

عنوان البحث

الحماية الجنائية الموضوعية لخصوصية البيانات الشخصية في ظلّ العصر الرقميّ

في القانون الإماراتيّ (دراسة مقارنة)

الباحث / هيثم على محمد الناعور

دكتوراه الفلسفة في القانون العام - كلية القانون جامعة الشارقة .

و السيد الأستاذ الدكتور / محمد نور الدين سيد

أستاذ القانون الجنائي المشارك

كلية القانون - جامعة الشارقة .

مُلخَصُ الدِّرَاسَةِ:

حاولت الدِّراسةُ توضيحَ تأثيرِ التكنولوجيا الحديثةِ على حياة الفرد، إذ أصبحت البياناتُ الشخصيةُ للأفراد تسبِّحُ في العالمِ الرقْمِيِّ لأغراضٍ اقتصاديةٍ أو سياسيةٍ أو تجاريةٍ أو اجتماعيةٍ، وقد أدّى ذلك إلى تعرُّض الفرد إلى الاعتداءِ علي بياناته الشخصية من الشركات الضخمة، ممّا دفع بالمشرِّعِ الاتِّحاديِّ إلى إيجادِ حمايةٍ للبياناتِ الخاصة، فعَمَلَ على تجريمِ انتهاكِ حرمةِ البيانات الشخصية في العالمِ الرقْمِيِّ وفقاً للقانونِ الاتِّحاديِّ رقم ٢٠٢١/٤٥ والقوانين والتشريعات المُكملة للعقوبات، فضلاً عما أقرّه دستور الدولة من حمايةٍ للحقوق والحريات؛ وذلك بالنصِّ عليها وإعطائها حمايةً دستوريةً بالموادِّ من ٢٥-٤٤. وقد ناقشت الدِّراسةُ البياناتِ الشخصيةَ المتصلةَ بشخصٍ مُعيَّن والمرتبطةَ بالاتِّصالِ بالتكنولوجيا الحديثة كشرطٍ أساسٍ لتقريرِ الحمايةِ القانونيةِ ذات الطابعِ الجزائيِّ وفَقَّ قوانينٍ وتشريعاتٍ دولة الإمارات. وقد استخدمَ الباحثُ المنهجَ الوصفيَّ التحليليَّ المُقارن؛ لتقريرِ الحمايةِ القانونيةِ في قوانينٍ وتشريعاتٍ دولة الإمارات العربية المتحدة، إضافةً إلى التشريعِ المُقارنِ مُتمثلاً في أحكامِ القانونِ المصريِّ، وتوصلنا في هذا الخصوص إلى عددٍ من النتائجِ والتوصياتِ الجوهريةِ، أهمُّها: أنه حتى وقتنا الراهن لم يتمَّ تنظيمِ لائحةٍ تنفيذيةٍ لقانونِ حمايةِ البيانات الشخصيةِ الاتِّحاديِّ، وهذا ما دعانا إلى التوصيةِ بالتَّعجيلِ في إصدارِ هذه اللائحة.

الكلمات المفتاحية: البيانات الشخصية - الحماية الجزائية - الخصوصية المعلوماتية - البيانات المُعالجة - المُجتمع الرقْمِي.

Abstract:

The study tried to clarify the impact of modern technology on the life of the individual, so the personal data of individuals swims in the digital world for economic, political, commercial or social purposes, and this has led to the exposure of the individual to the assault on his personal data from large companies, which prompted the federal legislator to find protection for private data, so he worked to criminalize the violation of the sanctity of personal data in the digital world in accordance with Federal Law No. 45/2021 and laws and legislation complementary to penalties, as well as the protection approved by the country's constitution rights and freedoms by stipulating them and giving them constitutional protection in articles 25-44, The study discussed personal data related to a specific person and related to communication with modern technology as a prerequisite for the determination of legal protection of a penal nature in accordance with the laws and legislation of the United Arab Emirates, the researcher has used the descriptive analytical comparative approach to report legal protection in the laws and legislation of the United Arab Emirates, in addition to comparative legislation represented in the provisions of Egyptian law, and we reached in this regard a number of conclusions and recommendations essential, the most important of which is that until the present time no executive regulation has been organized for the law Federal Personal Data Protection This is why we recommend expediting the issuance of this regulation.

Keywords: personal data – penal protection – information privacy – processed data – digital society.

مُقَدِّمَةٌ

أثر التطور التقني والرقمي والمعلوماتي في العالم على المجتمعات والأفراد والمؤسسات والهيكل الاقتصادي والتجارية والاجتماعية والسياسية، وقد أدى ذلك إلى ربط العلاقات بين الدول والعلاقات بين الشركات والأعمال والأفراد في جميع أنحاء العالم، وأصبح لا يمكن الاستغناء عن شبكة الإنترنت، إلا أنه على الرغم من إيجابيات التكنولوجيا الرقمية فإن لها العديد من السلبيات التي أثرت على حياة الأفراد بصفة خاصة وعلى المجتمع بصفة عامة، وأثرت سلباً على العلاقات الدولية والأعمال وخاصة عند استعمال التكنولوجيا الرقمية والشبكات بطريقة غير مشروعة، مما جعل ذلك من الساحة الرقمية الافتراضية ساحةً للمساس بالحقوق والحريات المقررة للأفراد، ومن هنا تبدو مخاطر التهديد للحياة الخاصة للأفراد والتي تمس الحريات العامة^(١).

وقد أدرك المشرع الاتحادي تلك الانتهاكات في البيئة الرقمية، ووضع القوانين التي تمنح للأفراد حقوقاً ليس للغير المساس بها، ومنها حماية المعطيات الشخصية للأفراد في البيئة الرقمية، وذلك بالمرسوم بقانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية، وكانت أبرز التشريعات التي استحدثتها وعدلتها دولة الإمارات العربية المتحدة مرسوم بقانون اتحادي رقم (٤٦) لسنة ٢٠٢١ بشأن المعاملات الإلكترونية وخدمات الثقة، وقانون حماية البيانات الشخصية رقم (٤٥) لعام ٢٠٢١، والقانون الاتحادي رقم (٣٨) لسنة ٢٠٢١ بشأن حقوق المؤلف والحقوق المجاورة، هذا بالإضافة إلى القانون الاتحادي رقم (١٥) لسنة ١٩٨٠ بشأن المطبوعات والنشر لتراخيص وأنشطة الطباعة والنشر في دولة الإمارات، فعمل بذلك المشرع على تجريم انتهاك خصوصية البيانات الشخصية، ووضع ضوابط عدة لأجل حماية هذه الخصوصية.

(١) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، بحثٌ مُقدّم في المؤتمر العلمي الدولي "الرقمنة والقانون - تطلعات المستقبل في الدول العربية" المنعقد يومي الجمعة والسبت ١٥ و١٦ يوليو ٢٠٢٢ بمدراج المختار السوسي، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش.

أهمية الدراسة:

تبرز أهمية الدراسة في كيفية توضيح ما توصل إليه المشرع الاتحادي لحماية البيانات الشخصية وخصوصية الإنسان؛ نتيجة زيادة التعدي في الحياة الخاصة للأفراد مع التطور التكنولوجي من الناحية الكمية والكيفية، ورافق التدخل ظهور المعلوماتية بأدواتها المتمثلة في جهاز الحاسوب والشبكات العالمية والمحلية للمعلومات، إضافة إلى الأهمية التالية:

1. تهديد حق الأفراد في احترام حياتهم الخاصة، وذلك بالقدرة الفائقة للمعلومات والبيانات الاسمية واسترجاعها وتصنيفها وتحليلها ومعالجتها، ومن ثم تبادلها دون أي عوائق بين الجهات المختلفة.
2. أثرت تقنية المعلومات على خصوصية الإنسان وحقوقه على نحو أظهر إمكان المساس به، بل أظهر الواقع العملي وجوب التدخل التشريعي لتنظيم أنشطة معالجة البيانات المتصلة بالشخص وتنظيم عمليات تخزينها في بنوك وقواعد المعلومات وعمليات تبادلها.
3. رغم اعتراف الدساتير والمواثيق الدولية بحق الفرد في خصوصية معلوماته وبياناته الشخصية لانتوائها على مبدأ السرية والعزلة، الناطوء، الخلوة، فإن التطور التكنولوجي والعلمي أعطى الآخرين حق الاطلاع على المعلومات والبيانات الشخصية التي تكون تحت يد الغير من البشر.

إشكالية الدراسة:

رغم حرص دولة الإمارات العربية المتحدة من خلال تشريعاتها وقوانينها على كفالة الخصوصية باعتباره حقاً مستقلاً قائماً بذاته، فلم تكتف بسن القوانين لحمايته، بل تسعى إلى ترسيخه في الأذهان؛ وذلك بغرس القيم النبيلة التي تلعب دوراً كبيراً وفعالاً في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم وخاصة في عصر التحول الرقمي، فإن وجود الأفراد في بيئة رقمية تتداول فيها المعلومات الشخصية على شبكة الانترنت، يشكل خطورة على حياة الفرد الخاصة أو خصوصيته، فبيانات الأفراد تتحرك وتُخزن وتُحول إلى مادة أولية تُستعمل لعدة أغراض، مما يؤدي إلى إبراز مخاطر التقنية وتهديدها للحياة الخاصة، وي طرح الإشكالية في السؤال الرئيس التالي: ما مدى الكفاية التنظيمية التي تناولها المشرع الإماراتي بصدد توفير الحماية الجزائية الموضوعية اللازمة لحماية خصوصية البيانات الشخصية، وعلى ضوء هذا التساؤل الأساس، نتناول عدداً من التساؤلات الفرعية، نعرض لها على النحو الآتي:

١. ما مفهوم الحماية الجنائية لحق الإنسان في خصوصية بياناته الشخصية؟
٢. ماهية الحق في الخصوصية في التشريعات الاتحادية؟
٣. ما علاقة الخصوصية المعلوماتية والحاسب الآلي والإنترنت بالبيانات الشخصية؟
٤. كيف يتم تحديد الأساس القانوني لمعالجة البيانات الشخصية في تشريعات دولة الإمارات العربية المتحدة؟

أهداف الدراسة:

يكن الهدف الرئيس للدراسة في توضيح مدى توفيق المشرع الاتحادي في سن القوانين والتشريعات التي توضح نطاق الحماية الجنائية في خصوصية البيانات الشخصية، إضافة إلى الأهداف الفرعية التالية:

١. التعرف على مفهوم الحماية الجنائية لحق الإنسان في خصوصية بياناته الشخصية والعديد من الحقوق التي كفلها القانون والدستور للحفاظ على الإنسان ضد تعسف السلطات العامة، كالحقوق العامة أو المطلقة أو الخاصة أو الأسرية أو الشخصية أو العينية أو المالية أو المعنوية.
٢. توضيح الحق في الخصوصية في التشريعات الاتحادية وحق كل فرد في مفهوم الحياة الخاصة أن يتمتع باحترام خصوصية حياته الشخصية والعائلية من بياناته الخاصة ومعلوماته التي يحفظها بهاتفه المحمول أو التي يستخدمها في شبكات التواصل الاجتماعي أو بالإنترنت.
٣. بيان علاقة الخصوصية المعلوماتية والحاسب الآلي والإنترنت بالبيانات الشخصية؛ لارتباط حياة أفراد المجتمع في العصر الحالي بصورة وثيقة بالتعامل مع أجهزة الحاسب الآلي والإنترنت.
٤. تحديد الأساس القانوني لمعالجة البيانات الشخصية في تشريعات دولة الإمارات العربية المتحدة وضوابط نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة وإجراءات الإبلاغ عن انتهاك البيانات الشخصية.
٥. تناول صور الحماية الجزائية التي أقرها المشرع لأجل حماية خصوصية البيانات الشخصية.

منهجية الدراسة:

اعتمد الباحث على استخدام المنهج الوصفي التحليلي المقارن؛ وذلك لتوضيح مدى توفيق المشرع الاتحادي في سن القوانين والتشريعات التي توضح مفهوم الحماية القانونية لحق الإنسان في خصوصية بياناته الشخصية؛ هل حقق المشرع الاتحادي التوازن بين المصلحة العامة التي تقرر أنه لا بد من تجميع وتخزين ومعالجة البيانات الخاصة للأفراد وبين ضرورة حماية البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها، هذا بالإضافة إلى أعمال جوهر الدراسة المقارنة بين موقف المشرع الإماراتي وما عليه الحال بصدد موقف المشرع المصري.

خطة الدراسة:

المبحث الأول: خصوصية البيانات الشخصية والمبادئ التي تحكمها

المطلب الأول: ماهية خصوصية البيانات الشخصية وتطورها.

المطلب الثاني: المبادئ الأساسية لحماية البيانات الشخصية.

المبحث الثاني: الحقوق والتزامات المتصلة بالبيانات

المطلب الأول: حقوق الشخص صاحب البيانات الخاضعة للمعالجة.

المطلب الثاني: التزامات المسؤول عن معالجة البيانات الشخصية.

المبحث الثالث: صور الحماية الجنائية الموضوعية لخصوصية البيانات الشخصية

المطلب الأول: جريمة التعدي على البيانات الشخصية.

الفرع الأول: أركان الجريمة.

الفرع الثاني: العقوبات المقررة للجريمة.

المطلب الثاني: جريمة التعدي على البيانات الشخصية الطبية والمصرفية

الفرع الأول: أركان الجريمة.

الفرع الثاني: العقوبات المقررة للجريمة.

المبحث الأول

ماهية خصوصية البيانات الشخصية والمبادئ الأساسية لحمايتها

تمهيدٌ وتقسيمٌ:

إنَّ حقَّ كلِّ فردٍ أنْ يتمتَّعَ باحترام خصوصية حياته الشخصية والعائلية من بياناته الخاصة ومعلوماته التي يحفظها بهاتفه المحمول أو التي يستخدمها في شبكات التواصل الاجتماعي أو بالإنترنت، مثل لقبه وعمره وعنوانه أو رقم هاتفه أو معلومات عن حياته المرضية الشخصية أو التأمين الصحي أو أيِّ معلومات إضافية خاصة لا يرغب أن يعلنها للآخرين، وذلك في مفهوم الحياة الخاصة، هذه المعلومات التي تعدُّ معلومات شخصية خاصة بالإنسان والتي يتعرَّضُ بانتهاكها من خلال الانتهاك المعلوماتي والجرائم المعلوماتية في شبكة الإنترنت^(٢).

