية للأفراد. يتضمن ذلك وضع تشريعات وقوانين صارمة تُعنى بحماية البيانات الشخصية من أي نوع من الاعتداء، سواء كان ذلك من خلال السرقة، التعديل غير المشروع، الإفشاء أو الاستخدام الغير قانوني للبيانات الشخصية[77].

تهدف القوانين الخاصة إلى تحديد المسؤوليات والالتزامات الملقاة على عاتق الجهات التي تتعامل مع البيانات الشخصية، مما يضمن معالجة هذه البيانات بشكل آمن ومحمي. كما تُلزم هذه القوانين الجهات باتخاذ تدابير وقائية لحماية البيانات الشخصية من أي تهديدات محتملة، وتفرض عقوبات رادعة في حالة الإخلال بالتزامات حماية البيانات[78].

علاوة على ذلك، تُوفر القوانين الخاصة الحقوق للأشخاص المعنيين بالبيانات، مما يمنحهم القدرة على الوصول إلى بياناتهم الشخصية، وتصحيح أي معلومات غير دقيقة، وطلب حذف بياناتهم في

بعض الحالات. كما تُعزز هذه الحقوق من الشفافية وتُعطي الأفراد السيطرة على بياناتهم الشخصية[79].

بالإضافة إلى ذلك، يُعد تجريم الاعتداء على البيانات الشخصية في القوانين الخاصة عاملاً أساسياً في بناء ثقة المستهلكين والأفراد في الخدمات الرقمية والإلكترونية، وهو ما يُعد ضرورياً لتحقيق التقدم التكنولوجي والابتكار. يُسهم هذا في خلق بيئة رقمية آمنة وموثوقة تُعزز من النمو الاقتصادي وتحفز على الابتكار[80].

وللتعرف على تجريم الاعتداء على البيانات الشخصية في القوانين الخاصة، سيتم تقسيم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: حماية البيانات الشخصية في المرسوم بالقانون الاتحادي رقم (15) لسنة 2020 في شأن حماية المستهلك.

المطلب الثاني: حماية البيانات الشخصية في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

المطلب الأول

حماية البيانات الشخصية في المرسوم بالقانون الاتحادي رقم (15) لسنة 2020 في شأن حماية المستهلك

المرسوم بالقانون الاتحادي رقم (15) لسنة 2020 في دولة الإمارات العربية المتحدة، الذي يتعلق بحماية المستهلك، يعتبر خطوة مهمة نحو تعزيز حقوق المستهلكين وضمان حمايتهم في مختلف المعاملات التجارية. بالرغم من أن التركيز الرئيسي لهذا القانون يكمن في حماية حقوق المستهلك وضمان تلقيهم للسلع والخدمات بجودة عالية وبشكل عادل، إلا أنه يتضمن أيضاً بعض الأحكام التي تتعلق بحماية البيانات الشخصية[81].

يؤكد القانون على ضرورة الحفاظ على سرية المعلومات الشخصية للمستهلكين، ويُلزم الجهات التجارية باتخاذ التدابير اللازمة لحماية هذه البيانات من أي استخدام غير مشروع أو إفشاء. كما يُحظر على الجهات التجارية جمع أو استخدام البيانات الشخصية للمستهلكين دون الحصول على موافقتهم الصريحة[82].

يُعزز هذا القانون من الشفافية في التعامل مع البيانات الشخصية، حيث يُلزم الجهات التجارية بإبلاغ المستهلكين بشكل واضح وصريح عن كيفية جمع بياناتهم واستخدامها وحمايتها. كما يُمكن للمستهلكين طلب الوصول إلى بياناتهم الشخصية وتصحيحها في حالة عدم الدقة[83].

علاوة على ذلك، يُوفر القانون آليات للتقديم بالشكاوى في حالة انتهاك حقوق المستهلك، بما في ذلك انتهاك حقوقهم فيما يتعلق بالبيانات الشخصية. يُعتبر تطبيق هذا القانون خطوة مهمة نحو تعزيز ثقة المستهلكين وحماية خصوصيتهم في عصر الرقمنة المتزايد[84].

وترى الباحثة، أن المرسوم بالقانون الاتحادي رقم (15) لسنة 2020 يُسهم في تعزيز الحماية القانونية للبيانات الشخصية للمستهلكين في الإمارات العربية المتحدة، مما يُعزز من حماية خصوصيتهم ويُساهم في بناء بيئة رقمية آمنة وموثوقة.

نص البند (5) من المادة (4) من المرسوم بقانون اتحادي رقم (15) لسنة 2020 بشأن حماية المستهلك في دولة الإمارات العربية المتحدة، على أنه: "تعتبر كافة الالتزامات المقررة بموجب هذا القانون حقوقاً للمستهلك، وبما يشمل: ... 5- حماية خصوصية وأمن بياناته وعدم استخدامها في أغراض الترويج والتسويق"[85].

المادة المذكورة أعلاه تحمل في طياتها الكثير من الدلالات والمعاني التي تهدف إلى تعزيز حماية المستهلك في البيئة الإلكترونية وضمان الحفاظ على خصوصيته وأمان بياناته الشخصية. فيما يلي تحليل معمق للبند (5) من المادة (4) من المرسوم بقانون اتحادي رقم (15) لسنة 2020: المادة تُشدد على مبدأ أساسي وهو أن الحماية القانونية لبيانات المستهلك لا تُعد مجرد التزام يُلقى على عاتق المتعاملين والشركات، بل هي في الواقع حق أصيل للمستهلك يجب احترامه وحمايته. هذا يعني أن المستهلك لديه الحق في أن يتوقع أن يتم التعامل مع بياناته الشخصية بشكل يحفظ خصوصيته ويضمن أمانها[86].

"حماية خصوصية وأمن بياناته" - هذا الجزء من النص يُؤكد على أهمية حماية خصوصية المستهلك وضمان أمان بياناته الشخصية. يعتبر هذا أمراً حاسماً في عصر الرقمنة حيث يتم جمع ومعالجة كميات هائلة من البيانات الشخصية يومياً. يُفترض بالشركات والمتعاملين توفير آليات وتدابير أمان فعّالة لحماية هذه البيانات من السرقة، الاختراق، أو الاستخدام غير المصرح به[87].

"وعدم استخدامها في أغراض الترويج والتسويق" - يُشدد هذا الجزء على أن بيانات المستهلك لا يجب أن تُستخدم في أغراض الترويج والتسويق دون موافقته الصريحة. هذا يعني أن المستهلك لديه الحق في أن يقرر ما إذا كان يرغب في تلقي الإعلانات والعروض الترويجية أم لا، وأنه يجب احترام خياراته في هذا الشأن[88].

وترى الباحثة أن النص القانوني هنا يُعبر عن التزام الدولة بحماية حقوق المستهلكين وضمان أن يتم التعامل مع بياناتهم الشخصية بما يتوافق مع معايير الخصوصية والأمان. يُعتبر هذا جزءًا لا يتجزأ من جهود تعزيز الثقة في البيئة الرقمية وضمان أن يتمكن المستهلكون من الاستفادة من الفوائد التي تقدمها التكنولوجيا دون أن يضطروا للتضحية بخصوصيتهم وأمان بياناتهم الشخصية.

المطلب الثاني

حماية البيانات الشخصية في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية

المرسوم بقانون اتحادي رقم (34) لسنة 2021 في دولة الإمارات العربية المتحدة يمثل إطارًا قانونيًا هامًا في مجال مكافحة الجرائم الإلكترونية والتصدي للشائعات التي يمكن أن تضر بالأمن الوطني والاستقرار الاجتماعي. فيما يتعلق بحماية البيانات الشخصية، يُسهم هذا القانون في توفير حماية قانونية للمعلومات الشخصية والخصوصية الرقمية للأفراد[89].