وقد قطعت دولة الإمارات العربية المتحدة العهد على نفسها؛ بأن لا تنمية بدون تنمية الإنسان أولاً، ومن هنا كان مسعاها نحو العمل بكلِّ جهدٍ وإخلاصٍ من أجل كفالة حقوق الإنسان وصيانة حرّيته ورفاهيته وتوفير كلِّ السبل الممكنة للنهوض بقدراته نحو الأفضل، وهيأت كلَّ المستلزمات التي تمكّن من أن يكون هذا الإنسان في مقمّة خططها الآنية والمستقبلية، وسنت لهذا الغرض العديد من القوانين الدستورية والقوانين ذات الاختصاص^(٣). وعلى المستوى الدولي تمّ تكريس مفهوم البيانات الشخصية وضرورة حمايتها بالقانون الفرنسي^(٤)، والمادة (٢) من التوجيه الأوروبي رقم ٤٦ / ٩٥^(٥)، فالبيانات الشخصية هي البيانات التي تسمح بأيِّ شكلٍ كان، وبطريقة مباشرة أو غير مباشرة، بتحديد شخص

(٢) حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت - دراسة مقارنة، ط١، القاهرة، دار النهضة العربية، ٢٠٠٩، ص ٤٤-٤٥.

(٣) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق، ص ٩.

(٤) المادة (١) من القانون الفرنسي لسنة ١٩٧٨، حيث نصّ على أن المعلوماتية لا يجب أن تمسّ هوية الشخص ولا حقوق الإنسان ولا حياته الخاصة ولا حرّياته الفردية أو العامة.

(٥) التوجيه الأوروبي رقم ٤٦ / ٩٥ الصادر بتاريخ ٢٤ تشرين الأول ١٩٩٥ الخاص بحماية الأشخاص الطبيعيين تجاه معالجة البيانات الشخصية والانتشار الحرّ لهذه البيانات.

طبيعيّ، وسواء تمّت معالجة هذه البيانات من قبل شخصٍ طبيعيّ أو من قبل شخصٍ حكيمٍ^(٦). من أجل ذلك الهدف، نوضّح ما سبق في المطلبين التاليين:

المطلب الأول: ماهية خصوصية المعلومات والبيانات الشخصية وتطورها.

المطلب الثاني: المبادئ الأساسية لحماية البيانات الشخصية.

المطلب الأول

ماهية خصوصية المعلومات والبيانات الشخصية وتطورها

جاءت الآلية التشريعية في دولة الإمارات العربية المتحدة بتنظيم قانونٍ خاصٍ لحماية البيانات الشخصية؛ بهدف المحافظة على الحريات والحياة الخاصة للأفراد والبيانات الشخصية التي أصبحت تُداول في العالم الافتراضي والمهددة بالمخاطر التي تُهدد حياة الأشخاص الخاصة؛ إذ لا تخضع البيانات الشخصية للحماية بدون اقترانها بالخصوصية^(٧)، فالخصوصية هي سببُ تقرير الحماية للبيانات، وبذلك يوجد ارتباط وثيق بين مفهومي الخصوصية وحماية البيانات الشخصية؛ إذ تنبثق البيانات الشخصية من الخصوصية، فالخصوصية من الحقوق الدستورية الأساسية الملزمة للشخص الطبيعي بصفته الإنسانية كأصلٍ عامٍّ، فهي أساسُ بنيان كلِّ مجتمعٍ سليمٍ؛ لذا حرصت الدولة على كفالة الحقِّ وعدته حقاً مستقلاً قائماً بذاته^(٨).

فالدولة تحفظ أمن مواطنيها بمواجهة الجرائم المرتبطة بالتكنولوجيا المعلوماتية والاتصالات الرقمية والمخالفات التي تمسُّ البيانات الشخصية والحياة الخاصة، وتعمل على تأمين أمن البنى التحتية واقتصادها

(٦) المادة (٢) من القانون الفرنسي لسنة ١٩٧٨.

(٧) منى كامل تركي: جرائم انتهاك الخصوصية عبر وسائل التواصل الاجتماعي في التشريعات الاتحادية لدولة الإمارات العربية المتحدة - المؤتمر العلمي الدولي الثالث للإعلام عبر الوسائط الإلكترونية - الحق في الخصوصية ومواقع شبكات التواصل الاجتماعي، ص ١٢-١٣.

(٨) فطيمة نساخ: حماية المعطيات ذات الطابع الشخصي في ظلّ العصر التكنولوجي والرقميّ وفق قانون ٢٠٠٧/١٨ الجزائري، مجلة الاقتصاد والصحافة، المجلد (٨)، العدد ٢، ص ٥١-٦٨.

ومُكافحة التّهديدات عبر اعتماد سياسات المراقبة الأمنية للتكنولوجيا وعدم المخاطرة ببعض حقوق المواطنين وحرّياتهم الأساسية، وأهمها الحق في حماية الحياة الخاصة^(٩)، ونوضّح ذلك كما يلي:

أولاً: تعريفُ البيانات الشخصية:

نظّم القانونُ حماية الخصوصية كجزء من المنظومة التشريعية في الدولة، مثل القانون الاتحادي رقم ٤٥ لسنة ٢٠٢١ بشأن حماية البيانات الشخصية، والقانون الاتحادي رقم ٤٤ بشأن إنشاء مكتب الإمارات للبيانات، والقانون الاتحادي رقم ١٥ لسنة ٢٠٢٠ بشأن حماية المستهلك، بما في ذلك خصوصية وأمن بيانات المستهلك، ومنع استخدامها لأغراض الترويج والتسويق، وتجاوز بيع بعض الشركات العملاقة لبيانات وأرقام المتعاملين لشركة الإعلانات الهاتفية^(١٠). وعُرفت البيانات الشخصية بأنها البيانات أو المعلومات التي تتعلّق بشخص طبيعيّ أو شخص اعتباريٍّ محدّد معروفٍ أو قابلٍ للتعريف عن طريق تلك البيانات، وعُرفت بأنها البيانات التي تُستخدم لتمييز الشخص عن غيره وتحديد هويته سواء كانت تلك البيانات دقيقةً أم غير دقيقة، فهي في حدّ ذاتها بياناتٌ تحتاجُ إلى معلوماتٍ إضافيةٍ للتوضيح سواء كانت في شكلٍ ماديٍّ أم إلكترونيٍّ، وكل بيان أو معلومة يُعبّر عن الحالة العقلية الصحية والثقافية الاجتماعية أو المهنية^(١١).

(٩) ثاني بن علي آل ثاني: الرقمنة وقانون حماية المعطيات ذات الطابع الشخصي، بحثٌ مقدّم في المؤتمر العلمي الدولي "الرقمنة والقانون - تطّعات المستقبل في الدول العربية" المنعقد يومي الجمعة والسبت ١٥ و ١٦ يوليو ٢٠٢٢ بمدرّج المختار السوسي، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش.

(١٠) نصّ القانون الاتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية الصادر بتعديل المرسوم بقانون اتحادي رقم ١٢ لسنة ٢٠١٦ والصادر بتعديل المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، والمعدل على القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات، وحظر في المادة ٢١ من القانون على كلّ من استخدم شبكة معلوماتية، أو نظاماً معلوماتياً إلكترونياً، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرّح بها قانوناً، بإحدى الطرق التالية: كالتقاط صور الغير، أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها.

(١١) سينثيا شاسينيو: الإطار القانوني لمعالجة البيانات الشخصية على مواقع التجارة الإلكترونية، باريس، ٢٠٠١، ص

وعُرِّفَت البيانات الشخصية بأنها كلُّ ما يرتبطُ بالشخص ومُعاملاته وآرائه أو آراء الغير فيه، وبذلك تعدُّ البيانات الشخصية: كلُّ معلومةٍ تتعلّقُ بشخصٍ طبيعيٍّ مُعيّنٍ أو يمكنُ تعيينه بطريقةٍ مباشرةٍ أو غير مباشرةٍ، بالرجوع إلى عناصرٍ تتعلّقُ بهويّته، باستثناء المعلومات المتّصلة بالحياة العامّة^(١٢).

ثانياً: تعريفُ الخصوصية المعلوماتية:

ارتبطت حياةُ أفراد المجتمع بصورةٍ وثيقةٍ بالتعامل مع العالم الرقمي وأجهزة الحاسب الآليّ والإنترنت، ونشرُ وتداولُ معلوماتٍ شخصيةٍ مهمّةٍ ومرورها عبر عدّة شبكاتٍ؛ لاحتمال وقوعها في أيدي أشخاصٍ آخرين، سواءً كان ذلك بعلم الأفراد أو بدون علمهم، ممّا يُشكّل انتهاكاً للخصوصية، ويترتّبُ على كون الحقّ بالحياة الخاصة من الحقوق الشخصية استثناءً صاحب الحقّ وحده بأسراره، التي لا يحقُّ لأحدٍ الاطّلاع عليها، ولا يستطيع صاحب السرِّ أن يتنازل عن سرِّ محدّد، ممّا يُزيلُ عنه الخصوصية^(١٣)، فالحياة الخاصة هي أفعالُ وآراءُ الفرد بحريّة، ولا ترتبطُ بأيّ التزامٍ تجاه الآخرين باعتبار أن الحرية شرطٌ للحياة الفردية الخاصة^(١٤).

ثالثاً: تطوّر مفهوم المُعطيات ذات الطابع الشخصي:

انتقل التطوّر من العالم الماديّ إلى العالم الرقميّ، وأصبح الأفراد أمام أخطارٍ جديدةٍ نتيجة دخول التقنيّات في حياة الشخص الذي أصبح بنفسه يُعرّض نفسه للأخطار؛ وذلك باستعماله مثلاً المواقع الإلكترونيّة والاجتماعيّة ومواقع البحث، فالدخولُ في هذه المواقع يستدعي إدخال البيانات أو المُعطيات

(١٢) منى كامل تركي: الذكاء الاصطناعي والأنظمة الرقمية، دورها في العمل الأمنيّ والعلاقات التعاقدية الدولية - دراسة تحليلية في تشريعات دولة الإمارات العربية المتّحدة والقوانين المقارنة، دبي، الدولية للكتب القانونيّة والنشر والتوزيع، ط١، ٢٠٢٢، ص ٩٨-٩٩.

(١٣) أحمد فتحي سرور: الحقّ في الحياة الخاصة، بحثٌ مقدّمٌ لمؤتمر "الحق في الحياة الخاصة" بكلية الحقوق، جامعة الإسكندرية، سنة ١٩٨٧م، ص ٩٣؛ منى كامل تركي: رقمنة الهوية الوطنيّة بين حماية المُعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق، ص ١٦.

(١٤) ممدوح خليل البحر: حماية الحياة الخاصة في القانون الجنائيّ - دراسة مقارنة، ط١، القاهرة، دار النهضة العربيّة، سنة ١٩٨٣م، ص ١٩٠؛ روسكو باوند، ضمانات الحرية في الدستور الأمريكيّ، ترجمة: د/ لبيب شنب، ط١، الإسكندرية، منشأة المعارف، ١٩٧٣م، ص ١.

الشخصية، ويتم تخزين المعطيات والبيانات في المواقع، وقد تستعمل من هذه المواقع بطريقة تشكل تهديداً على الشخص المعني، من هنا ومع أنظمة الحاسوب والحواسب الكبيرة الفائقة السرعة التي يمكنها حفظ كمية هائلة من البيانات وتداولها بسرعة، ليس فقط ضمن إطار دولة واحدة؛ إنما على مستوى دول العالم قاطبة، بما في ذلك البيانات الخاصة بالأفراد؛ فقد أدى التطور التقني إلى تطور التشريعات والقوانين^(١٥).

إذ لم يكن مفهوم البيانات الشخصية بعيداً عن التطور التكنولوجي الذي احتوى على التقنيات التي تحمل البيانات والمعلومات الشخصية إلى العالم الافتراضي اللامادي، فتصبح في متناول الغير على المستوى العالمي، مما قد تشكل تهديداً خطيراً على المعطيات الشخصية للشخص، فالزيادة المطردة في استخدام الإنترنت ووسائل التواصل المتطورة أنشأت الخطر الذي يهدد بيانات الأفراد الشخصية من حيث الحصول عليها وتداولها ومعالجتها^(١٦).

وتعد حماية البيانات الشخصية حقاً أساساً لكل إنسان؛ ولذلك تم تفعيل اللائحة العامة لحماية البيانات (GDPR) كإطار جديد لحماية هذا الحق، ففي الاتحاد الأوروبي تمكن اللائحة الأوربينية من استعادة السيطرة على معلوماتهم الشخصية داخل وخارج نطاق الإنترنت، ويترتب على ذلك أن المصلحة العامة هي التي ترسم حدود هذا الحق وتحدد نطاقه وفقاً لمبدأ المشروعية، وذلك عن طريق الموازنة بين مصلحة الفرد في الحق في الخصوصية، وبين حاجة المجتمع للأمن والنظام والإعلام، وقد أولت كافة التشريعات أهمية خاصة لحرمة الحياة الخاصة، وهذا ما دفع البشرية إلى البحث عن ضوابط لضمان الحقوق والواجبات والتأكيد عليها، ومنها إعلان دستور حقوق الإنسان بالحق في احترام الحياة الخاصة

(١٥) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق، ص ١٧.

(١٦) طارق جمعة السيد راشد: الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي - دراسة مقارنة، مجلة القانون والاقتصاد - ملحق خاص العدد (الثاني والتسعون)، ص ١٩٠ - ٣١٤.

باعتباره من حقوق الإنسان، بالمادة (١٢/ الإعلان العالمي)، والمادة (١٧/ العهد الدولي للحقوق المدنية)^(١٧).

فقد تخرج البيانات الشخصية التي تخضع في الأصل للحماية من هذا النطاق؛ لاعتبارات المصلحة العامة ولاعتبارات العدالة والكشف عن الجرائم والمخالفات، فالمساس بالبيانات الشخصية أو إفشاؤها يُعدُّ مبرراً إذا كان الهدف من ذلك الكشف عن جريمة أو مخالفة ما، أو إذا كان لغايات علمية أو صحفية في بعض الحالات، فإن البيانات الشخصية الخاضعة للحماية هي تلك البيانات التي تمت معالجتها، وأي بيانات لم يتم معالجتها لا تخضع للحماية، لذلك يجب أن تكون المعلومات قد تم جمعها، وحفظها، ونقلها للغير أو التّجار بها^(١٨).

وقد أدّى تقدّم التكنولوجيا الرقمية إلى العديد من الفوائد التي تُعزّز حقوق الإنسان والتنمية؛ إذ تُمكن من التواصل والترابط مع المجتمعات في جميع أنحاء العالم، كما تعمل على التعبئة والإعلام والتحقيق واستخدام الاتّصالات المشفّرة واستخدام صور الأقمار الصناعية في تدفق البيانات؛ من أجل الدفاع مباشرة عن حقوق الإنسان وتعزيزها^(١٩)، إلا أن الاعتماد على استخدام التكنولوجيا الرقمية أو الذكاء الاصطناعي في جميع الأعمال قد يوقع انتهاكات على الإنسان لما يمكنه حدوثه من إساءة الاستخدام الرقمي لتطبيقات الذكاء الاصطناعي في سرقة معلوماته الشخصية من الهوية الوطنية أو أرقام الحسابات البنكية أو صورهِ

(١٧) الإعلان العالمي لحقوق الإنسان الصادر في ١٠/ ١٢/ ١٩٤٨ من الجمعية العامة للأمم المتحدة، وتتابع بعد ذلك الاتفاقيات الدولية، وفي مقدمتها الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية الموقعة في روما في ٤ تشرين الثاني/ نوفمبر ١٩٥٠، والعهد الدولي الخاص بحقوق الإنسان المدنية والسياسية الصادرة عن الأمم المتحدة، والتي نصّت فيها المادة (١٧) على أنه (لا يجوز التدخل بشكل تعسفي أو غير قانوني بخصوصيات أحد).

(١٨) علاء الدين عبد الله الخصاصونة، فراس الكساسبة، لافي محمد درادكة: الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد رقم (٨)، العدد (٢)، جمادى الآخرة ١٤٣٢هـ/ يونيو ٢٠١١م، ص ١٧٥-٢٢٦.

(١٩) كيث غولدستين، أوهاد شيم توف، والسيد دان برازيريس: الحق في الخصوصية في العصر الرقمي، تقرير المفوض السامي لحقوق الإنسان، ٩ أبريل ٢٠١٨.

الشخصية أو أي من البيانات الشخصية الخاصة التي يُمثل التعدي عليها انتهاكاً لحقوق الإنسان^(٢٠)، إضافةً إلى الإساءات والانتهاكات التي تحدث في وسائل التواصل الاجتماعي بأنواعها المختلفة من ابتزاز وتهديد بالصور وغير ذلك من أوجه الاستغلال والمتاجرة في بيع البيانات الشخصية^(٢١).

ومن هنا اتجه المشرع الاتحادي إلى تعديل وسن التشريعات لتحقيق الأمن القانوني وتنظيم البيانات الشخصية بمقتضى تشريع خاص جسد في مضمونه المبادئ الأساسية لحماية البيانات الشخصية، وجمع المعلومات، وهدف القانون من معالجة البيانات الشخصية مع حماية حق الفرد في الموافقة على المعالجة، وحقه في الاطلاع على البيانات الشخصية، وحقه في طلب تصحيح البيانات الشخصية، إلى جانب ذلك وضع المشرع هيئة متخصصة لمعالجة البيانات الشخصية والمعطيات ذات الطابع الشخصي وفقاً لأحكام القانون^(٢٢).

المطلب الثاني

المبادئ الأساسية لحماية البيانات الشخصية

حدّد المشرع في مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية ضوابط معالجة البيانات الشخصية والتزامات العامة للشركات التي تتوافر لديها بيانات شخصية عن الأفراد والعاملة في مجال معالجة البيانات الشخصية في تأمين البيانات والحفاظ على سريتها وخصوصيتها والإجراءات والتدابير المتوافرة لديها؛ لضمان عدم اختراقها أو إتلافها أو تغييرها أو العبث بها وضوابط نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة وإجراءات الإبلاغ عن انتهاك البيانات

(٢٠) علاء الدين عبد الله الخصاونة، فراس الكساسبة، لافي محمد درادكة: الحماية القانونية للخصوصية والبيانات

الشخصية في نطاق المعلوماتية، مرجع سابق، ص ١٧٥-٢٢٦.

(٢١) فطيمة نساخ: حماية المعطيات ذات الطابع الشخصي في ظلّ العصر التكنولوجي والرقمي، مرجع سابق، ص

٥١-٦٨.

(٢٢) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق،

ص ١٨.

الشخصية^(٢٣)، كما منح القانون لصاحب البيانات الشخصية عدة حقوق تشمل الحصول دون أي مقابل على المعلومات والقرارات التي تتخذ بناءً على معالجة بياناته الشخصية والحق في طلب تصحيح بياناته الشخصية الخاطئة أو القديمة وحق النسيان الذي يُوفّر للفرد الحق بأن يطلب من أي شركة يطبق عليها القانون بأن تحذف بياناته بشكل كلي، وحق الإعلام الذي يوفّر للمستهلك الحق بأن يتم إعلامه في حال تم اختراق نظام شركة مطبق عليها القانون، حيث يتم إعلامه أن بياناته قد انتهكت^(٢٤). ونوضح ذلك كما يلي:

أولاً: موافقة الفرد المسبقة على معالجة البيانات الشخصية:

ربط المشرع الاتحادي معالجة المعطيات ذات الطابع الشخصي بشرط الموافقة الصريحة للشخص، وأعطى له حق الرجوع عن موافقه في أي وقت، فلم يجعل المشرع الموافقة واجبةً في حالة إذا كانت المعالجة ضروريةً، ومنها احترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة لحماية حياة شخص المعني لتنفيذ عقد يكون الشخص المعني طرفاً فيه أو لتنفيذ إجراءات سابقة للعقد اتخذت على طلبه للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادرٍ على التعبير عن رضاه لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية يتولاها المسؤول عن المعالجة أو الغير الذي يتم إطلاعُه على المعطيات؛ وذلك لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه، مع مراعاة مصلحة الشخص المعني وحقوقه وحرياته الأساسية^(٢٥).

وطرح قانون حماية البيانات الشخصية مبدأ الموافقة باعتباره الأساس القانوني الرئيس الواجب استخدامه، وتكون الموافقة خياراً من بين عدة خيارات أخرى كقواعد لمعالجة البيانات الشخصية، ووضع

(٢٣) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية دخل حيز التنفيذ بتاريخ ٢ يناير ٢٠٢٢. وأوجب على مراقبي البيانات ومعالجي البيانات توفيقاً لأحكام القانون خلال ستة أشهر من تاريخ إصدار لائحته التنفيذية.

(٢٤) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق، ص ١٨.

(٢٥) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

قواعد قانونية لمعالجة البيانات الشخصية تعتمد على الغرض من المعالجة، فالموافقة هي إحدى الأسس القانونية للمعالجة، وحظر القانون معالجة البيانات الشخصية من دون موافقة الفرد ما لم ينطبق أحد الاستثناءات، إضافة إلى ذلك بينما تتضمن بدائل الموافقة قواعد معينة مثل تنفيذ عقد وأداء التزام قانوني لا ينص قانون حماية البيانات الشخصية على مبدأ "المصلحة المشروعة" كأساس قانوني لمعالجة البيانات الشخصية.

على سبيل المثال، تنص اللائحة العامة لحماية البيانات على إمكانية معالجة البيانات الشخصية عند الضرورة بناءً على المصالح المشروعة للجهة المتحكمة بالبيانات، أو مصالح صاحب البيانات، أو مصالح الأطراف الثالثة. وقد تكون هذه المصالح تجارية أو فردية أو فوائد مجتمعية، وقد يؤدي عدم وجود مبدأ المصلحة المشروعة في القانون إلى جعل الامتثال أكثر تعقيداً لعدد من هيئات القطاع الخاص التي تلجأ إلى المصلحة المشروعة كفتة شاملة^(٢٦).

ثانياً: الإجراءات المسبقة عن المعالجة:

قررت المادة (٢/ قانون حماية البيانات الشخصية) الخاص بدولة الإمارات العربية المتحدة، أنه يمكن أن يسري على المتحكمين بالبيانات أو معالجي البيانات المتواجدين خارج الدولة إذا قاموا بمعالجة البيانات الشخصية لأشخاص موجودين في الإمارات العربية المتحدة. في الواقع، تسري أحكام حماية البيانات، بموجب قانون حماية البيانات الشخصية على كل صاحب بيانات يُقيم في الإمارات العربية المتحدة أو له مقر عمل فيها وكل متحكم أو معالج متواجد في الدولة، بصرف النظر عما إذا كانت معالجة البيانات الشخصية تتم داخل دولة الإمارات العربية المتحدة أو خارجها؛ أو كل متحكم أو معالج متواجد خارج الدولة ويقوم بمزاولة أنشطة معالجة البيانات الشخصية لأصحاب البيانات في الدولة^(٢٧).

(٢٦) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

(٢٧) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

المبحث الثاني

حقوق الشخص صاحب البيانات والتزامات المسؤول عن معالجتها

تمهيد وتقسيم:

تتمثل الخصوصية في قدرة الشخص على منع المعلومات المتعلقة به من أن تصبح معروفةً للآخرين، إذا لم يختَر برغبته أن يقدم المعلومات والبيانات الشخصية في المواقع الإلكترونية أو التطبيقات الإلكترونية للهاتف والتي يقوم بالدخول فيها وتسجيل بياناته الخاصة من الاسم ورقم الهاتف واليـمـيل وغيرها^(٢٨)، ووفقاً للمادة (٢/ حماية البيانات) يسري على المتحكمين بالبيانات أو معالجي البيانات المتواجدين خارج الدولة إذا قاموا بمعالجة البيانات الشخصية لأشخاص موجودين في دولة الإمارات العربية المتحدة، كما تسري أحكام حماية البيانات على كل صاحب بيانات يُقيم بالدولة أو له مقر عمل فيها، وكل متحكم أو معالج متواجد في الدولة بصرف النظر عما إذا كانت معالجة البيانات الشخصية تتم داخل دولة الإمارات العربية المتحدة أو خارجها؛ أو كل متحكم أو معالج متواجد خارج الدولة ويقوم بمزاولة أنشطة معالجة البيانات الشخصية لأصحاب البيانات في الدولة^(٢٩). ونوضح ذلك كما يلي:

المطلب الأول: حقوق الشخص صاحب البيانات والمعلومات الخاضعة للمعالجة.

المطلب الثاني: التزامات المسؤول عن معالجة البيانات الشخصية.

المطلب الأول

حقوق الشخص صاحب البيانات الخاضعة للمعالجة

شكل وجود الأفراد في البيئة الرقمية لتداول المعلومات الشخصية على شبكة الإنترنت من خلال مواقع الشبكة سواء للدخول للتصفح أو الاشتراك في المواقع للحصول على المعلومات التي يبحث عنها أو موافقته على تنزيل البرامج التي يرغب في الالتحاق بها بوضع معلوماته وبياناته الخاصة للحصول على الخدمات المطلوبة خطورة على حياته الخاصة؛ أي خصوصيته، فبيانات الأفراد تتحرك وتخزن

(٢٨) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق،

ص ١٩.

(٢٩) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

وتُحوّل إلى مادةٍ أوليّةٍ تُستعمل لعدة أغراضٍ، ممّا يؤديّ إلى مخاطر التقنيّة وتهديدها للحياة الخاصّة^(٣٠)، ونوضّح ذلك كما يلي:

أولاً: الحقوق المتعلّقة بالبيانات الشخصية:

وفقاً لأحكام المرسوم بقانون الاتّحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية واللائحة العامّة لحماية البيانات يتمتّع الإنسان بالحقوق التالية فيما يتعلّق ببياناته الشخصية، فقد منح المشرّع الاتّحاديّ بقانون حماية البيانات الشخصية للأفراد حقّ حماية المعطيات الشخصية للأفراد في البيئة الرقمية أو الافتراضية، انسجاماً مع أفضل الممارسات الدوليّة، وينصّ القانون الإماراتي في المواد ١٣ إلى ١٨ على مجموعة واسعة من حقوق أصحاب البيانات الأفراد، بما في ذلك الحقّ في الوصول إلى البيانات الشخصية، والحقّ في الحصول على المعلومات، والحقّ في إمكانية نقل البيانات الشخصية، والحقّ في نقل البيانات الشخصية، والحقّ في التصحيح، وحقّ الإسقاط والحقّ في المحو، والحقّ في تقييد المعالجة، إضافةً إلى حقّ الاعتراض على المعالجة الآليّة وغير الآليّة، فإنّ قانون حماية البيانات الشخصية لا ينصّ على مهلة زمنيّة محدّدة لردّ المتحكّم على طلب الوصول إلى المعلومات من قبل صاحب البيانات^(٣١).

وضع قانون حماية البيانات الشخصية عدداً من الضمانات المتعلّقة بحقوق المستخدم، والتي أسماها القانون الشخص المعنيّ بالبيانات، وتعدّ هذه الضمانات هي القواعد الأساسية التي يجب الالتزام بها أثناء عملية جمع ومعالجة البيانات الشخصية، ورغم أهميّة هذه الضمانات والتي تُعدّ الهدف الأساس لإصدار قانون حماية البيانات الشخصية، فإنها جاءت في صياغاتٍ لتتصرّ على أصل الحقّ دون بيان مفصّل أو تعريفات للمفاهيم الأساسية المتعلّقة به، كما أنّ نصوص القانون وزّعت هذه الضمانات في صورٍ مختلفةٍ بحقوق الشخص المعنيّ بالبيانات وشروط جمع ومعالجة البيانات وصورة شروط وضوابط تتعلّق بعملية جمع البيانات، وهو ما يصعب على المخاطبين بالقانون فهم حقوقهم وإدراكها بشكلٍ مستساغ.