القانون يُجرم العديد من الأفعال التي تُشكل اعتداءً على البيانات الشخصية، بما في ذلك الوصول غير المشروع إلى النظم الإلكترونية والبيانات، وانتهاك خصوصية الأفراد عبر الشبكة الإلكترونية. يُعاقب القانون أيضًا على الإفشاء غير المشروع للبيانات الشخصية والمعلومات السرية، مما يُسهم في حماية خصوصية الأفراد وسرية بياناتهم[90].

كما يحث القانون الجهات والأفراد على اتخاذ التدابير الأمنية اللازمة لحماية البيانات الشخصية من الاختراق والتلاعب. يُعزز ذلك من الثقة في المعاملات الإلكترونية ويُساهم في خلق بيئة رقمية آمنة[91].

المرسوم بقانون يُشدد على ضرورة تحقيق التوازن بين حرية التعبير وحماية البيانات الشخصية، حيث يُجرم نشر المعلومات الكاذبة والشائعات التي يمكن أن تضر بسمعة الأفراد وخصوصيتهم. يُعد ذلك خطوة مهمة في مكافحة التضليل الإعلامي وحماية الحقوق الشخصية في الفضاء الرقمي[92].

وترى الباحثة، أن المرسوم بقانون اتحادي رقم (34) لسنة 2021 في الإمارات العربية المتحدة يُعتبر خطوة هامة نحو تعزيز الحماية الجنائية للبيانات الشخصية والخصوصية الرقمية، ويُسهم في مكافحة الجرائم الإلكترونية والشائعات التي يمكن أن تضر بالمجتمع والأفراد.

نصت المادة (6) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة، على أنه: "يعاقب بالحبس مدة لا تقل عن (6) ستة أشهر والغرامة التي لا تقل عن (20,000) عشرين ألف درهم ولا تزيد على (100,000) مائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات شخصية إلكترونية، باستخدام تقنية المعلومات أو وسيلة تقنية معلومات. 2- فإذا كانت البيانات أو المعلومات المُشار إليها في البند (1) من هذه المادة، تتعلق بفحوصات أو تشخيص أو علاج أو رعاية أو سجلات طبية أو حسابات مصرفية أو بيانات ومعلومات وسائل الدفع الإلكترونية عد ذلك ظرفاً مشدداً. 3- ويعاقب بالحبس والغرامة، أو بإحدى هاتين العقوبتين، كل من تلقى أي من البيانات والمعلومات المُشار إليها بالبندين (1)، (2) من هذه المادة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها"[93].

المادة (6) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 تعد من النصوص القانونية المهمة في دولة الإمارات العربية المتحدة التي تهدف إلى مكافحة الجرائم الإلكترونية وحماية البيانات والمعلومات الشخصية للأفراد. تتميز هذه المادة بتقديمها تعريفاً واضحاً للسلوكيات المعاقب عليها والعقوبات المرتبطة بها، بالإضافة إلى توضيح الظروف المشددة للعقوبة والمسؤولية القانونية للأشخاص الذين يتلقون أو يستخدمون البيانات المحصل عليها بطريقة غير مشروعة[94].

الفقرة الأولى من المادة تحدد السلوكيات المعاقب عليها بشكل دقيق، وتشمل الحصول على البيانات الشخصية الإلكترونية، الاستحواذ عليها، تعديلها، إتلافها، إفشاءها، تسريبها، إلغاءها، حذفها، نسخها، نشرها أو إعادة نشرها بدون تصريح. وتشدد على أن استخدام تقنية المعلومات أو وسيلة تقنية معلومات في ارتكاب هذه الأفعال يعد محوراً رئيسياً لتحديد المسؤولية الجنائية[95].

الفقرة الثانية تُبرز الظروف المشددة للعقوبة، موضحة أنه إذا كانت البيانات أو المعلومات الشخصية تتعلق بموضوعات حساسة وخاصة مثل الفحوصات الطبية، التشخيص، العلاج، الرعاية الصحية، السجلات الطبية، الحسابات المصرفية، أو بيانات وسائل الدفع الإلكترونية، فإن ذلك يعتبر ظرفاً مشدداً يُمكن أن يؤدي إلى تشديد العقوبة المفروضة على الجاني[96].

الفقرة الثالثة تتناول المسؤولية الجنائية للأشخاص الذين يتلقون أو يستخدمون البيانات الشخصية المحصل عليها بشكل غير مشروع. تُشدد هذه الفقرة على أن الشخص الذي يتلقى هذه البيانات ويحتفظ بها أو يخزنها أو يتعامل بها أو يستخدمها، رغم علمه بعدم مشروعية الحصول عليها، يعد مسؤولاً جنائياً ويمكن معاقبته بالحبس والغرامة، أو بإحدى هاتين العقوبتين[97].

وترى الباحثة، أن هذه المادة تسعى إلى تعزيز حماية البيانات الشخصية في الفضاء الإلكتروني وردع الأفعال التي قد تؤدي إلى انتهاك خصوصية الأفراد وأمان بياناتهم الشخصية، وذلك من خلال تحديد العقوبات والمسؤوليات الجنائية بشكل واضح وصارم.

الفصل الثاني

حالات معالجة البيانات الشخصية

تمهيد وتقسيم:

معالجة البيانات الشخصية تعتبر عملية حساسة ومعقدة تتطلب توافر معايير عالية من الشفافية والأمان، وهناك العديد من الحالات التي يمكن فيها معالجة هذه البيانات بطريقة قانونية وآمنة. يتم معالجة البيانات الشخصية في سياقات مختلفة، مثل الأغراض الإدارية والمالية، التحليلات واتخاذ القرارات، الأبحاث والتطوير، وكذلك في سياق الخدمات الصحية والتعليمية. في جميع هذه الحالات، يجب أن يتم التعامل مع البيانات الشخصية بطريقة تضمن حمايتها من التلاعب والوصول غير المشروع. يتطلب القانون عادةً الحصول على موافقة صريحة من الشخص المعني قبل معالجة بياناته الشخصية، ويجب توضيح الغرض من المعالجة بشكل واضح وشفاف. كما يجب على الجهات المعنية بمعالجة البيانات تطبيق تدابير أمان صارمة لحماية هذه البيانات من أي تهديدات محتملة، وضمان السرية التامة. في حالات الخرق أو التلاعب بالبيانات الشخصية، يجب على الجهات المعنية اتخاذ الإجراءات الفورية لتصحيح الوضع وإبلاغ الشخص المعني والسلطات المختصة. تلتزم الجهات المعنية أيضًا بمبدأ الشفافية وتوفير الحق في الوصول والتصحيح للشخص المعني بشأن بياناته الشخصية[98].

وللتعرف على حالات معالجة البيانات الشخصية، سيتم تقسيم هذا الفصل إلى ثلاثة مباحث، وذلك على النحو التالي:

المبحث الأول: حالات معالجة البيانات الشخصية بدون موافقة صاحبها.

المبحث الثاني: نقل ومشاركة البيانات الشخصية عبر الحدود.

المبحث الثالث: تقديم الشكوى والتظلم لضمان حماية البيانات الشخصية.

المبحث الأول

حالات معالجة البيانات الشخصية بدون موافقة صاحبها

تمهيد وتقسيم:

توجد حالات استثنائية يمكن فيها معالجة البيانات الشخصية بدون الحاجة إلى الحصول على موافقة صاحبها، وهي تتضمن غالباً الظروف التي تكون فيها المعالجة ضرورية لأغراض محددة ومشروعة. على سبيل المثال، قد تتم المعالجة بدون موافقة في حالات الضرورة القصوى لحماية الحياة أو الصحة البدنية للشخص المعني أو لشخص آخر، أو إذا كانت المعالجة ضرورية لأداء عقد يكون الشخص المعني طرفاً فيه، أو لاتخاذ الإجراءات التمهيدية لإبرام عقد. كما يمكن معالجة البيانات بدون موافقة عندما تكون هناك مصلحة عامة ذات أهمية قصوى، أو للامتثال لالتزام قانوني، أو لحماية المصالح الحيوية للشخص المعني. في هذه الحالات، يجب أن تتم المعالجة بما يتوافق مع المبادئ العامة لحماية البيانات، وعلى الجهات المسؤولة عن المعالجة توفير الضمانات الكافية لحماية البيانات وضمان معالجتها بشكل عادل وشفاف. يتوجب كذلك على الجهات المعنية تقديم معلومات واضحة حول سبب المعالجة والغرض منها، وتحديد الأساس القانوني الذي يبرر المعالجة بدون موافقة، مع توفير الإمكانية للشخص المعني بممارسة حقوقه فيما يتعلق ببياناته الشخصية[99].

وللتعرف على حالات معالجة البيانات الشخصية بدون موافقة صاحبها، سيتم تقسيم هذا المبحث إلى ثلاثة مطالب، وذلك على النحو التالي:

المطلب الأول: أن تكون المعالجة ضرورية لحماية المصلحة العامة.

المطلب الثاني: أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات.

المطلب الثالث: أن تكون المعالجة ضرورية لحماية الصحة العامة.

المطلب الأول

أن تكون المعالجة ضرورية لحماية المصلحة العامة

تعتبر المصلحة العامة من الأسباب الجوهرية التي يمكن بموجبها معالجة البيانات الشخصية بدون الحصول على موافقة صاحبها، حيث يتم التأكيد على أن المعالجة في هذه الحالة يجب أن تكون ضرورية ولا مفر منها لحماية مصالح عليا تتعلق بالمجتمع ككل. في سياق التشريع الإماراتي، يتم تحديد هذه الحالات بدقة لضمان أن لا يتم استغلال الاستثناء بشكل ينتهك خصوصية الأفراد. يتطلب هذا من الجهات المعالجة للبيانات توفير مبررات واضحة وقوية تثبت أن المعالجة تخدم المصلحة العامة بشكل مباشر، وأنه لا يمكن تحقيق الغرض المرجو بدون استخدام البيانات الشخصية. على سبيل المثال، قد يتعلق الأمر بمعالجة البيانات لأغراض الوقاية من الأمراض والأوبئة، أو لضمان الأمان الوطني. يجب على الجهات المعنية أيضًا أن تتخذ جميع التدابير اللازمة لضمان أمان البيانات وحمايتها من أي إساءة استخدام، وأن تقوم بمراجعة دورية لتقييم ما إذا كانت الحاجة إلى المعالجة ما زالت قائمة أم لا. في النهاية، يجب أن تكون هناك توازن دقيق بين حماية البيانات الشخصية وتحقيق المصلحة العامة، مع ضمان حقوق الأفراد وحرياتهم الأساسية[100].

نص البند (1) من المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، على أنه: "يُحظر معالجة البيانات الشخصية بدون موافقة صاحبها، وتُستثنى أي من الحالات التالية من هذا الحظر وتعتبر المعالجة حينها مشروعة: 1- أن تكون المعالجة ضرورية لحماية المصلحة العامة"[101].

النص المُقدم في البند (1) من المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة يرسي مبدأ أساسي يتعلق بحماية البيانات الشخصية، وهو أنه لا يُمكن معالجة هذه البيانات دون الحصول على موافقة صاحب البيانات. هذا المبدأ يعكس الاهتمام المتزايد بحماية خصوصية الأفراد وضمان أن يتم استخدام بياناتهم بطريقة شفافة وآمنة[102].

النص يشير أيضًا إلى وجود استثناءات لهذا القاعدة، حيث يُمكن معالجة البيانات الشخصية دون الحصول على موافقة صاحبها في حالات معينة. واحدة من هذه الحالات، والتي تُشدد عليها في هذا البند بالذات، هي إذا كانت المعالجة ضرورية لحماية المصلحة العامة[103].

مصطلح "المصلحة العامة" يحمل في طياته طابعًا واسعًا ويمكن أن يشمل مجموعة من الظروف والسياقات المختلفة. في سياق حماية البيانات، قد يُشير هذا إلى الحاجة إلى معالجة البيانات لأسباب تتعلق بالصحة العامة، الأمان القومي، أو لمكافحة الجريمة وحماية النظام العام، وغيرها من الأمور التي تؤثر على المجتمع بأكمله[104].

مع ذلك، من المهم أن يتم تفسير هذا الاستثناء بدقة وعناية، حيث يجب عدم استخدامه بشكل يسمح بالتجاوز على خصوصية الأفراد وحقوقهم دون مبرر قوي. يتوجب على الجهات التي تقوم بمعالجة البيانات في سياق "المصلحة العامة" أن تظهر بوضوح الحاجة إلى هذه المعالجة وأن تُثبت أنه لا يُمكن تحقيق الغرض المطلوب بطرق أخرى أقل تدخلاً في خصوصية الأفراد[105].

وترى الباحثة، أن هذا النص يُسلط الضوء على التوازن الدقيق الذي يجب أن يتم الحفاظ عليه بين حماية خصوصية الأفراد وضمان القدرة على معالجة البيانات الشخصية عند الحاجة لتحقيق مصالح

المجتمع العامة. يُمثل هذا جزءًا أساسيًا من الإطار القانوني لحماية البيانات في دولة الإمارات العربية المتحدة، ويعكس التزام الدولة بضمان استخدام البيانات الشخصية بطريقة مسؤولة وشفافة.

المطلب الثاني

أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات

في سياق حماية البيانات الشخصية ومعالجتها إلكترونياً في التشريع الإماراتي، يُعدُّ السماح بمعالجة البيانات الشخصية بدون الحصول على موافقة صاحبها في حال كانت هذه البيانات قد أصبحت متاحة ومعروفة للعامة بفعل من صاحب البيانات نفسه استثناءً مهماً. يُشترط في هذه الحالة أن يكون الشخص قد قام بنشر بياناته بشكل علني وواضح، مما يعني تنازله ضمنياً عن جزء من حقوقه في حماية هذه البيانات. ومع ذلك، يتوجب على الجهات التي تقوم بمعالجة البيانات مراعاة مبادئ الحماية واتخاذ الإجراءات اللازمة لضمان عدم استخدام البيانات بطريقة تنتهك خصوصية الشخص أو تضر بمصالحه. كما يجب عليهم التأكد من صحة البيانات وتحديثها، وأن يكون الغرض من المعالجة واضحاً ومحدداً. يُعدُّ التشريع الإماراتي في هذا المجال صارماً، حيث يضع حماية الأفراد وخصوصيتهم في مقدمة أولوياته، مما يتطلب من الجهات المعنية الالتزام بمعايير عالية من الشفافية والمسؤولية عند معالجة البيانات الشخصية، حتى وإن كانت هذه البيانات قد أصبحت متاحة للعامة بفعل من صاحبها[106].

نص البند (2) من المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، على أنه: "يُحظر معالجة البيانات الشخصية بدون موافقة صاحبها، وتُستثنى أي من الحالات التالية من هذا الحظر وتعتبر المعالجة حينها مشروعة: 2- أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعلومة للكافة بفعل من صاحب البيانات"[107].

تنص المادة المذكورة من القانون الاتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة على تحديد استثناء من القاعدة العامة التي تتطلب الحصول على موافقة صاحب البيانات قبل معالجة بياناته الشخصية. الاستثناء المحدد في هذا البند يشير إلى الحالة التي تكون فيها البيانات الشخصية قد أصبحت متاحة ومعلومة للعامة بفعل من صاحب البيانات نفسه[108].

هذا يعني أنه إذا قام الشخص بنشر بياناته الشخصية بنفسه في مكان عام أو على منصات التواصل الاجتماعي أو في أي سياق آخر يمكن الوصول إليه بسهولة من قبل العامة، فإن هذه البيانات تصبح متاحة للجميع ولا تتطلب المعالجة موافقة إضافية من صاحبها[109].

مع ذلك، يجب التنويه إلى أن هذا الاستثناء لا يعني أن البيانات الشخصية المنشورة يمكن استخدامها بشكل عشوائي أو دون قيود. يتوجب على الجهات التي تقوم بمعالجة هذه البيانات أن تتأكد من أن استخدامها يتماشى مع القوانين واللوائح المعمول بها وأنه لا ينتهك حقوق وخصوصية الأفراد[110].