(٣٠) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق،

(٣١) مرسوم القانون الاتّحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

وأكدت اللائحة العامة لحماية البيانات بالمادة (١٥/ القانون العام لحماية البيانات) على أنه يمكن طلب معلومات حول البيانات المخزنة والمعلومات المتعلقة بفئات البيانات التي تُعالجها والأغراض التي تُعالجها من أجلها وأصل البيانات والمستلمين والحق في التصحيح (المادة ١٦ من اللائحة العامة لحماية البيانات)، والحق في الحذف (المادة ١٧ من اللائحة العامة لحماية البيانات)، والحق في تقييد المعالجة (المادة ١٨ من القانون العام لحماية البيانات)، والحق في نقل البيانات (المادة ٢٠ من اللائحة العامة لحماية البيانات)، والحق في الاعتراض (المادة ٢١ من اللائحة العامة لحماية البيانات)، والحق في تقديم شكوى إلى الهيئة المشرفة على حماية البيانات.

نظراً لتطور المجتمع الرقمي وتطور استخدامات الفضاء الافتراضي وتطور وسائل وشبكات الاتصال؛ أصبحت المعلومات والمعطيات تنتقل بصورة سريعة، وأصبح ذلك التطور يشكل خطورة كبيرة على الحياة الخاصة للأفراد وعلى الحقوق المقررة دستورياً للأفراد، وما يشكل حقاً فإنه يشكل من جانب آخر التزاماً على الغير، فقد غزت وسائل وشبكات الاتصال الرقمية وشبكات الإنترنت المؤسسات التجارية والهيكل الاقتصادي ومجالات الأعمال والحكومات والسياسات والبيوت وشبكات التواصل الاجتماعي، وربطت العلاقات فيما بين الدول ببعضها البعض وفيما بين الشركات التجارية والأعمال بمختلف الدول وفيما بين الأفراد، وأصبحت الساحة الرقمية الافتراضية ساحة للمساس بالحقوق والحريات المقررة للأفراد.

ثانياً: المعلومات الواجب إحاطة صاحب البيانات بها:

في الحالات التي يتم فيها الحصول على البيانات من صاحبها مباشرة على مدير البيانات إحاطته عند تسجيل هذه البيانات باسم مدير البيانات كاملاً ومجال نشاطه أو مهنته، بحسب الأحوال وعنوانه والأغراض التي من أجلها يعتزم معالجة البيانات وأية معلومات ضرورية أخرى، بحسب ظروف كل حالة يكون من شأنها أن تكفل جعل المعالجة منصفة بالنسبة لصاحب البيانات، ومن ذلك أسماء مستلمي البيانات أو فئاتهم، وبيان ما إذا كانت الإجابة على أية أسئلة توجه إلى صاحب البيانات إجبارية أو اختيارية، وعند الاقتضاء توضيح العواقب التي تترتب على الامتناع عن الإجابة، وبيان حق صاحب البيانات في أن يتم إخطاره - إذا ما طلب ذلك - بالبيانات الخاصة به كاملة وبحقه في أن يتم تصحيحها،

وبيان ما إذا كان سيتم استخدام البيانات لأغراض التسويق المباشر، وأية معلوماتٍ أخرى تُلزم صاحبَ البيانات لمباشرة حقوقه المقررة بموجب أحكام هذا القانون^(٣٢).

ثالثاً: ممارسة أصحاب البيانات الشخصية للحقوق:

سعى المشرع في المرسوم بقانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية إلى تحقيق حماية المعطيات الشخصية للأشخاص الطبيعيين، وهو من الحقوق التي لها من الحماية الدستورية وفقاً لدستور دولة الإمارات العربية المتحدة، وأن هذه المقومات التي يحميها القانون للفرد في مكوناته الجسدية والنفسية وهويته وتوجهاته الفكرية كمعلوماتٍ ومعطياتٍ شخصية لصيقة بالشخص، ولا يجوز جمعها ولا التشهير بها بدون مبررٍ أو بدون موافقة الشخص الذي تعينه، وحدد القانون الخاص بحماية البيانات الشخصية مبادئ أساسية لحماية المعطيات ذات الطابع الشخصي التي تتمثل في الموافقة المسبقة ونوعية المعطيات وجملة من الإجراءات لا بد من التقيد بها لإجراء عملية معالجة المعطيات ذات الطابع الشخصي^(٣٣).

١. **حق الوصول:** يسمح لمالك البيانات بالحصول على معلوماتٍ حول ما إذا كانت تجميلي تعالج البيانات الشخصية التي تهمة أم لا، وفي هذه الحالة له الحق في الحصول على معلوماتٍ حول البيانات الشخصية الخاضعة للمعالجة.
٢. **حق التصحيح:** يسمح لك بتصحيح الأخطاء وتعديل البيانات التي يتبين أنها غير دقيقة أو غير كاملة.
٣. **حق الحذف:** يسمح بحذف البيانات الشخصية وإيقاف معالجتها بواسطة تجميلي، ما لم يكن هناك التزام قانوني بالاحتفاظ بها و/ أو لا توجد أسباب مشروعة أخرى لمعالجتها بواسطة تجميلي.
٤. **حق التقيد:** يسمح لمالك البيانات الشخصية التي تخضع للمعالجة أن يطلب من تجميلي تطبيق تدابير على هذه البيانات؛ من أجل الحد من معالجة البيانات أثناء التحقق من دقة نفس البيانات أو شرعية

(٣٢) فتحة حزام: الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لتمنراست، المجلد ٨، العدد ٤ لسنة ٢٠١٩، ص ٢٨١-٢٩٩.

(٣٣) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

مُعالجتها، أو لمنع تعديلها، أو عند الاقتضاء، محوها أو حذفها؛ للاحتفاظ بها كدليل أو أساس للمطالبات.

٥. **حق الاعتراض:** في ظروف معينة ولأسباب تتعلق بوضعهم الخاص، يجوز لمالكي البيانات الشخصية الاعتراض على معالجة بياناتهم. ستتوقف تجميلي عن معالجة البيانات، باستثناء الأسباب المشروعة أو ممارسة المطالبات المحتملة أو الدفاع عنها.

٦. **قابلية النقل:** تسمح للطرف المهتم بتلقي بياناته الشخصية و/ أو إمكانية نقل البيانات مباشرة إلى شخص آخر مسؤول بتنسيق منظم، شائع الاستخدام ويمكن قراءته آلياً.

٧. يمكن لأصحاب الحقوق الشخصية ممارسة حقوقه في الوصول أو التعديل أو الحذف أو تقييد المعالجة أو الاعتراض أو قابلية نقل بياناته الشخصية أو إلغاء موافقته^(٣٤).

رابعاً: مدة الاحتفاظ بالمعلومات الشخصية:

يتم حفظ المعلومات الشخصية للمدة الزمنية اللازمة لتحقيق الأغراض الموضحة في إشعار الخصوصية؛ ما لم يكن القانون النافذ يقتضي أو يجيز الاحتفاظ بها لمدة أطول، والبيانات الشخصية التي تتم معالجتها للأغراض التسويقية يتم تخزينها إلى حين يمارس الشخص حقه بسحب موافقته. وبمجرد ممارسته لهذا الحق يتم الاحتفاظ ببياناته الشخصية فقط خلال فترة التقادم النافذة لأي نزاعات أو التزامات قد تنشأ من جراء معالجة تلك المعلومات، وهي مدة أقصاها ١٥ عاماً في دولة الإمارات العربية المتحدة.^(٣٥)

(٣٤) محمد كمال شاهين: الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي - دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، ٢٠١٨، ص ٩١.

(٣٥) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

المطلب الثاني

التزامات المسؤول عن معالجة البيانات الشخصية

ذهب المشرع الإماراتي إلى بلورة تشريعات وسياسات قمعية، من بينها مشاريع قوانين تتعلق بالجرائم الإلكترونية وقوانين مكافحة الإرهاب؛ سعياً إلى تجريم حرية التعبير على الشبكة الإلكترونية وتحويل الإنترنت إلى منصة تخضع للرقابة والمراقبة بهدف المحافظة على الحريات والحياة الخاصة للأفراد، ونوضح ذلك كما يلي:

أولاً: التزام المسؤول بضرورة ضمان سرية المعالجة:

يجب على المسؤول عن المعالجة أن يلتزم بضمان سرية البيانات الشخصية، وكذلك المعالج من الباطن وكافة الأشخاص الذين اطلعوا أثناء ممارستهم لمهامهم على معطيات ذات طابع شخصي، ويستمر ذلك حتى بعد انتهاء مهامهم تحت طائلة العقوبات المنصوص قانوناً بموجب قانون حماية الأشخاص الطبيعيين، وفي مجال معالجة المعطيات ذات الطابع الشخصي أوجب المشرع التقيد بالتراتب المقرر قانوناً لعملية المعالجة والمتمثلة في اتخاذ تدابير لضمان سلامة المعالجة، إذ يلتزم المسؤول عن المعالجة وفق المرسوم بقانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية باتخاذ كل التدابير التقنية والاحترازية اللازمة؛ من أجل حماية وتأمين المعطيات ذات الطابع الشخصي من القرصنة والتلف، وكل استخدام غير مشروع خاصة إذا كانت مرسلّة عبر شبكة معيّنة، وتزيد هذه التدابير كلما زادت قيمة وأهميّة هذه المعطيات^(٣٦).

وإذا كان المسؤول عن المعالجة يستخدم مسؤولاً آخر من الباطن يعمل لحسابه، وجب عليه تقديم الضمانات الكافية من أجل سلامة وتأمين المعطيات ذات الطابع الشخصي، ويجب أن يكون هذا التفويض بعقد أو سند قانوني مكتوب، أو يمكن حفظه لأغراض جمع الأدلة. كما ينص القانون بوجه الخصوص على أن لا يتصرف المعالج من الباطن إلا وفقاً لتوجيهات وتعليمات من المسؤول الأول عن المعالجة، فقد حدد القانون ضوابط معالجة البيانات الشخصية والتزامات العامة للشركات والمؤسسات التي تتوافر لديها بيانات شخصية عن الأفراد بحكم نشاطها والعاملة في معالجة البيانات الشخصية والتزاماتها في

(٣٦) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

تأمين البيانات الشخصية والحفاظ على سريتها وخصوصيتها والإجراءات والتدابير المتوافرة لديها؛ لضمان عدم اختراق البيانات أو إتلافها أو تغييرها أو العبث بها، وإجراءات الإبلاغ عن انتهاك البيانات الشخصية والحالات التي تتطلب تعيين مسؤول حماية البيانات وأدواره^(٣٧).

وكذلك حقوق صاحب البيانات الشخصية في الحصول دون أي مقابل على المعلومات والقرارات التي تتخذ بناءً على معالجة بياناته الشخصية والحالات التي يحق لصاحب البيانات طلب تصحيح بياناته الشخصية غير الدقيقة والحالات التي يحق له تقييد أو إيقاف معالجة بياناته الشخصية، وحدد القانون ضوابط نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة^(٣٨).

ثانياً: التزام المسؤول بحماية المعطيات ذات الطابع الشخصي:

يقع على المسؤول عن المعالجة حماية المعطيات ذات الطابع الشخصي من الإلتاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين؛ وذلك بوضع التدابير التقنية والتنظيمية الملائمة، إذ يقع لزاماً على المسؤول عن المعالجة اختيار معالج من الباطن الذي يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على احترامها، وتقوم المعالجة من الباطن بموجب عقد بين المعالج من الباطن والمسؤول عن المعالجة، وبمقتضى العقد ليس للمعالج من الباطن التصرف إلا بناءً على تعليمات من المسؤول عن المعالجة والأشخاص الذين اطلعوا على المعطيات ذات الطابع الشخصي بالسري المهني، كذلك بعد انتهاء مهامهم ليس لكل شخص يعمل تحت سلطة المسؤول عن المعالجة أو سلطة المعالج من الباطن والذي يستطيع الوصول إلى المعطيات أن يعالج المعطيات دون تعليمات المسؤول عن المعالجة إلا في حالة تنفيذ التزام قانوني^(٣٩).

(٣٧) منى كامل تركي: رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، مرجع سابق، ص ١٨-١٩.

(٣٨) مرسوم القانون الاتحادي رقم ٢٠٢١/٤٥ بشأن حماية البيانات الشخصية.

(٣٩) تومي يحيى: الحماية القانونية للمعطيات ذات الطابع الشخصي - دراسة تحليلية، مجلة الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد ٤، العدد ٢، ٢٠١٩، ص ١٥٥٤-١٥٢١.

ثالثاً: تعزيز حماية البيانات الشخصية وإصدار الإرشادات والتعليمات:

سمح قانون حماية البيانات الشخصية الاتحادي بنقل البيانات الشخصية عبر الحدود بموافقة مكتب البيانات مع استيفاء شروط معينة وفقاً للمادة (٢٢/ حماية البيانات) تتم الموافقة على عمليات النقل الدولية بالدرجة الأولى بناءً على مستوى الحماية المناسب في الدولة المستقبلة أو أي وسيلة أخرى تُبرر النقل وفقاً للمادة (٢٣/ حماية البيانات) (٤٠).

تنص المادة (٢٢/ حماية البيانات) على أن كفاية مستوى الحماية تُحدّد إما من خلال (١) وجود تشريع لحماية البيانات يحتوي على أهم الأحكام المتعلقة بحماية البيانات الشخصية أو (٢) من خلال الاتفاقات الثنائية/ المتعددة الأطراف، وفي حين أن الحالة الثانية واضحة، غير أن معايير تقييم تشريعات حماية البيانات في البلدان الثالثة للموافقة على عمليات النقل الدولية لا تزال غامضة، ولا يزال يتعين وضع قائمة بالشروط الملائمة.

وقد أشار القانون إلى إنشاء مكتب بيانات (منشأ بموجب المرسوم بقانون اتحادي رقم ٤٤/٢٠٢١) ليكون بمثابة هيئة وطنية لحماية البيانات من أجل التعامل مع عمليات خرق البيانات المبلّغ عنها، والشكاوى الواردة من أصحاب البيانات والموافقة على عمليات النقل عبر الحدود، والملاءمة، واقتراح السياسات والاستراتيجيات لتعزيز حماية البيانات الشخصية وإصدار الإرشادات والتعليمات (٤١).