بالإضافة إلى ذلك، يجب أن يكون هناك وعي بأن البيانات الشخصية، حتى لو كانت متاحة للعامة، لا تزال تحمل طابعاً شخصياً وحساساً، ويجب التعامل معها بعناية واحترام لخصوصية صاحبها[111].

وترى الباحثة، أن هذا الاستثناء يسعى إلى تحقيق التوازن بين حماية خصوصية الأفراد وضرورة تسهيل بعض الأنشطة التي قد تتطلب معالجة البيانات الشخصية. ويعكس التزام الدولة بضمان حماية البيانات الشخصية، مع الأخذ في الاعتبار السياق الذي تم فيه الكشف عن هذه البيانات.

المطلب الثالث

أن تكون المعالجة ضرورية لحماية الصحة العامة

في إطار الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً بموجب التشريع الإماراتي، تبرز الأهمية القصوى لمعالجة البيانات الشخصية دون الحاجة إلى موافقة صاحبها عندما تكون هذه المعالجة ضرورية لحماية الصحة العامة. يُعتبر هذا الاستثناء حيوياً في حالات الطوارئ الصحية والأوبئة، حيث يتطلب الأمر جمع وتحليل البيانات الصحية للأفراد بشكل سريع وفعّال لاتخاذ التدابير اللازمة للحد من انتشار الأمراض وحماية المجتمع[112]. ومع ذلك، يستلزم ذلك ضمانات قوية لحماية حقوق الأفراد وخصوصيتهم، مع التأكيد على مبدأ الشفافية والمساءلة في معالجة البيانات. يجب أن تكون المعالجة محددة الغرض، ومقتصرة على ما هو ضروري لتحقيق الهدف المرجو، ويجب أن تُتخذ جميع التدابير اللازمة لضمان أمان البيانات وحمايتها من أي سوء استخدام. يُعد التشريع الإماراتي في هذا السياق متقدماً، حيث يوفر إطاراً قانونياً متكاملاً يحمي البيانات الشخصية مع السماح بمرونة كافية للتعامل مع الحالات الطارئة التي تتطلب معالجة سريعة وفعّالة للبيانات الشخصية بهدف حماية الصحة العامة[113].

نص البند (5) من المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، على أنه: "يُحظر معالجة البيانات الشخصية بدون موافقة صاحبها، وتُستثنى أي من الحالات التالية من هذا الحظر وتعتبر المعالجة حينها مشروعة: 5- أن تكون المعالجة ضرورية لحماية الصحة العامة، وتشمل الحماية من الأمراض السارية والأوبئة أو

لأغراض سلامة وجودة الرعاية الصحية والأدوية والعقاقير والأجهزة الطبية، وفقاً للتشريعات السارية في الدولة"[114].

تستهدف هذه المادة المذكورة ضمان حماية البيانات الشخصية للأفراد في دولة الإمارات العربية المتحدة، وتشدد على ضرورة الحصول على موافقة صاحب البيانات قبل معالجتها. ومع ذلك، تعترف بضرورة إيجاد توازن بين حماية الخصوصية وتحقيق الصالح العام، ولهذا تتضمن استثناءات لحالات محددة تعتبر فيها معالجة البيانات الشخصية مشروعة حتى بدون موافقة صاحبها. يبرز البند (5) من المادة (4) واحدة من هذه الحالات الاستثنائية، حيث يعتبر المعالجة ضرورية لحماية الصحة العامة، بما في ذلك الحماية من الأمراض السارية والأوبئة، وضمان سلامة وجودة الرعاية الصحية والأدوية والعقاقير والأجهزة الطبية. يُظهر هذا النص إدراك المشرع لأهمية البيانات الشخصية وحاجة المجتمع إلى معالجتها في سياقات معينة تتطلب الاستجابة السريعة والفعّالة لحماية الصحة العامة، ويؤكد على ضرورة الالتزام بالتشريعات السارية في الدولة أثناء القيام بذلك، مما يضمن أن يتم تحقيق التوازن بين حماية الخصوصية وضمان الصحة العامة بشكل فعّال ومسؤول[115].

المبحث الثاني

نقل ومشاركة البيانات الشخصية عبر الحدود

تمهيد وتقسيم:

في إطار دراسة الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في التشريع الإماراتي، تُعتبر قضية نقل ومشاركة البيانات الشخصية عبر الحدود من الجوانب الحيوية التي تستحق الدراسة العميقة. الإمارات العربية المتحدة، بصفتها مركزاً تجارياً ومالياً عالمياً، تشهد تبادل هائل للبيانات الشخصية عبر الحدود، مما يثير تحديات معقدة تتعلق بحماية الخصوصية وأمان البيانات. التشريع الإماراتي يتطلب إقامة ضوابط صارمة لضمان أن يتم نقل البيانات الشخصية بطريقة آمنة وأن تظل محمية وفقاً للمعايير القانونية المحلية[116]، حتى عندما تُنقل إلى دول أخرى قد تكون لديها مستويات حماية مختلفة. يجب أن تتوفر آليات واضحة لضمان الموافقة الواعية من قبل الأفراد على نقل بياناتهم، ويجب وضع قيود على كيفية استخدام ومعالجة هذه البيانات في الخارج. كما يُطلب من الكيانات التي تقوم بنقل البيانات توفير ضمانات كافية لحماية هذه البيانات والتحقق من أن الجهات الخارجية التي تتلقى البيانات تلتزم بنفس معايير الحماية. هذا الالتزام بالحفاظ على سلامة وخصوصية البيانات الشخصية عند نقلها عبر الحدود يُظهر التزام الإمارات القوي بحماية حقوق الأفراد وخصوصيتهم في عصر الرقمنة العالمية[117].

وللتعرف على نقل ومشاركة البيانات الشخصية عبر الحدود، سيتم تقسيم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال وجود مستوى حماية ملائم.

المطلب الثاني: نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال عدم وجود مستوى حماية ملائم.

المطلب الأول

نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال وجود مستوى حماية ملائم

يحتل موضوع نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة مكانة خاصة، خصوصاً عندما يكون هناك مستوى حماية ملائم في الدولة المستقبلة للبيانات. يتطلب القانون الإماراتي توفير ضمانات قوية لحماية البيانات الشخصية، ويعتبر نقل البيانات إلى الخارج مقبولاً فقط إذا كانت الدولة المستقبلة توفر مستوى حماية مكافئ أو أعلى من الحماية المقدمة في الإمارات[118]. هذا يعني أنه يجب على الجهات المعنية إجراء تقييم شامل للنظم القانونية والتنظيمية في الدولة المستقبلة قبل الشروع في عملية النقل، لضمان عدم تعرض البيانات للخطر. بالإضافة إلى ذلك، يجب أن يكون هناك شفافية كاملة وإعلام واضح للأفراد المعنيين بشأن نقل بياناتهم، مع توفير الحق في الاعتراض والتحكم في كيفية استخدام ومشاركة بياناتهم الشخصية. إن التأكيد على مستوى الحماية الملائم يعكس التزام الإمارات بتعزيز معايير حماية البيانات الشخصية وتعزيز الثقة في النظام الرقمي، مما يسهم في تعزيز الابتكار والتنمية الاقتصادية مع ضمان حماية حقوق الأفراد وخصوصيتهم[119].

نصت المادة (22) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، على أنه: "يجوز نقل البيانات الشخصية إلى خارج الدولة في الأحوال الآتية المعتمدة من المكتب: 1- أن تكون للدولة أو الإقليم الذي سيتم نقل البيانات الشخصية إليها تشريعات خاصة بحماية البيانات الشخصية فيها، تتضمن أهم الاحكام والتدابير والضوابط والاشتراطات والقواعد الخاصة بحماية خصوصية وسرية البيانات الشخصية لصاحب البيانات، وقدرته على ممارسة حقوقه، وأحكام تتعلق بفرض التدابير المناسبة على المتحكم أو المعالج من خلال جهة رقابية أو قضائية. 2- انضمام الدولة إلى الاتفاقيات الثنائية أو متعددة الأطراف المتعلقة بحماية البيانات الشخصية مع الدول التي سيتم نقل البيانات الشخصية إليها"[120].