ومنح المشرع بالمادة (٢٧/ حماية البيانات) إمكانية تفويض بعض صلاحيات المكتب إلى سلطات الحكومات المحلية، فالقانون يستثني القطاع العام من نطاق تطبيقه، إلا أن تفويض الرقابة في مجال حماية البيانات ليس بالتأكيد حكماً قانونياً شائعاً على وجه الخصوص؛ لأن ضمان الرقابة المستقلة مسألة أساسية، وقد يفرض المكتب عقوبات إدارية، غير أن القانون لا يُحدّد طبيعتها ولا يُحدّد أي مبالغ؛ إذ إن الأحكام تحتاج إلى التوضيح من خلال اللائحة التنفيذية؛ لذلك قد يصعب إثبات المعاملة بالمثل ومبدأ الملاءمة الثنائية إذا كان القانون الإماراتي نفسه ينص على هذه الاستثناءات العديدة إلى جانب الملاءمة

(٤٠) مرسوم القانون الاتحادي رقم ٤٥/٢٠٢١ بشأن حماية البيانات الشخصية.

(٤١) مرسوم القانون الاتحادي رقم ٤٥/٢٠٢١ بشأن حماية البيانات الشخصية.

يسمح القانونُ بعمليات النقل عبر الحدود لأسبابٍ مُختلفةٍ، مثل الموافقة الصريحة لصاحب البيانات أو المصلحة العامة أو ضرورة تنفيذ التزامٍ تعاقديٍّ مُلزَمٍ بالنسبة إلى صاحب البيانات والمتحكّم بالبيانات^(٤٢).

(٤٢) مرسوم القانون الاتحادي رقم ٤٥/٢٠٢١ بشأن حماية البيانات الشخصية.

المبحث الثالث

صور الحماية الجنائية الموضوعية لخصوصية البيانات الشخصية

تمهيد وتقسيم:

في هذا المقام نتناول الحديث عن صور الحماية الموضوعية التي نظمها المشرع الجزائري لأجل حماية هذه البيانات، وفي هذا النطاق نتناول الحديث عن التعدي على البيانات الشخصية من جانب، ومن جانب آخر نتناول الحديث عن البيانات الشخصية الطبية، وهذا ما نعرض له بصورة مفصلة من خلال تقسيم هذا المبحث إلى مطلبين، وذلك على النحو الآتي:

المطلب الأول: جريمة التعدي على البيانات الشخصية.

المطلب الثاني: جريمة التعدي على البيانات الشخصية الطبية والمصرفية.

المطلب الأول

جريمة التعدي على البيانات الشخصية

في إطار الحديث عن جريمة التعدي على البيانات الشخصية نقسم حديثنا في هذا المقام إلى فرعين، بحيث نتناول في الفرع الأول الحديث عن أركان الجريمة، أما الفرع الثاني فنستعرض الحديث عن العقوبات التي قررها المشرع بصددها، وذلك بصورة مفصلة على النحو الآتي:

الفرع الأول

أركان الجريمة

نتناول في هذا الفرع أركان هذه الجريمة ونعرض لها بصورة مفصلة على النحو الآتي:

أولاً: الركن المادي للجريمة:

يُقصدُ به ماديّات الجريمة؛ أي المظهر الخارجي للجريمة في العالم المحيط، وقد تعارف الفقه على أن الركن المادي يتكوّن من ثلاثة عناصر جوهرية، هي: السلوك الإجرامي، النتيجة الإجرامية، علاقة السببية بينهما، وإزاء ذلك نفصل هذه العناصر بصورة دقيقة في إطار الجريمة الماثلة، وذلك على النحو الآتي:

أ) السلوك الإجرامي:

يعدُّ هذا السلوك^(٤٣) أولَ عناصرِ الركنِ الماديِّ للجرائمِ بصفةٍ عامَّةٍ^(٤٤)، والسلوكُ الماديُّ على ضوءِ ما تقضي به القواعدُ العامَّةُ ينقسمُ إلى صورتين، الصورة الأولى تتمثَّلُ في السلوكِ الإيجابيِّ، أمَّا الصورة الثانية فتتمثَّلُ في السلوكِ السلبيِّ، وفي نطاقِ خصوصيةِ النموذجِ الإجراميِّ المُتقدِّمِ لا بدُّ من بيانِ أنَّ السلوكَ الإجراميَّ في هذه الجريمة هو سلوكٌ إيجابيٌّ لا محالة، وهذا مفاده انتفاءُ قيامِ الجريمة بموجبِ السلوكِ السلبيِّ بالامتناع، وعلى ضوءِ البيانِ المُتقدِّمِ نعرضُ السلوكياتِ المُتعدِّدة التي يقومُ بها النموذجُ الإجراميُّ لهذه الجريمة.

١- صورُ السلوكِ الإجراميِّ في القانونِ الإماراتيِّ:

جاء نصُّ المادةِ (٦) من قانونِ مكافحةِ الشائعاتِ والجرائمِ الإلكترونيَّةِ الإماراتيِّ مُعولاً على عددٍ من السلوكياتِ كما أوردها النصُّ، هي "... حصلَ أو استحوذَ أو عدلَ أو أتلفَ أو أفشى أو سربَّ أو ألغى أو حذفَ أو نسخَ، أو نشرَ أو أعادَ نشرَ بغيرِ تصريحِ بياناتٍ أو معلوماتٍ شخصيَّةٍ...".

وتحملُ كلُّ صورةٍ من الصورِ المُتقدِّمةِ بياناً له خصوصيتهُ إذا ما نظرنا إلى مفهومه في هذا الصدد، إذ يعدُّ المقصودُ بالحصولِ هو التوصلُ إلى البيانِ بغيرِ الطريقِ الذي نظمته المُشرِّع، وإذا كان الحصولُ قد يتمُّ من الشخصِ ذاته أو الغير، إلّا أنَّ الاستحواذَ يأتي بمعنى حيازةِ البيانِ، ولا يقعُ هذا السلوكُ سوى من الغير، أمَّا التَّعديلُ فهو تغييرٌ في جوهرِ البيانِ وطمسِ حقيقته، أمَّا الاتِّلافُ فيُقصدُ به تدميرُ الملفِّ، والإفشاءُ والتَّسريبُ يأتيانِ بمعنى السَّماحِ للغيرِ بالاطِّلاعِ على البيانِ ومعرفته دون وجهِ قانونيِّ، كلُّ ما هنالك أنَّ الإفشاءَ يأتي بسلوكٍ إيجابيِّ، على خلافِ التَّسريبِ الذي قد يكونُ بموجبِ سلوكٍ سلبيِّ بالامتناع، أمَّا الإلغاءُ فيُقصدُ به إنهاءُ وجودِ البيانِ، وهو في هذا الصددِ قريبٌ من الحذفِ، أمَّا

(٤٣) د. فتوح عبد الله الشاذلي، شرح قانون العقوبات، القسم العام، الكتاب الأول، (الإسكندرية: دار المطبوعات

الجامعيَّة، ٢٠١٨م)، ص ٢٥٥ وما بعدها.

(٤٤) ذهبت المحكمةُ الاتِّحاديَّةُ العليا الإماراتيَّةُ في قضائها إلى أنه "يجبُ لقيامِ الركنِ الماديِّ للجريمة فعلٌ يقارفه الجاني، وإنَّ الفعلَ هو السلوكُ الإجراميُّ الذي يرتكبه الجاني، ولا تقومُ الجريمة قانوناً إلّا إذا كان هذا السلوكُ أو الفعلُ غيرَ مشروعٍ وصادراً عن إرادةٍ جنائيَّةٍ يقترنُ بها نشاطُ الجاني..."، الطَّعن رقم ١٢٣ لسنة ٢٢ قضائيَّة، الأحكام الجزائيَّة،

بتاريخ ٣/١/٢٠٠١م، مكتب فني (٢٣)، الجزء (٢)، ص (٧٩٥)، منشور لدى شبكة قوانين الشرق

"www.eastlaws.com.uoseresources.remotexs.xyz/data/ahkam/app."

النسخُ فهو يأتي بمعنى المطابقة، وأما النشر وإعادته فيُقصد به إضفاء طابع العلانية على البيانات، وتجدر الإشارة إلى أن كافة هذه السلوكيات قريبة في معناها من بعضها البعض، كل ما هنالك أنه يتعين إعمال هذا السلوك غير المشروع دون تصريح أو على غير النحو المتبع قانوناً.

وتجدر الإشارة إلى أن هذه الصور المتقدمة جميعها وردت على سبيل الحصر، ومن ثم لا يحق القياس عليها؛ نظراً لكون القياس غير معمول به في نطاق القوانين الجنائية، هذا بالإضافة إلى أن المشرع الجنائي يأخذ بيقين التفسير المضيق، والذي يحول واستخدام صور أخرى على خلال المتقدم؛ تقديراً للمبدأ العام الذي يعد ما تقدم نتائج له، وهو مبدأ الشرعية، أي لا جريمة ولا عقوبة إلا بنص، وإذا كان المشرع حدد الأفعال التي يتم العقاب عليها، فإن هذه الأفعال لا يجوز التزيد عليها أو الإنقاص منها، وإلا بات ذلك خروجاً غير مبرر عن النص، وانتهاكاً لإرادة المشرع في ذات الوقت.

وتعد الصور المتقدمة جميعها غير مشروعة، والسبب الجوهري في ذلك هو أن المشرع الإماراتي أراد أن يشمل النص كافة صور التعامل على البيانات والمعلومات الشخصية؛ وذلك للحيلولة وتحقيق المخالفة، إذ نظم في إطار قانون حماية البيانات الشخصية الاتحادي، الحالات التي على ضوءها

يتم معالجة البيانات الشخصية بدون موافقة صاحبها^(١)، كما حدّد ضوابط معالجة هذه البيانات^(٢)، كما نظّم من جانب آخر شروط الموافقة على معالجة البيانات^(٣).

(١) تنصّ المادة (٤) من قانون حماية البيانات الشخصية الاتّحاديّ الإماراتيّ على أنه يُحظر معالجة البيانات الشخصية دون موافقة صاحبها، وتسنّتي أيّ من الحالات التالية من هذا الحظر وتعتبر المعالجة حينها مشروعة: أن تكون المعالجة ضروريةً لحماية المصلحة العامّة.

أن تكون المعالجة مرتبطةً بالبيانات الشخصية التي أصبحت متاحةً ومعلومةً للكافة بفعل من صاحب البيانات. أن تكون المعالجة ضروريةً لإقامة أيّ من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلّق بالإجراءات القضائية أو الأمنية.

أن تكون المعالجة ضروريةً لأغراض الطبّ المهنيّ أو الوقائيّ من أجل تقييم قدرة الموظّفين على العمل، أو التشخيص الطبيّ أو تقديم الرّعاية الصحيّة أو الاجتماعيّة أو العلاج أو خدمات التأمين الصحيّ أو إدارة أنظمة وخدمات الرّعاية الصحيّة أو الاجتماعيّة وفقاً للتشريعات السّارية في الدولة.

أن تكون المعالجة ضروريةً لحماية الصحة العامّة، وتشمل الحماية من الأمراض السّارية والأوبئة أو لأغراض ضمان سلامة وجودة الرّعاية الصحيّة والأدوية والعقاقير والأجهزة الطبيّة، وفقاً للتشريعات السّارية في الدولة. أن تكون المعالجة ضروريةً لأغراض أرسيفيّة أو دراسات علميّة وتاريخيّة وإحصائيّة وفقاً للتشريعات السّارية في الدولة.

أن تكون المعالجة ضروريةً لحماية مصالح صاحب البيانات. أن تكون المعالجة ضروريةً لأغراض قيام المتحكّم أو صاحب البيانات بالتزاماته ومباشرة حقوقه المقرّرة قانوناً في مجال التوظيف أو الضمان الاجتماعيّ أو القوانين المعنيّة بالحماية الاجتماعيّة، وذلك بالقدر الذي يُسمح به في تلك القوانين.

أن تكون المعالجة ضروريةً لتنفيذ عقدٍ يكون صاحب البيانات طرفاً فيه أو لتأخذ إجراءات بناءً على طلب صاحب البيانات؛ بهدف إبرام عقد أو تعديله أو إنهائه.

أن تكون المعالجة ضروريةً لتنفيذ التزامات محدّدة في قوانين أخرى في الدولة على المتحكّم. أيّة حالات أخرى تحدّدها اللائحة التنفيذية لهذا المرسوم بقانون".

(٢) تنصّ المادة (٥) من قانون حماية البيانات الشخصية الاتّحاديّ الإماراتيّ على أنه "يتمّ معالجة البيانات الشخصية وفقاً للضوابط الآتية:

أن تكون المعالجة بطريقة عادلة وشفافة ومشروعة.

٢- صور السلوك الإجرامي في القانون المصري:

لم ينظم المشرع المصري التجريم المتقدم بذات الكيفية التي نظم بها المشرع الاتحادي الإماراتي؛ نظراً لأن هذا الأخير نظم كافة هذه الصور في نطاق محدود، وهو نص المادة (١/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية، على خلاف المشرع المصري، والذي نظم ذات صور السلوك الإجرامي،

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 مشابهاً أو متقارباً من الغرض الذي جمعت هذه البيانات من أجله.

أن تكون البيانات الشخصية كافية ومقتصرة على ما هو ضروري وفقاً للغرض الذي تمت المعالجة من أجله. أن تكون البيانات الشخصية دقيقة وصحيحة، وأن تخضع للتحديث متى اقتضى الأمر ذلك. أن تتوفر تدابير وإجراءات لضمان محو أو تصحيح البيانات الشخصية غير الصحيحة. أن تكون البيانات الشخصية محفوظة بشكل 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 وفقاً للقوانين والتشريعات السارية في هذا الشأن.

عدم الاحتفاظ بالبيانات الشخصية بعد استنفاد الغرض من معالجتها، ويجوز الإبقاء عليها في حال تم إخفاء هوية صاحب البيانات باستخدام خاصية "آلية إخفاء الهوية".

أيّة ضوابط أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون".

(١) تنص المادة (٦) من قانون حماية البيانات الشخصية الاتحادي الإماراتي على أنه "شروط الموافقة على معالجة البيانات:

يُشترط للاعتداد بموافقة صاحب البيانات على معالجتها ما يلي:

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

أن تكون الموافقة مُدَّةً بطريقة واضحة وبسيطة وغير مُبهمة وسهلة الوصول إليها سواء كانت كتابية أو إلكترونية. أن تتضمن الموافقة ما يفيد حق صاحب البيانات بالعدول عنها، وأن يكون إجراء العدول بطريقة سهلة.