تعالج المادة (22) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 مسألة نقل البيانات الشخصية من دولة الإمارات العربية المتحدة إلى خارج حدودها، وهي قضية حساسة نظراً للمخاطر المحتملة على خصوصية الأفراد وحماية بياناتهم الشخصية. تحدد المادة شروطاً واضحة وصارمة لضمان أن يتم هذا النقل في إطار قانوني يحمي البيانات من الاستغلال أو التسريب[121]. أولاً، يجب أن تكون الدولة أو الإقليم الذي سيتم نقل البيانات إليها تمتلك تشريعات متقدمة في مجال حماية البيانات الشخصية، والتي تتضمن بوضوح الأحكام والضوابط اللازمة لحماية خصوصية الأفراد وضمان قدرتهم على ممارسة حقوقهم. يجب أن تشتمل هذه التشريعات على إجراءات لفرض التدابير المناسبة على الجهات التي تتحكم أو تعالج البيانات، سواء عن طريق الرقابة الإدارية أو القضائية. ثانياً، يجب أن تكون الدولة المستقبلة للبيانات طرفاً في اتفاقيات ثنائية أو متعددة الأطراف تتعلق بحماية البيانات

الشخصية، مما يعزز من ضمانات حماية البيانات ويوفر إطاراً دولياً للتعاون في هذا المجال. وبالتالي، تسعى هذه المادة إلى إرساء أساس قوي لحماية البيانات الشخصية عند نقلها عبر الحدود، مع التأكيد على ضرورة الحصول على موافقة واعتماد من المكتب المختص في الدولة، لضمان الالتزام بأعلى معايير الحماية والشفافية[122].

المطلب الثاني

نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال عدم وجود مستوى حماية ملائم

في إطار البحث الدقيق حول الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في التشريع الإماراتي، يبرز التحدي الكبير المتعلق بنقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في الحالات التي لا يوجد فيها مستوى حماية ملائم في الدولة المستقبلة للبيانات. يُعتبر هذا الأمر محفوفًا بالمخاطر، حيث أن غياب معايير حماية البيانات الملائمة قد يعرض المعلومات الشخصية للخطر، ويُمكن أن يؤدي إلى استغلالها أو إساءة معاملتها بطرق قد تضر بالأفراد المعنيين. يُلزم القانون الإماراتي بوجوب توفر ضمانات قانونية وتنظيمية قوية قبل الإقدام على مثل هذه العمليات، ويشدد على ضرورة إجراء تقييم دقيق لمخاطر نقل البيانات ووضع آليات لحمايتها[123].

في هذا السياق، يُصبح التحقق من الامتثال للقوانين والتنظيمات الإماراتية والتأكد من توفير الحماية الكافية للبيانات الشخصية عند نقلها عبر الحدود، أمراً بالغ الأهمية. يُعد التزام الجهات المعنية بمبادئ الشفافية والمسؤولية، وتوفير الإعلام الكافي للأفراد حول كيفية وأماكن معالجة بياناتهم الشخصية، إضافةً إلى ضمان حقوقهم في الوصول إلى بياناتهم وتصحيحها، عناصر جوهرية لبناء نظام فعّال لحماية البيانات الشخصية في مواجهة التحديات التي يطرحها نقل البيانات عبر الحدود[124].

نصت المادة (23) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، على أنه: "1- استثناءً مما ورد في المادة (22) من هذا المرسوم بقانون، يجوز نقل البيانات الشخصية إلى خارج الدولة في الحالات التالية: أ- في الدول التي لا يتوافر فيها قانون لحماية البيانات، يجوز للمنشآت العاملة في الدولة وفي تلك الدول أن تنقل البيانات بموجب عقد أو اتفاقية يلزم المنشأة في تلك الدول بتطبيق الأحكام والتدابير والضوابط والاشتراطات الواردة في هذا المرسوم بقانون شاملاً أحكاماً تتعلق بفرض التدابير المناسبة على المتحكم أو المعالج من خلال جهة رقابية أو قضائية معينة في تلك الدولة وتحدد في العقد. ب- الموافقة الصريحة من صاحب البيانات على نقل بياناته الشخصية خارج الدولة بما لا يتعارض مع المصلحة العامة والأمنية للدولة. ج- إذا كان النقل ضروري لتنفيذ التزامات وإثبات الحقوق أمام الجهات القضائية أو ممارستها أو الدفاع عنها. د- إذا كان النقل ضروري لإبرام أو تنفيذ عقد مبرم بين المتحكم وصاحب البيانات، أو بين المتحكم والغير لتحقيق مصلحة صاحب البيانات. ه- إذا كان النقل ضروري تنفيذاً لإجراء متعلق بتعاون دولي. و- إذا كان النقل ضروري لحماية المصلحة العامة. 2- تحدد اللائحة التنفيذية لهذا

المرسوم بقانون الضوابط والاشتراطات للحالات المشار إليها في البند (1) من هذه المادة، والتي يجب أن تتوفر في حالات نقل البيانات الشخصية إلى خارج الدولة"[125].

تُقدم المادة (23) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 توضيحات واستثناءات هامة بشأن نقل البيانات الشخصية من دولة الإمارات العربية المتحدة إلى خارج الدولة، وذلك في سياق حماية البيانات الشخصية. تُعتبر هذه المادة استثناءً من القواعد العامة الموضحة في المادة (22) التي تتطلب ضوابط صارمة لنقل البيانات الشخصية إلى خارج الدولة[126].

تُمكن المادة (23) الجهات المعنية في الإمارات من نقل البيانات الشخصية إلى دول لا تمتلك تشريعات لحماية البيانات، شريطة إبرام عقد أو اتفاقية تلزم الطرف المستقبل للبيانات بتطبيق نفس الأحكام والضوابط التي ينص عليها القانون الإماراتي، بما في ذلك فرض التدابير المناسبة لحماية البيانات وتحديد جهة رقابية أو قضائية في الدولة المستقبلة للبيانات لمتابعة تنفيذ هذه الالتزامات[127].

كما تتيح المادة إمكانية نقل البيانات بناءً على موافقة صريحة من صاحب البيانات، شرط ألا يتعارض ذلك مع المصلحة العامة والأمنية للدولة. وتتضمن المادة أيضاً حالات أخرى تبرر نقل البيانات، مثل الحاجة لتنفيذ التزامات قانونية، أو إثبات حقوق أمام الجهات القضائية، أو تنفيذ عقود، أو تحقيق التعاون الدولي، أو حماية المصلحة العامة. وأخيراً، تُشير المادة إلى أن اللائحة التنفيذية للمرسوم بقانون ستحدد الضوابط والاشتراطات الخاصة بنقل البيانات الشخصية إلى خارج الدولة، مما يُعطي إطاراً تفصيلياً وواضحاً لتنفيذ هذه الاستثناءات[128].

المبحث الثالث

تقديم الشكوى والتظلم لضمان حماية البيانات الشخصية

تمهيد وتقسيم:

في إطار ضمان حماية البيانات الشخصية، يعتبر حق تقديم الشكوى والتظلم حجر الزاوية لتمكين الأفراد من الدفاع عن خصوصيتهم وحماية بياناتهم. يتيح هذا الحق للأشخاص المتضررين من معالجة بياناتهم الشخصية بطريقة غير قانونية أو غير عادلة، أو الذين يعتقدون أن حقوقهم في مجال حماية البيانات قد انتهكت، اللجوء إلى الجهات الرقابية المختصة لتقديم شكواهم وطلب التدخل لحل المشكلة. تلعب الجهات الرقابية دوراً حيوياً في تحقيق التوازن بين حقوق الأفراد ومتطلبات معالجة البيانات، من خلال التحقيق في الشكاوى، وتقديم التوجيهات، واتخاذ الإجراءات اللازمة لضمان الامتثال للقوانين واللوائح المعمول بها. يُعزز توفير آلية فعّالة لتقديم الشكوى والتظلم من ثقة الأفراد في نظام حماية البيانات، ويسهم في خلق بيئة رقمية آمنة تحترم الحقوق الشخصية وتحمي البيانات الشخصية من أي استغلال أو إساءة معاملة[129].