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

ولكن في نطاق المواد (٢/١٤)^(١)، (١٧)^(٢) من قانون مكافحة جرائم تقنية المعلومات، كل ما هنالك أن المشرع الإماراتي توسع في عرض هذه الصور السلوكية، لا سيما وبصدد سلوك الاستحواذ، وتعد سياسة المشرع في هذا المقام جلية، وهي ذاتها ما تم تنظيمه من قبل المشرع الإماراتي، إذ عول المشرع المصري على تنظيم حقوق الشخص المعني بالبيانات وشروط جمع ومعالجة هذه البيانات^(٣)، هذا

(١) تنص المادة (٢/١٤) من قانون حماية البيانات الشخصية المصري على أنه "وتحدد اللائحة التنفيذية لهذا القانون السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها".

(٢) تنص المادة (١٧) من قانون حماية البيانات الشخصية المصري على أنه "يحظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات، إلا بتوافر الشروط الآتية:

الحصول على موافقة من الشخص المعني بالبيانات.

أن يتضمن الاتصال هوية منشئه ومرسله.

أن يكون للمرسل عنوان صحيح وكاف للوصول إليه.

الإشارة إلى أن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر.

وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها".

(٣) تنص المادة (٢) من قانون حماية البيانات الشخصية المصري على أنه "لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشاؤها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانوناً.

ويكون للشخص المعني بالبيانات الحقوق الآتية:

العلم بالبيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.

العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

التصحيح، أو التعديل، أو المحو، أو الإضافة، أو التحديث للبيانات الشخصية.

تخصيص المعالجة في نطاق محدد.

العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.

بالإضافة إلى تنظيم شروط جمع البيانات الشخصية لأجل المعالجة^(١)، كما نظم شروط المعالجة^(٢)، وذلك بأكمله على النحو الوارد في قانون حماية البيانات الشخصية.

ب) النتيجة الإجرامية:

إذا كنا نسلّم بأن النتيجة الإجرامية هي النتائج عن السلوك الإجرامي، وهذا ما يدعونا إلى استعراض إشكاليتين جوهريتين في هذا الصدد، وهما على النحو الآتي:

أ- الإشكالية الأولى: إمكانية قيام الشروع:

يقصد بالشروع: البدء في تنفيذ السلوك الإجرامي ثم توقّف آثار هذا السلوك لأسباب لا دخل لإدارة الجاني فيها، وهذا المفهوم تعارف عليه الفقه، وكذلك القضاء، يستوي في ذلك القضاء

وباستثناء البند (٥) من الفقرة السابقة، يُؤدّي الشخصُ المعنيُّ بالبيانات مقابل تكلفة الخدمة المقدّمة إليه من المتحكّم أو المُعالج فيما يخصُّ ممارسته لحقوقه، ويتولّى المركز إصدار قرارات تحديد هذا المُقابل بما لا يُجاوز عشرين ألف جنيه".

(١) تنصُّ المادة (٣) من قانون حماية البيانات الشخصية المصريّ على أنه "يجبُ لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافرُ الشروط الآتية:

أن تجمعَ البيانات الشخصية لأغراضٍ مشروعةٍ ومُحدّدةٍ ومُعلّنةٍ للشخص المعنيّ.
أن تكونَ صحيحةً وسليمةً ومُؤمّنةً.

أن تُعالجَ بطريقةٍ مشروعةٍ وملائمةٍ للأغراض التي تمّ تجميعها من أجلها.

ألا يتمّ الاحتفاظُ بها لمدةٍ أطولَ من المدة اللازمة للوفاء بالغرض المُحدّد لها.

وتُحدّد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات".

(٢) تنصُّ المادة (٦) من قانون حماية البيانات الشخصية المصريّ على أنه "تعدُّ المعالجة الإلكترونية مشروعةً وقانونيةً في حال توفر أيٍّ من الحالات الآتية:

مُوافقة الشخص المعنيّ بالبيانات على إجراء المعالجة من أجل تحقيق غرضٍ مُحدّدٍ أو أكثر.

أن تكونَ المعالجة لازمةً وضروريةً تنفيذًا للالتزام تعاقديةً أو تصرف قانونيٍّ أو لإبرام عقدٍ لصالح الشخص المعنيّ بالبيانات، أو لمباشرة أيٍّ من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها.

تنفيذ التزام ينظّمه القانون أو أمر من جهات التحقيق المختصة أو بناءً على حكم قضائيّ.

تمكين المتحكّم من القيام بالتزاماته أو أيّ ذي صفةٍ من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعنيّ بالبيانات".

الإماراتي^(١) أم المقارن^(٢)، وفي إطار ذلك وبصورة إجمالية، نرى أن طبيعة صور السلوك الإجرامي في الجريمة المتقدمة تختلف باختلاف طبيعة السلوك الإجرامي الذي عولت عليه إرادة المشرع، إذ إن كل مفهوم من المفاهيم السالفة يحمل في ماهيته خصوصية جوهرية، وعلى ضوء ذلك فهناك من السلوكيات ما تعدُّ صالحةً لتطبيق أحكام الشروع بصدها، وأخرى لا يمكنُ إعمالُ الشروع بشأنها، لذلك فإن القولَ والفصلَ في هذه المسألة يرجعُ إلى طبيعة السلوك الإجرامي المخالف ذاته.

ب-الإشكالية الثانية: طبيعة الجريمة:

تعرضُ هذه الإشكالية ما إذا كانت الجريمة المتقدمة من قبيل الجرائم المادية، أم أنها من الجرائم الشكلية، والفرقُ بين كليهما يتلخصُ في أن الجرائم المادية هي الجرائم التي يعدُّ ركنها المادي مكوناً من نشاطٍ أو سلوكٍ إجراميٍّ، ونتيجة إجرامية، وبينهما علاقة سببية، وهذه الجرائم بطبيعتها إما تامة، وإما شروع، ومن ثم فإنَّ الشروع في نطاقها متصور، أما الطائفة الأخرى فهي طائفة الجرائم الشكلية، وهذه الطائفة من الجرائم يتألفُ ركنها المادي من فعلٍ إجراميٍّ تامٍّ؛ أي إنَّ الجريمة تتحقق بمجرد ارتكاب هذا السلوك الإجرامي، وذلك دون النظر إلى النتائج.

وعلى ضوء ما تقدم، فإنَّ مسألة ما إذا كانت الجريمة من قبيل الجرائم الشكلية من عدمه أمرٌ يرجعُ إلى طبيعة السلوك الإجرامي ذاته، وذلك على النحو الذي أسلفناه بصدد الحديث عن مكنة الشروع في الجريمة المتقدمة.

٣-علاقة السببية:

-
- (١) ذهبت محكمة النقض المصرية إلى أن "الشروع في حكم المادة ٤٥ من قانون العقوبات هو البدء في تنفيذ فعل بقصد ارتكاب جنائية أو جنحة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الفاعل فيها، فلا يشترط لتحقيق الشروع أن يبدأ الفاعل بتنفيذ جزء من الأعمال المكونة للركن المادي للجريمة، بل يكفي لاعتباره شارعاً في ارتكاب جريمة أن يأتي فعلاً سابقاً على تنفيذ الركن المادي لها مؤدياً إليه حالاً" الطعن رقم ١٨٨٠٧ لسنة ٨٥ قضائية، الدوائر الجنائية، جلسة ٢٠١٧/١٢/٢٠م، منشور هذا الحكم على الموقع الرسمي للمحكمة <https://www.cc.gov.eg>.
- (٢) قضت المحكمة الاتحادية العليا الإماراتية بأنَّ الشروع هو البدء في تنفيذ بقصد ارتكاب جريمة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الجاني فيها...، الطعن رقم ٨٢ لسنة ٢٦ قضائية، الأحكام الجزائية، بتاريخ ٢٠٠٥/١/٨م، وقريب من ذلك: الطعن رقم ١٣٥٧ لسنة ٢٠٢١ قضائية، الدائرة الجزائية، بتاريخ ٢٠٢٢/٣/٢٢م، نُشر هذا الحكم على شبكة قوانين الشرق.

تعدُّ علاقة السببية^(١) هي الرباط الوثيق الذي يربط السلوك الإجرامي بالنتيجة الإجرامية، إذ إن توافرها يكتمل به النموذج القانوني للجريمة المُتقدِّمة، ولا يُؤثِّر على توافر علاقة السببية من عدمه وكونها عنصراً من عناصر الركن المادي ما إذا كانت الجريمة من قبيل الجرائم المادية أو الجرائم الشكلية، وتتحقَّق علاقة السببية بمجرد التعامل على هذه البيانات وثبوت أن هذا التعامل يرجع إلى إحدى صور السلوكيات التي نظَّمها النصُّ.

وتذهب المحكمة الاتِّحادية العليا الإماراتية إلى أن "استخلاص توافر علاقة السببية من المسائل الموضوعية التي تخضع لتقدير محكمة الموضوع"^(٢)...، كما ذهبت محكمة النقض المصرية إلى أن^(٣) "علاقة السببية في المواد الجنائية هي علاقة مادية تبدأ بالفعل الذي قارفه عمداً، وثبوت قيام هذه العلاقة من المسائل الموضوعية التي ينفرد قاضي الموضوع بتقديرها، فمتى فصل في شأنها إثباتاً أو نفيًا فلا رقابة لمحكمة النقض عليه..."^(٤).

ثانياً: الركن المعنوي للجريمة:

إن جريمة التعامل على البيانات والمعلومات الشخصية بدون تصريح تعدُّ من قبيل الجرائم العمدية، أي لا بدُّ من توافر القصد الجنائي، وأن احتمالية قيام الخطأ واعتبار الجريمة غير عمدية أمرٌ مُستبعد نسبياً، وعلى ضوء ذلك نعرض لعناصر القصد الجنائي على النحو الآتي:

(أ) علم الجاني:

(١) د. عزري الزين، العلاقة السببية كشرط لمسؤولية الإدارة في مجال العمران، بحثٌ منشورٌ بمجلة العلوم الإنسانية،

العدد (٢٢)، جامعة منتوري، قسنطينة، الجزائر، ديسمبر ٢٠٠٤م، ص ٩١ وما بعدها.

(٢) حكم المحكمة الاتِّحادية العليا الإماراتية، الطعن رقم ١٨ لسنة ٢٠١٦ قضائية، الدائرة الجزائية بتاريخ ٢١/٣/٢٠١٦م،

منشور لدى شبكة قوانين الشرق.

(٣) حكم محكمة النقض المصرية، الطعن رقم ٢٠٦٦ لسنة ٨٩ قضائية، الدوائر الجنائية، جلسة ٦/٦/٢٠٢١م، منشورٌ

على الموقع الرسمي للمحكمة <https://www.cc.gov.eg>.

(٤) حكم محكمة النقض المصرية، الطعن رقم ١٢١٩٦ لسنة ٩٠ قضائية، الدوائر الجنائية، جلسة ٤/١٢/٢٠٢١م،

منشور على الموقع الرسمي للمحكمة <https://www.cc.gov.eg>.

يعدُّ العلمُ أولَ عناصرِ القصدِ الجنائيِّ^(١)، والعلمُ في هذا النطاقِ يشملُ كافةَ عناصرِ الركنِ الماديِّ، والعلمُ الذي نقصده هو العلمُ التامُّ أو اليقينيُّ دون العلمِ الظنيِّ؛ نظراً لكون العلمِ الظنيِّ يقومُ به ركنُ الخطأ، والخطأ في هذا الخصوص إذا تولّد أُقيم معه ركن غير العمد، وباتت الجريمة غير عمدية، ونعرضُ في هذا الصددِ للمفترضات التي يتعيّن العلمُ التامُّ بها من قبلِ الجاني، وهي على النحو الآتي:

أ- العلمُ بأنَّ السلوكِ الحاصلِ من قبَله يعدُّ لا محالةً مُنتهكاً ومُتعارضاً لقواعدِ الخصوصيةِ التي أناطها الدستورُ بالتنظيم، وانتهاكاً للحرمة التي يتعيّن أن يتمتّع بها الأفرادُ كافةً، وهذا العلمُ يؤكّد الطابعِ العمديِّ للجريمة؛ نظراً لأنَّ الحقَّ في الخصوصيةِ من جانبٍ يعدُّ من قبيلِ المبادئِ الدستوريةِ العامة، وحقاً دستورياً خالصاً، هذا بالإضافة إلى ما يمثله ذلك من انتهاكٍ لقواعدِ النظامِ العامِّ التي يقوم عليها المجتمع.

ب- العلمُ قائمٌ بكونِ السلوكِ المُخالفِ الذي أتاه مُتعارضاً مع القواعدِ التي نظّمها المُشرّعُ في القوانينِ العقابية، بغضِّ النظر عن هذا القانونِ ومُسمّاه، يستوي في ذلك قانونُ الجرائمِ والعقوباتِ أو القوانينِ الخاصة التي تردُّ المُتعدّي على البياناتِ والمعلوماتِ الشخصية^(٢)؛ لما تُعول عليه القواعدُ العامةُ باعتبار أن القوانينِ الجزائية على وجه الخصوص لا يجوزُ تماماً الجهلُ بأحكامها، باعتبار قواعد القانونِ الجنائيِّ استثناءً مُتعارفاً عليه في إعمالِ مبدأ عدم جواز الاعتذار بالجهل بالقانون.

ج- العلمُ بأنَّ السلوكِ المُقام من جانبه يترتّبُ عليه قيامُ نتائج غير عادلة، وغير مشروعة، في حال تحقُّقها يترتّبُ عليها المُشرّعُ جزاءً جنائياً يصل في مقداره إلى حدِّ المساسِ بالحريةِ الشخصية، وكذاك الذمّة المالية.

د- العلمُ بوجود النتيجة غير المباشرة، وهذه الأخيرة تتصلُّ بما يترتّبهُ الجزاءُ الجنائيُّ بالنسبة لذوي الجاني إثر توقيع الجزاء عليه؛ نظراً لأنَّ العقوبة المُقيّدة للحرية قد تُفقد العائلةَ مصدرَ إعالتها، الأمرُ الذي يُوثرُ سلباً عليها.

ب) اتّجاه الإرادة:

(١) إنَّ القصدِ الجنائيِّ يُقصد به - كما يذهب جانبٌ من الفقه - علمُ الجاني بالوقائعِ المُكوّنة للجريمة وتوقُّعه للنتيجة ثم اتّجاه الإرادة إلى ارتكاب الفعل، وليست إرادة النتيجة، يُراجع: د. فايز علي الأسود، القصد الجنائي في القانون والشرعية الإسلامية - فقه الإمام الشافعي كنموذج، مؤتمر الإمام الشافعي، منشور على الإنترنت، ص ١٢٢١.

(٢) قد يكون الأمرُ منظماً بقانون حماية البيانات الشخصية، أو قانون مكافحة الشائعات والجرائم الإلكترونية.

تعدُّ الإرادةُ العنصرَ الثانيَ من عناصر القصد الجنائيِّ العامِّ، وهي نشاطٌ نفسيٌّ داخليٌّ يقطن داخل الجاني، ومدلولُ الإرادة في هذه الجريمة هو إرادةُ السلوك، وإرادةُ الجاني التي تتجه نحو الاستحواذ أو الحصول أو إتلاف أو أية صورةٍ من الصور التي عدّها النصُّ على البيانات أو المعلومات الشخصية؛ إذ بتحقق أو تمام الاستحواذ أو الإتلاف أو غيرهما تتمُّ الجريمة.

والإرادةُ يتعيَّن أن يتوافرَ فيها بعض السمات المهمّة؛ إذ يتطلَّب القانون أن تكون إرادةُ الجاني خاليةً من أيِّ عيبٍ يؤثّر عليها، لا سيما الإكراه^(١)، فتخلُّ أحد العيوب أو العوارض والمساس بإرادة الجاني يترتّب عليه التأثيرُ على قيام الجريمة والمسئوليّة عنها بدايةً، وكذلك على النتائج ذاتها، فلا جزاء إذا كانت إرادة الجاني مكرهةً على إتيان هذا العمل الإجرامي.

٣- طبيعةُ القصد الجنائيِّ:

نذهبُ في هذا الخصوص إلى أن جريمةَ التعاملِ على البيانات والمعلومات الشخصيةً بدون تصريحٍ هي جريمةٌ من قبيل جرائم القصد الجنائيِّ العامِّ^(٢)؛ نظراً لخلوّ النصِّ المنظّم للجريمة من هدفٍ خاصٍّ سعى المشرِّع إلى تنظيمه في إطار النصِّ في مرحلة التّفريد التّشريعيِّ، وعليه فإنّ القول بأنّ الجريمة المتقدّمة من جرائم القصد الخاصِّ أمرٌ لا يمكن التّسليم به، وانحرافٌ عن إرادة المشرِّع وغايته حيال النصِّ.

الفرع الثاني

العقوباتُ المقرّرة للجريمة

في ضوء الحديث عن العقوبات التي نظّمها المشرِّع بصدد الجريمة المتقدّمة، نقسّم تفصيلاً هذه العقوبات حسب الحقّ الذي تهل منه هذه العقوبة، ونفرّق في هذا الصّدّد بين موقف المشرِّع الإماراتيِّ ونظيره المصريِّ، وذلك على النحو الآتي:

(أ) العقوبةُ في القانون الإماراتيِّ:

(١) د. أحمد بن محمد بن مشيع الثبيتي، المسئوليّة الجنائيّة للصغير والمكروه والمجنون، بحثٌ منشورٌ بمجلة الدِّراسات

العربيّة، كليّة دار العلوم، جامعة المنيا، ٢٠١٨م، ص ٦٥٢٥ وما بعدها.

(٢) لذلك فإنّ موقفنا في هذا الخصوص يتجه إلى أنّ القصد الخاصِّ لا بدُّ أن يُثبّر النصِّ، فلا يمكن التّحويل إلى قصدٍ

خاصٍّ لم يُشر إليه المشرِّع، أو على الأقلِّ يمكن الاستدلال عليه من فحوى النصِّ.

نفرق في هذا الصدد بين العقوبة المُقيدة للحرية^(١)، وبين العقوبة الماسة بالذمة المالية، وذلك على النحو الآتي:

١- العقوبة المُقيدة للحرية:

حددها المشرع الاتحادي الإماراتي في عقوبة الحبس، باعتبارها عقوبة مُقيدة للحرية^(٢) في حالة وقوع أي سلوك من السلوكيات التي عدتها المادة (٦) من قانون مكافحة الشائعات والجرائم الإلكترونية، إذ كانت العقوبة حدّها الأدنى ستة أشهر، والمُلاحظ أنّ المشرع لم يضع حدًا أقصى للعقوبة، وعلى ضوء هذا النصّ يمكننا إبداء ملاحظتين:

الملاحظة الأولى: أنّ عقوبة الستة أشهر كحدّ أدنى لا نراها تُحقّق في هذا المقام الغاية التي أرادها المشرع؛ نظرًا لما قد يعتري هذه العقوبة من حالات الإفراج الشرطيّ خلال مدة مُعيّنة بالنظر إلى اعتبارات حسن السير والسلوك، فالعدالة لا يُمكنها أن تتحقّق بهذا النمط، والردع لا يمكن أن تنتج له ثمار إذا كانت العقوبة في حالة من الضالّة بالشكل المتقدّم.

الملاحظة الثانية: أنّ إرادة المشرع وإن عولت بصورة صريحة على إقرار الحدّ الأدنى فإن الحدّ الأقصى لذات الجريمة من عقاب يستدلّ عليه بصورة ضمنية؛ إذ يعدّ الحدّ الأقصى المتعيّن اعتباره لموادّ الجرح هو ثلاث سنواتٍ وفق ما تقضي به القواعد العامة.

٢- العقوبة المالية:

نظّم المشرع الاتحادي الإماراتي طي النصّ المتقدّم عقوبة الغرامة باعتبارها عقوبة أصلية^(٣)، إذ نصّ على حدّ أدنى لعقوبة الغرامة مقداره عشرون ألف درهم، وحدّ أقصى مائة ألف درهم، وإن كنا نرى من منطلق المنطق القانوني أنّ القضاء على جرم مُعيّن أو الحدّ منه لا يمكن إتمامه إلا إذا كان الحقّ الذي يمسه الجزاء قاسياً، معرضاً الشخص للخطر، ولا أشدّ في ذلك من التعويل على غرامة

(١) راجع: د/ فتوح عبد الله الشاذلي، علم الإجرام وعلم العقاب (الإسكندرية: دار المطبوعات الجامعية، ٢٠١٧م)، ص ٣٥٢ وما بعدها.

(٢) يُراجع تفصيلاً: خلود عبد الرحمن العبادي، العقوبات المُجتمعية في التشريعات الجزائية الأردنية - واقع وطموح، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٥م، ص ٢٦ وما بعدها.

(٣) عولت المادة (٦٧) من قانون الجرائم والعقوبات الاتحادي الإماراتي على اعتبار الغرامة من قبيل العقوبات الأصلية.

مالية جسيمة، بحيث يتحقق الردع الخاص في أقسى صورته، لذلك كنا نأمل من المشرع زيادة الحد الأدنى للغرامة عن الحد الذي أقره النص^(١).

ومما تجدر الإشارة إليه في هذا الخصوص أن المشرع منح القاضي سلطة تقديرية واسعة بصدد تطبيق الجزاء، في مرحلة التفريد القضائي، وهذا يعد مظهرًا جليًا بالنظر إلى إرادته في الاختيار حال التطبيق بين القضاء بالحبس والغرامة معاً، أو أيهما، إلا أننا نرى في هذا المقام أنه لم يضع معياراً معيناً على ضوئه يمكن القول بازدواج الجزاء أو اختيار أيهما، لذلك لا نرى داعياً في هذا الخصوص إلى إعمال السلطة التقديرية، والسبب في ذلك نراه من جانبنا متمثلاً في أن تدرج السلوكيات المادية التي شملها النص لا يمكنها أن تكون متدرجة من حيث الجسامه؛ ما لم يكن هناك سلوك مغاير بطبيعته لما هو متقدم؛ أي إن نظرة المشرع إلى هذه الجريمة تكون بالنظر إلى سلوكها؛ فلما أن يقع أو لا يقع.

ولا مانع في هذا الصدد من التحويل على العقوبة التبعية التي نظمتها المادة (٥٦) من قانون مكافحة الشائعات والجرائم الإلكترونية^(٢).

ب) العقوبة في القانون المصري:

في ضوء بيان إرادة المشرع المصري من عقوبة التعامل على البيانات والمعلومات الشخصية بدون تصريح أو وجه حق، نعرض لكل من العقوبة السالبة للحرية التي نظمها المشرع، وكذلك العقوبة الماسة بالذمة المالية، وذلك على النحو الآتي:

١- العقوبة السالبة للحرية:

(١) يُراجع بصدد العقوبات المالية: أ.م. د. صباح سامي داود، صابرين إبراهيم رضا، عقوبة الغرامة البديلة لسلب الحرية، بحث منشور بعدد خاص لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الثاني، المجلد (٣٦)، أيلول ٢٠٢١م، منشور إلكتروني، ص ٣٠٣.

<https://jols.uobaghdad.edu.iq/index.php/jols/article/download/434/356/763>

(٢) تنص المادة (٥٦) من قانون مكافحة الشائعات والجرائم الإلكترونية على أنه "مع عدم الإخلال بحقوق الغير حسن النية، وفي حال الإدانة يُحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، وبحذف المعلومات أو البيانات.

نظم المُشرِّع عقوبة الحبس باعتبارها العقوبة واجبة التطبيق حال المساس أو التعدي بدون وجه حقٍ على البيانات أو المعلومات الشخصية، وفي هذا الصدد نفرِّق بين عقوبتين للحبس، وذلك في الفرضين الآتيتين:

الفرض الأول: تكون العقوبة الحبس بحدٍّ أدنى لا يقلُّ عن سنتين، إذا كان الدخولُ إلى نظام معلوماتيٍّ بدون وجه حقٍ يترتَّبُ عليه إلتافٌ أو محوٌ للبيانات، أو أية صورةٍ من السلوكيات الأخرى التي عولت عليها المادة (٢/١٤) من قانون مكافحة جرائم تقنية المعلومات^(١).

الفرض الثاني: تكون فيه العقوبة هي ذاتها، أي الحبس بحدٍّ أدنى لا يقلُّ عن سنتين، وذلك في حالة إلتافٍ أو تعطيلٍ أو تعديل مسارٍ أو الإلغاء الجزئيٍّ أو الكليٍّ للبيانات أو المعلومات، بالإضافة لما عددهم المادة (١٧) من قانون مكافحة جرائم تقنية المعلومات في ذات النطاق^(٢).

ويعدُّ تنظيم المُشرِّع المصريِّ العقوبة السالبة للحرية أفضلَ مما نظَّمه المُشرِّع الإماراتيُّ في ذات الصدد؛ نظراً لأنَّ جسامه الجزاء بعدُّ أكثرَ الطرق فاعليَّةً نحو تحقيق الردع بصورتَيْه، يستوي في ذلك العام أو الخاص.

٢- العقوبة المالية:

تعدُّ عقوبة الغرامة التي نظَّمها المُشرِّع المصريُّ مُختلفةً عما نظَّمه في المواد (٢/١٤)، (١٧) من قانون مكافحة جرائم تقنية المعلومات، إذ في ضوء ما عولت عليه المادة (٢/١٤) سالف الإشارة إليها، عدَّ المُشرِّع غرامةً ماليَّةً حدُّها الأدنى مائة ألف جنيه، وحدُّها الأقصى مائتا ألف جنيه، أما في

(١) تنصُّ المادة (٢/١٤) من قانون مكافحة جرائم تقنية المعلومات المصريِّ على أنه: فإذا نتجَ عن ذلك الدخولُ إلتافٌ أو محوٌ أو تغييرٌ أو نسخٌ أو إعادة نشرٍ للبيانات أو للمعلومات الموجودة على ذلك الموقع أو الحساب الخاصِّ أو النظام المعلوماتيِّ، تكون العقوبة الحبسَ مدَّةً لا تقلُّ عن سنتين، وغرامةً لا تقلُّ عن مائة ألف جنيه ولا تُجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

(٢) تنصُّ المادة (١٧) من قانون مكافحة جرائم تقنية المعلومات المصريِّ على أنه: يُعاقبُ بالحبسِ مدَّةً لا تقلُّ عن سنتين، وبغرامةٍ لا تقلُّ عن مائة ألف جنيه ولا تُجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كلُّ من ألتفَّ أو عطَّلَ أو عدَّلَ مسارٍ أو ألغى كلياً أو جزئياً متعمداً وبدون وجه حقٍ البرامج والبيانات أو المعلومات المُخزَّنة أو المُعالجة أو المولدة أو المُخلقة على أيِّ نظامٍ معلوماتيٍّ وما في حكمه، أيًّا كانت الوسيلة التي استخدمت في الجريمة.

نطاق ما عوّلت عليه المادة (١٧) من ذات القانون سالف الإشارة إليها، فكانت العقوبة مُتفكّةً في حدّها الأدنى مع سابقتها، أي مائة ألف جنيه، ولكنها مُختلفةٌ في حدّها الأقصى، بلوغاً خمسمائة ألف جنيه. تجدر الإشارة إلى أنه تمّ تعديل ما نظّمه المُشرّع بصدّد حالات الإعفاء، وكذلك العقوبات التبعيّة، والمنصوص عليها في المواد (٣٨)^(١)، (٤١)^(٢) من قانون مُكافحة جرائم تقنيّة المعلومات.

المطلب الثاني

جريمة التّعدي على البيانات الشخصية

الطبيّة أو المصرفيّة

في إطار هذا المطلب نقسّم حديثنا إلى فرعين، نعرضُ في الأول الحديث عن أركان هذه الجريمة، أمّا الثاني فننتاولُ فيه أحكام العقاب، وذلك على النحو الآتي:

(١) تنصُّ المادة (٣٨) من قانون مُكافحة جرائم تقنيّة المعلومات المصريّ على أنه مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أيّ جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدّات والأجهزة ممّا لا يجوزُ حيازتها قانوناً، أو غيرها ممّا يكونُ قد استُخدم في ارتكاب الجريمة، أو سهّل أو ساهم في ارتكابها، وفي الحالات التي يتعيّن لمزاولة النشاط فيها الحصولُ على ترخيص من إحدى الجهات الحكوميّة، وكان الشخصُ الاعتباريُّ المُدان بأيّ جريمة منصوصٍ عليها في هذا القانون لم يحصلُ على الترخيص، فيحكم فضلاً عن العقوبات المُقرّرة بالغلق.