وللتعرف على كيفية تقديم الشكوى والتظلم لضمان حماية البيانات الشخصية، سيتم تقسيم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: تقديم الشكوى في حالة وجود مخالفة تتعلق بمعالجة البيانات الشخصية.

المطلب الثاني: التظلم من قرارات مكتب الإمارات للبيانات.

المطلب الأول

تقديم الشكوى في حالة وجود مخالفة تتعلق بمعالجة البيانات الشخصية

عندما يتعرض الأفراد لمخالفات تتعلق بمعالجة بياناتهم الشخصية، يصبح تقديم الشكوى إلى الجهات المعنية خطوة جوهرية للحفاظ على حقوقهم وضمان احترام خصوصيتهم. يتوجب على الشخص المتضرر أن يُعد وثيقة شكوى مفصلة، يُوضح فيها طبيعة المخالفة، والأطراف المعنية، والتأثير الذي ترتب على معالجة بياناته بشكل غير قانوني[130]. ينبغي أن تشتمل الشكوى على جميع الأدلة والمستندات الداعمة التي يمكن أن تُسهم في إثبات الواقعة وتسهيل عمل الجهات الرقابية في التحقيق واتخاذ الإجراءات اللازمة. من الضروري أن تُقدم الشكوى في الوقت المناسب ووفقاً للإجراءات المحددة لضمان سرعة الاستجابة وفعالية التعامل مع المشكلة[131]. إن وجود آلية شفافة وفعّالة لتقديم الشكوى يعكس التزام الدولة بحماية البيانات الشخصية ويُعزز من ثقة المواطنين في نظام حماية الخصوصية، ما يُسهم في خلق بيئة رقمية آمنة وموثوقة[132].

نصت المادة (24) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، على أنه: "1- لصاحب البيانات أن يتقدم إلى المكتب بشكوى، إذا كان لديه ما يحمله على الاعتقاد بوقوع أي مخالفة لأحكام هذا المرسوم بقانون، أو بأن المتحكم أو المعالج يقوم بمعالجة بياناته الشخصية بالمخالفة لأحكامه وفقاً للإجراءات والقواعد التي يحددها المكتب في هذا الشأن. 2- يتولى المكتب استلام الشكاوى المقدمة من صاحب البيانات وفقاً للبند (1) من هذه المادة، والتحقق منها بالتنسيق مع المتحكم والمعالج. 3- للمكتب توقيع الجزاءات الإدارية المشار إليها في المادة (26) من هذا المرسوم بقانون في حال ثبوت مخالفة المتحكم أو المعالج لأحكامه أو مخالفة القرارات الصادرة تنفيذاً له"[133].

تركز المادة (24) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 على إعطاء صاحب البيانات الحق في تقديم شكوى إلى المكتب المعني بحماية البيانات في دولة الإمارات العربية المتحدة، في حال كان لديه أسباب تجعله يعتقد أن هناك مخالفة لأحكام هذا المرسوم بقانون، أو أن المتحكم أو المعالج يتعامل مع بياناته الشخصية بطريقة مخالفة للقانون[134].

تُلزم هذه المادة المكتب بالتحقق من الشكاوى المقدمة والتنسيق مع المتحكم والمعالج لضمان التحقيق الشامل في الشكوى وتحديد ما إذا كانت هناك مخالفة فعلاً للقوانين المتعلقة بحماية البيانات الشخصية[135].

بالإضافة إلى ذلك، تمنح المادة المكتب الحق في توقيع الجزاءات الإدارية المحددة في المادة (26) في حال ثبتت مخالفة المتحكم أو المعالج للقوانين أو للقرارات الصادرة تنفيذًا لهذا المرسوم

بقانون[136].

وترى الباحثة، أن بهذه الطريقة، تسعى المادة (24) إلى تعزيز حماية البيانات الشخصية وتوفير وسيلة للأفراد للدفاع عن حقوقهم وضمان معالجة بياناتهم الشخصية بشكل قانوني وآمن. تُظهر هذه المادة التزام الإمارات بحماية البيانات الشخصية وتوفير الآليات اللازمة لضمان احترام هذه الحقوق.

المطلب الثاني

التظلم من قرارات مكتب الإمارات للبيانات

التظلم من قرارات مكتب الإمارات للبيانات يعتبر جزءًا لا يتجزأ من حقوق الأفراد في ضمان حماية بياناتهم الشخصية، حيث يمنحهم فرصة لمراجعة وتقييم القرارات التي قد تؤثر على خصوصيتهم وحماية بياناتهم. عندما يتقدم الفرد بتظلم، يُتوقع منه أن يُقدم بيانًا وافيًا ودقيقًا يشرح فيه أسباب اعتراضه على القرار، مرفقًا بكافة الوثائق والمستندات التي يعتقد أنها قد تساهم في دعم قضيته. تتطلب هذه العملية من مكتب الإمارات للبيانات أن يعيد النظر في قراره بناءً على المعلومات والأدلة الجديدة المُقدمة، وأن يتخذ قرارًا عادلاً ومنصفًا يعكس التزام الدولة بحماية البيانات الشخصية[137]. يجب أن يكون النظام القانوني واضحًا وشفافًا بشأن الإجراءات والمواعيد النهائية للتظلم، وأن يضمن للأفراد الحق في الحصول على استجابة في وقت معقول. إن السماح للأفراد بالتظلم من قرارات مكتب الإمارات للبيانات يُعزز من مبدأ المساءلة والشفافية في عملية حماية البيانات، ويُسهم في بناء ثقة المواطنين في النظام القانوني والرقابي الذي يحمي خصوصيتهم[138].

نصت المادة (25) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، على أنه: "يجوز لكل ذي مصلحة التظلم خطياً لمدير عام المكتب من أي قرار أو جزاء إداري أو إجراء اتخذ بحقه من قبل المكتب، وذلك خلال (30) ثلاثين يوماً من تاريخ إخطاره بذلك القرار أو الجزاء الإداري أو الإرجاء، ويتم البت في هذا التظلم خلال (30) ثلاثين يوماً من تاريخ تقديمه. ولا يجوز الطعن على أي قرار يصدره المكتب تطبيقاً لأحكام هذا المرسوم بقانون، دون التظلم منه. وتبين اللائحة التنفيذية لهذا المرسوم بقانون إجراءات التظلم والبت فيه"[139].

يتبين أن المادة (25) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية تنص على توفير آلية قانونية للأشخاص ذوي المصلحة للتعبير عن معارضتهم وتقديم تظلماتهم بخصوص القرارات الإدارية أو العقوبات التي قد تكون قد فُرضت عليهم من قبل المكتب المسؤول عن حماية البيانات الشخصية[140]. يُمنح الأشخاص مهلة زمنية قدرها 30 يومًا من تاريخ إبلاغهم بالقرار أو العقوبة الإدارية لتقديم تظلمهم خطيًا إلى المدير العام للمكتب، ومن ثم يُلزم المكتب بالبت في التظلم خلال مدة زمنية مماثلة. هذه الآلية تضمن للأفراد حقهم في الاعتراض والدفاع عن مصالحهم، وتفتح المجال لإعادة النظر في القرارات الإدارية التي قد تؤثر على حقوقهم. بالإضافة إلى ذلك، تشدد المادة على أنه لا يمكن الطعن في أي قرار يصدره المكتب إلا بعد استنفاذ طريق التظلم،

مما يعني أن الطريق القانوني يجب أن يُتبع بشكل صحيح قبل اللجوء إلى أية وسائل قضائية أخرى. وأخيرًا، تترك المادة التفصيل الدقيق لإجراءات التظلم والبت فيه لتحديده في اللائحة التنفيذية لهذا المرسوم بقانون، مما يوفر المرونة اللازمة لضمان تنفيذ الإجراءات بشكل فعال وعادل[141].

خاتمة البحث

تُمثل الحماية الجنائية للبيانات الشخصية المعالجة إلكترونيًا في التشريع الإماراتي حجر الزاوية في ضمان حقوق الأفراد وحماية خصوصياتهم في عصر يزداد فيه الاعتماد على التكنولوجيا بشكل متسارع. إذ يُعد التشريع الإماراتي نموذجًا يحتذى به في توفير الحماية القانونية والجنائية للبيانات الشخصية، متضمنًا العديد من الأحكام والتدابير التي تُعزز من قدرة الدولة على حماية مواطنيها من أي انتهاكات قد تطال خصوصياتهم الرقمية.

تُظهر دراستنا التحليلية الدقة والعمق في النظر إلى مختلف جوانب حماية البيانات الشخصية، مُسلطة الضوء على الجهود الكبيرة التي بذلتها دولة الإمارات في سبيل وضع تشريعات رصينة تُلبي متطلبات العصر الرقمي وتُحقق التوازن بين حقوق الأفراد وضرورات التطور التكنولوجي.

من الجدير بالذكر أن حماية البيانات الشخصية لا تتوقف عند حدود التشريعات والقوانين فحسب، بل تتطلب تضافر جهود كافة الجهات الفاعلة في المجتمع، بما في ذلك الأفراد والمؤسسات والهيئات الرقابية. فالوعي الرقمي والثقافة القانونية لدى الأفراد تلعب دورًا محوريًا في تعزيز حماية البيانات الشخصية وضمان احترام الخصوصية.

في الختام، تُشكل هذه الدراسة إسهامًا مهمًا في فهم وتحليل الإطار القانوني لحماية البيانات الشخصية في الإمارات، مُقدمةً توصيات وإرشادات قيمة يمكن أن تسهم في تطوير التشريعات وتعزيز آليات الحماية. وتبقى الحاجة ماسة إلى مواصلة البحث والدراسة في هذا المجال، لضمان مواكبة التطورات التكنولوجية المتسارعة وتحقيق أعلى مستويات الحماية للبيانات الشخصية.

أولاً: النتائج:

1- أظهر البحث أن دولة الإمارات قد خطت خطوات كبيرة نحو تطوير التشريعات الرامية لحماية البيانات الشخصية المعالجة إلكترونياً، مما يعكس إدراك الدولة لأهمية هذه القضية في عصر الرقمنة. وتُشير النتائج إلى أن هناك إرادة سياسية قوية والتزامًا حكوميًا بتعزيز حماية الخصوصية والبيانات الشخصية.

2- أكدت الدراسة على الدور الحيوي الذي يلعبه التوعية والتثقيف في مجال حماية البيانات الشخصية، مُشيرة إلى أن زيادة الوعي العام حول هذه القضايا يُمكن أن يساهم بشكل كبير في تعزيز الحماية وتقليل حالات المخالفات والانتهاكات.

3- سلطت الدراسة الضوء على أهمية التعاون والتنسيق الدولي في مجال حماية البيانات الشخصية، خاصة في ظل الطبيعة العابرة للحدود للعديد من المعاملات الإلكترونية وتبادل البيانات. وأشارت إلى أن الإمارات قد اتخذت خطوات في هذا الاتجاه، لكن هناك حاجة إلى مزيد من الجهود لتعزيز التعاون الدولي وضمان حماية فعّالة للبيانات.

4- لفتت الدراسة الانتباه إلى التحديات الكبيرة التي تطرأ نتيجة للتطورات المستمرة في مجال تكنولوجيا المعلومات، وكيف يمكن أن تؤثر هذه التحديات على حماية البيانات الشخصية. وشددت على ضرورة تحديث التشريعات بشكل دوري لمواكبة هذه التطورات وضمان استمرارية الحماية الفعّالة.

5- أبرزت النتائج أهمية دور الهيئات الرقابية في مراقبة تطبيق التشريعات وضمان الالتزام بأحكام حماية البيانات الشخصية. ودعت إلى ضرورة تعزيز قدرات هذه الهيئات وتوفير الموارد اللازمة لها لتمكينها من أداء دورها بكفاءة، فضلاً عن تشجيع التعاون بينها وبين الجهات المعنية الأخرى لتحقيق أفضل النتائج في مجال حماية البيانات الشخصية

ثانياً: التوصيات:

1- يُوصى بضرورة تحديث التشريعات الإماراتية المتعلقة بحماية البيانات الشخصية بشكل دوري ومستمر لمواكبة التطورات السريعة في مجال تكنولوجيا المعلومات والاتصالات، وذلك لضمان بقاءها فعّالة وقادرة على التصدي للتحديات الجديدة التي قد تظهر في هذا المجال. وفي هذا السياق، يجب التأكيد على أهمية التعاون الدولي لتبادل الخبرات وأفضل الممارسات في مجال حماية البيانات الشخصية، وكذلك لتعزيز قدرات الكوادر البشرية المختصة في هذا المجال.

2- من الضروري أيضاً العمل على رفع مستوى الوعي بين المواطنين والمقيمين في الإمارات حول أهمية حماية البيانات الشخصية والمخاطر المترتبة على إساءة استخدامها، وذلك من خلال حملات توعية فعّالة وبرامج تثقيفية مستمرة. ويجب أن تشمل هذه الجهود أيضاً التوعية بالحقوق والواجبات المتعلقة بحماية البيانات الشخصية، وكيفية التعامل مع الانتهاكات المحتملة.

3- على صعيد آخر، يُوصى بتعزيز دور الهيئات الرقابية المعنية بحماية البيانات الشخصية في الإمارات، من خلال توفير الموارد اللازمة لها وتطوير قدراتها الفنية

والإدارية. ويجب أن يشمل ذلك تمكين هذه الهيئات من ممارسة صلاحياتها بشكل فعّال واتخاذ الإجراءات اللازمة في حالة وقوع انتهاكات لأحكام حماية البيانات الشخصية.

4- أخيرًا، يُوصى بتشجيع البحث العلمي والدراسات التحليلية في مجال حماية البيانات الشخصية في الإمارات، بما يسهم في تعميق الفهم لهذه القضية وتطوير الحلول العملية للتحديات المرتبطة بها. ويمكن تحقيق ذلك من خلال دعم المؤسسات البحثية والأكاديمية، وتشجيع التعاون بينها وبين القطاع الخاص والهيئات الحكومية المعنية.

قائمة المراجع

أولاً: قائمة المراجع العربية:

(1) أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية". الدمام: دار الحكمة، 2021.

(2) خالد بن أحمد الجابري: "الجرائم الإلكترونية وأثرها على الخصوصية". أبوظبي: دار الفكر العربي، 2018.

(3) سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا". الرياض: مكتبة العبيكان، 2020.

(4) سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي". دبي: دار القلم، 2021.

(5) عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي". دبي: مكتبة دبي، 2019.

(6) عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي". أبوظبي: دار الكتاب الجامعي، 2019.

(7) علي بن سلطان المنصوري: "الأمان الرقمي وحماية البيانات الشخصية". دبي: دار المعرفة، 2019.
(8) فاطمة سعيد الشامسي: "دور القانون في حماية البيانات الشخصية على الإنترنت". الشارقة: دار الثقافة، 2021.
(9) محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني". الرياض: دار النهضة العربية، 2020.
(10) محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية". دبي: مكتبة الفلاح، 2020.

ثانياً: قائمة المراجع الأجنبية:

(1) Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE". Springer.
(2) Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East". Oxford University Press.
(3) Patel, S. (2019). "Electronic Data Protection in the Arabian Gulf: A Legal Analysis". Cambridge University Press.
(4) Sullivan, C., & Burger, E. (2020). "Cybersecurity, Privacy and Data Protection in the UAE: A Comprehensive Overview". Wiley.

Notes

[←1]

د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني". الرياض: دار النهضة العربية، 2020م، ص104.

[←2]

0 د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي". دبي: دار القلم، 2021م، ص12.

[←3]

() د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي". أبوظبي: دار الكتاب الجامعي، 2019م، ص57.

[←4]

0 د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية". دبي: مكتبة الفلاح، 2020م، ص213.

[←5]

[)]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East". Oxford University Press, p.10.

[←6]

[)]Sullivan, C., & Burger, E. (2020). "Cybersecurity, Privacy and Data Protection in the UAE: A Comprehensive Overview". Wiley, p.64.

[←7]

[)]Sullivan, C., & Burger, E. (2020). "Cybersecurity, Privacy and Data Protection in the UAE: A Comprehensive Overview", Ibid, p.65.

[←8]

() المادة (1) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←9]

0 د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي". دبي: مكتبة دبي، 2019، ص26.

[←10]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.11.

[←11]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص214.

[←12]

0 د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية". الدمام: دار الحكمة، 2021، ص153.

[←13]

[0]Sullivan, C., & Burger, E. (2020). "Cybersecurity, Privacy and Data Protection in the UAE: A Comprehensive Overview", Ibid, p.66.

[←14]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص58.

[←15]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا". الرياض: مكتبة العبيكان، 2020، ص115.

[←16]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص215.

[←17]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص119.

[←18]

0 د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص28.

[←19]

() المادة (1) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←20]

0 د. خالد بن أحمد الجابري: "الجرائم الإلكترونية وأثرها على الخصوصية". أبوظبي: دار الفكر العربي، 2018م، ص151.

[←21]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص59.

[←22]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص216.

[←23]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص109.

[←24]

[0]Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE". Springer, p.174.

[←25]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص60.

[←26]

0 د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص29.

[←27]

() المادة (1) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←28]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص154.

[←29]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص217.

[←30]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص155.

[←31]

()د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص30.

[←32]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص218.

[←33]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.15.

[←34]

[)]Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE", Ibid, p.178.

[←35]

() د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص62.

[←36]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص111.

[←37]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص219.

[←38]

() د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي"، مرجع سابق، ص14.

[←39]

() المادة (5) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←40]

()د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص63.

[←41]

[)]Sullivan, C., & Burger, E. (2020). "Cybersecurity, Privacy and Data Protection in the UAE: A Comprehensive Overview", Ibid, p.68.

[←42]

() المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←43]

0د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص33.

[←44]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص220.

[←45]

() د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص64.

[←46]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص156.

[←47]

() د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي"، مرجع سابق، ص15.

[←48]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.16.

[←49]

() المادة (13) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←50]

0د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص34.

[←51]

() د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص65.

[←52]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص222.

[←53]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص157.

[←54]

() د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي"، مرجع سابق، ص16.

[←55]

[)]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.17.

[←56]

() المادة (16) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←57]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص158.

[←58]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص223.

[←59]

[]Sullivan, C., & Burger, E. (2020). "Cybersecurity, Privacy and Data Protection in the UAE: A Comprehensive Overview", Ibid, p.70.

[←60]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص67.

[←61]

() د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي"، مرجع سابق، ص17.

[←62]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.18.

[←63]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص80.

[←64]

[0]Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE", Ibid, p.180.

[←65]

() المادة (431) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات لدولة الإمارات العربية المتحدة.

[←66]

0د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص37.

[←67]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص225.

[←68]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص115.

[←69]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص124.

[←70]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.19.

[←71]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص81.

[←72]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص158.

[←73]

() المادة (432) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات لدولة الإمارات العربية المتحدة.

[←74]

0د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص38.

[←75]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص226.

[←76]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص160.

[←77]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.24.

[←78]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص82.

[←79]

[0]Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE", Ibid, p.188.

[←80]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص122.

[←81]

() د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص39.

[←82]

() د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي"، مرجع سابق، ص18.

[←83]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص129.

[←84]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص228.

[←85]

()البند (5) من المادة (4) من المرسوم بقانون اتحادي رقم (15) لسنة 2020 بشأن حماية المستهلك في دولة الإمارات العربية المتحدة

[←86]

()د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص147.

[←87]

() د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص83.

[←88]

0د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص40.

[←89]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص123.

[←90]

()د. خالد بن أحمد الجابري: "الجرائم الإلكترونية وأثرها على الخصوصية"، مرجع سابق، ص155.

[←91]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص84.

[←92]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص229.

[←93]

() المادة (6) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة.

[←94]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص148.

[←95]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص130.

[←96]

0د. علي بن سلطان المنصوري: "الأمان الرقمي وحماية البيانات الشخصية". دبي: دار المعرفة، 2019م، ص88.

[←97]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص149.

[←98]

[)]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.26.

[←99]

()Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE", Ibid, p.190.

[←100]

[0]Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE", Ibid, p.195.

[←101]

() البند (1) من المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←102]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص233.

[←103]

() د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص86.

[←104]

0د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص41.

[←105]

[0]Al-Hassan, A. (2018). "The Impact of Cybersecurity Laws on Personal Data Protection in the UAE", Ibid, p.212.

[←106]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص132.

[←107]

() البند (2) من المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←108]

[)]Patel, S. (2019). "Electronic Data Protection in the Arabian Gulf: A Legal Analysis". Cambridge University Press, p.35.

[←109]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص87.

[←110]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص162.

[←111]

() د. علي بن سلطان المنصوري: "الأمان الرقمي وحماية البيانات الشخصية"، مرجع سابق، ص89.

[←112]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص189.

[←113]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.27.

[←114]

() البند (5) من المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←115]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص166.

[←116]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص133.

[←117]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص166.

[←118]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص235.

[←119]

() د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص88.

[←120]

() المادة (22) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←121]

() د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي"، مرجع سابق، ص21.

[←122]

() د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص43.

[←123]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.29.

[←124]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص236.

[←125]

() المادة (23) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←126]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص89.

[←127]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص134.

[←128]

() د. سعيد بن حمد الشرقاوي: "الحماية القانونية للمعلومات الشخصية في عصر التكنولوجيا"، مرجع سابق، ص187.

[←129]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.34.

[←130]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص90.

[←131]

0د. أمل بنت عبد الله العميمي: "الأمن السيبراني وحماية البيانات الشخصية"، مرجع سابق، ص169.

[←132]

() د. فاطمة سعيد الشامسي: "دور القانون في حماية البيانات الشخصية على الإنترنت". الشارقة: دار الثقافة، 2021م، ص225.

[←133]

() المادة (24) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←134]

() د. محمد راشد الزرعوني: "الخصوصية الإلكترونية وحماية البيانات الشخصية"، مرجع سابق، ص237.

[←135]

() د. سلمان بن محمد الأحمدي: "الجرائم الإلكترونية وحماية البيانات الشخصية في التشريع الإماراتي"، مرجع سابق، ص22.

[←136]

0د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص44.

[←137]

[0]Johnson, M., & Turner, P. (2021). "Digital Privacy and Security: Navigating the Challenges in the Middle East", Ibid, p.35.

[←138]

() د. محمد بن ناصر القحطاني: "حماية البيانات الشخصية في القانون الإلكتروني"، مرجع سابق، ص135.

[←139]

() المادة (25) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في دولة الإمارات العربية المتحدة.

[←140]

() د. عبد الرحمن بن سعيد البلوشي: "تحديات حماية البيانات الشخصية في القانون الإماراتي"، مرجع سابق، ص46.

[←141]

0د. عبد الله بن خالد السويدي: "الحماية القانونية للبيانات الشخصية في العالم الرقمي"، مرجع سابق، ص92.