(٢) تنصُّ المادة (٤١) من قانون مُكافحة جرائم تقنيّة المعلومات المصريّ على أنه: يُعفى من العقوبات المُقرّرة للجرائم المنصوص عليها في هذا القانون كلُّ من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائيّة أو السلطات العامّة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها، ويجوزُ للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغُ بعد كشف الجريمة وقبل التصرف في التحقيق فيها إذا مكّن الجاني أو الشريك، في أثناء التحقيق، السلطات المُختصة من القبض على مُرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتّحقيق على كشف الحقيقة فيها، وعلى القبض على مُرتكبي جريمةٍ أخرى مُماثلة لها في النوع والخطورة، ولا يُخلُ حكم هذه المادةُ بوجوب القضاء بردِّ المال المُتحصّل من الجرائم المنصوص عليها في هذا القانون.

الفرع الأول أركان الجريمة

عولت المادة (٢/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي الإماراتي على تجريم التعدي على البيانات الشخصية الطبية أو المصرفية، وذلك بنصه: "... فإذا كانت البيانات أو المعلومات المشار إليها في البند (١) 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، إذ تعد الجريمة المتقدمة في إطار النص السابق على الرغم من اعتبارها نموذجاً إجرامياً له طابعه من الخصوصية والاستقلال، إلا أنها تعد ظرفاً مشدداً في ذات الوقت، وذلك على النحو الوارد بالنص السالف.

تعد جريمة التعدي على البيانات الشخصية الطبية أو المصرفية من قبيل الجرائم التي أَرادها المشرع الاتحادي الإماراتي، وأقام لها تنظيمًا كاملاً، إذ لم يعرض المشرع لتنظيم هذه الجريمة لا في قانون حماية البيانات الشخصية، ولا في قانون مكافحة الشائعات والجرائم الإلكترونية، مفاد ذلك أن التشريع المصري جاء خالياً من هذا التنظيم، وإزاء ذلك نقصد في ضوء من الخصوصية الإلمام بكافة جوانب هذه الجريمة، وتطبيقها في نطاق التشريع الاتحادي الإماراتي؛ كونه نموذجاً فعلياً لهذه الجريمة، وعليه نعرض في هذا الفرع البناني القانوني لهذه الجريمة موضحاً أركانها، وذلك على النحو الآتي.

تتمثل أركان الجريمة في قيام ركنين جوهريين، أحدهما - كما أشرنا سلفاً - يتمثل في الركن المادي، والآخر يتمثل في الركن المعنوي، ويتطلب القانون تعاضراً هذين الركنين، يستوي في ذلك إن تعلق الأمر بالمشرع الإماراتي أم بغيره من مشرعي النظم الأخرى المقارنة، وإزاء ذلك نعرض لأركان الجريمة في إطار الخصوصية التي تتضمنها جريمة التعدي على البيانات الشخصية الطبية أو المصرفية، وذلك على النحو الآتي:

أولاً: الركن المادي في الجريمة:

يعد الركن المادي هو الركن الأساس لأية جريمة، ولا يمكن أن تُقام جريمة إلا بتوافر هذا الركن^(١)، وقد نظم المشرع الركن المادي لهذه الجريمة وغيره في المادة (٢/٦) من قانون مكافحة

(١) د. فتوح عبد الله الشاذلي، شرح قانون العقوبات، القسم العام، الكتاب الأول، المرجع السابق، ص ٢٥٥ وما بعدها.

الشائعات والجرائم الإلكترونية الإماراتي، وكذلك قانون مكافحة جرائم تقنية المعلومات المصري، لا سيما عموم نص المادة (١٧) منه؛ نظراً لأن المشرع لم ينص عليها بصورة جلية.

ومن تحليل واستقراء النص المتقدم، نجد أن ماهية البيانات الطبية تكمن في الفحوصات الطبية، التشخيص الطبي، العلاج الطبي، الرعاية الطبية، السجلات الطبية.

وتتميز البيانات الطبية على النحو الذي قدمته المادة (٢/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي الإماراتي بالآتي^(١):

- **الخصيصة الأولى:** تتمثل في الطابع الشخصي للبيانات الطبية، إذ إن هذه البيانات تُعد إحدى صور البيانات الشخصية المتعين حمايتها؛ لما فيها من قيمة وخصوصية يجب أن يتمتع بها كافة الأفراد، الأمر الذي يتعين معه أن تكون لتلك البيانات حرمة كمحل للحماية الجنائية، لا يتوجب معها بطبيعة الحال المساس بها أو التعدي عليها.
- **الخصيصة الثانية:** الطابع الإلكتروني للوسيلة المستخدمة في الحصول على البيانات الطبية الإلكترونية، سواء من موقع إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات أو نظام للمعلومات الإلكترونية.
- **الخصيصة الثالثة:** أن مفهوم البيان الطبي الإلكتروني، الوارد النص عليه في المادة السابعة سالف الحديث عنه، يتمثل في (الفحوصات - التشخيصات - العلاجات - الرعاية)، وهي تعد واردة على سبيل الحصر، فلا يجوز القياس عليها، ولكن مصطلح الفحوصات أو التشخيصات يشمل كافة صور الفحص أو التشخيص الطبي.
- **الخصيصة الرابعة:** الطابع الحمائي لهذه البيانات الطبية الإلكترونية، ويتمثل الطابع الحمائي في هذا الخصوص في الحماية الجنائية لاعتبار البيانات الطبية الإلكترونية في حاجة إلى خصوصية، ويعد الحق مقررًا من قبل المشرع الجزائري، إذ أقام جزاءً رادعاً للتعدي على هذه البيانات^(٢).

(١) د. شيماء عبد الغني عطا الله، تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية، بحث منشورٌ بمجلة كلية القانون الكويتية العالمية، يونيو ٢٠١٥، العدد ١٠، السنة الثالثة، ص ٥٠٣.

(٢) سليم جلد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقهاء الإسلامي، مذكرة لنيل شهادة الماجستير في الشريعة والقانون، ٢٠١٢ - ٢٠١٣م، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، ص ١٦.

أما عن السلوك الإجرامي فإنه يعد وفقاً للمعنى الفلسفي كل نشاط مادي أو معنوي يمارسه الإنسان، فهو بذلك يستوعب الحركات والسكنات والمقاصد والأفكار، وفي إطار بيان السلوك من الناحية القانونية لا يتم الاعتداد في هذا الخصوص إلا بالنشاط القائم في العالم الخارجي، إذ يجب إخراج الأفكار الداخلية التي تعد باطنة إلى حيز الوجود المادي^(١)، ويعد السلوك أهم عناصر الركن المادي؛ نظراً لما يُمثله من اعتباره قاسماً مشتركاً بين كافة الجرائم، إذ لا قيام للركن المادي ولا قيام للجريمة بدونه، وبالتالي يندم العقاب، ويؤكد الفقه في مجموعه على أنه "لا جريمة بغير سلوك"^(٢).

ويعد السلوك القائم في جريمة التعدي على البيانات الطبية الإلكترونية سلوكاً يشمل بين جنباته عدداً من الصور، إذ إن التعدي له مدلول عام، إذ إن كافة الجرائم الواردة في قوانين الجزاء جميعها تركز على فعل (التعدي)، والناظر إلى المادة (٢/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي سالف الذكر، يدرك أن السلوك الإجرامي يتمثل في الصور الآتية:

- إتلاف البيانات الطبية الإلكترونية: ويتم الإتلاف المعلوماتي في هذه الصورة بعدة أساليب، منها الحذف والمحو والإلغاء، أو إدخال برامج خبيثة كالفيروسات، وبرامج الدودة والقنابل المنطقية والزمنية، وقد يكون القصد من سلوك الإتلاف هو مجرد الحصول على منفعة أياً كان شكلها، علماً بأن سلوك الإتلاف الذي يتولى الجاني القيام به يعلم أنه سلوك غير مشروع^(٣).
- تعديل البيانات الطبية الإلكترونية: ويعد التعديل هنا كسلوك مجرم واضحاً جلياً لما يمكن تصوّره بشأن ما يحدث بخصوص البيانات الطبية الإلكترونية، ومن الأمور المسلم بها أن التعديل قد يكون بالحذف أو بالإضافة، وكلاهما يكون الغرض منه حصول نتيجة إجرامية، إذ إن القول بتعديل بيان طبي معين لما فيه صلاح أو خير لمريض معين أمر لا يمكن تصوّره، وإن كان ذلك بات تزويراً

(١) د. جلال ثروت، نظم القسم العام في قانون العقوبات، نظرية الجريمة، (مصر، دار الجامعة الجديدة، ٢٠١٠م)، ص ١٤٧.

(٢) د. فتوح عبد الله الشاذلي، شرح قانون العقوبات، القسم العام، الكتاب الأول، (مصر، دار المطبوعات الجامعية، ٢٠١٨م)، ص ٢٥٥ - ٢٥٦.

(٣) د. محمد عبد الرحمن عنانزة، القصد الجرمي في الجرائم الإلكترونية، الطبعة الأولى، (عمان: دار الأيام للنشر والتوزيع، ٢٠١٧م)، ص ١١٧.

مُعاقباً عليه، وعلى ذلك فالدخولُ إلى الشبكة المعلوماتية من أجل تعديل بيانٍ طبيٍّ مُعيّن، لا بدُّ أن يتمَّ على نحوٍ مشروع.

وإذا كانت هذه السلوكيات المُتقدّمة، والتي تدرجُ في النصِّ، هي الأكثرُ حصولاً في الواقع العمليِّ، إلا أنها لم تكنُ الوحيدة، بل إنَّ هناك عدداً من السلوكيات الأخرى التي عرضها النصُّ كما هو الحال بصدد الحصول على البيانات أو الاستحواذ عليها أو إنشائها أو تسريبها أو إلغائها أو حذفها أو نسخها أو نشرها أو إعادة نشرها، وذلك بغير تصريح أو موافقة ذوي الشأن، وعلى إثر حصر هذه السلوكيات، نقول: إنَّ هذه السلوكيات نُكرت على سبيل الحصر وليس على المثال؛ نظراً لعدم إمكانية التوسُّع في نطاق النصِّ، ولكن لماذا لم ينظِّم المشرِّعُ الإماراتيُّ ضمن السلوكيات المُتقدّمة، حالةَ تغيير البيانات الشخصية الطبية؟ وهل اكتفي بكون التغيير تعديلاً؟ وإن كانت وجهته على هذا النحو، فالأمرُ بطبيعة الحال لا بدُّ أن يُثير خلطاً؛ نظراً لأنَّ تغيير البيانات الطبية قد يكونُ تغييراً كاملاً، وبالتالي خرج عن نطاق التَّعديل، ولا يمكنُ حينئذٍ القولُ بأنَّ هناك تعديلاً^(١).

وهناك عددٌ من الأساليب المُستحدثة في إتلاف البيانات، يستوي في هذا المقام البيانات الطبية أو غيرها من البيانات، ومن هذه الأساليب التقنية التي تتمُّ بها عمليةُ الإتلاف هي^(٢): الفيروسات، وتتمثَّل في برامجٍ مُشفَّرةٍ تمَّ تصميمها بقدرةٍ على التكاثر والانتشار من نظامٍ إلى آخر، وذلك إما بواسطة قرصٍ مُمغنط أو عبر شبكة التَّصالات، وتشكِّل هذه الوسيلةُ التقنيةُ في مجال ارتكاب الجرائم المعلوماتية خطراً حقيقياً وتهديداً جدياً لكافة مستخدمي أجهزة الحاسوب وشبكات الإنترنت؛ وذلك نظراً للتزايد الهائل في حجم الاعتماد على تقنيات نظم المعلومات لدى الأفراد والمؤسسات، وما تولَّده هذه الوسيلةُ يتمثَّل في تدمير نظم المعلومات وقواعد البيانات، ولما كان للفيروس أغراضٌ متعدِّدة، البعض منها حمائيٌّ والبعض

(١) ويرجعُ السبب وراء ذلك إلى أنَّ اصطلاح التَّعديل يتسمُّ بالطابع الجزئيِّ، فلا يمكنُ أن يكونَ التَّعديلُ كاملاً للبيان، لذلك جرت العادةُ على أنَّ تعديل البيانات مقصودها إدخالُ ثمة بياناتٍ أخرى إليها أو تغيير جانبٍ بسيطٍ منها، ولكن اصطلاح التغيير قد يقعُ في بعض الأحيان كاملاً، وعلى سبيل القول تمَّ تغييرُ بيانات شخصٍ ما إلى بيانات شخصٍ آخر.

(٢) نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، (عمان - دار الثقافة للنشر والتوزيع)، ٢٠١٠م، ص ١٢٥ وما بعدها.

الآخر تخريبي، فإننا نرى أن أية وسيلة منهم أو غرض يحقق صور الإلتفاف يعد محققاً للسلوك المادي لجريمة الاعتداد.

أما الوسيلة التقنية الثانية فهي برامج الدودة، وهي برامج مصممة للانتقال عبر شبكات الاتصال من جهاز إلى آخر، وهو ما يؤدي إلى عجز النظام المعلوماتي عن أداء عمله عن طريق محو عدة أجزاء من المعلومات^(١).

أما الوسيلة التقنية الثالثة، فتتمثل في القنابل المنطقية والزمنية، والقنابل المنطقية هي برامج تظل خاملة إلى أن تتحقق لها بعض الشروط، فتتفجر وتدمر الملفات الموجودة داخل جهاز الحاسوب، وتعد هذه القنابل في حالة سكون، ولا يتم اكتشافها لمدة قد تطول وقد تقصر، ويتولى تحديد هذه المدة المؤشر الموجود داخلها، أما القنابل الزمنية أو كما يسميها البعض القنابل الموقوتة، وهي برامج يتم إدخالها بطرق مشروعة بتخفيه عند إدخالها مع برامج أخرى وتعمل على تحقيق الإلتفاف والتدمير في زمن معين؛ نظراً لأن الانفجار يتم في توقيت معين^(٢).

ثانياً: الركن المعنوي للجريمة:

يعد الركن المعنوي^(٣) هو الركن الثاني للجريمة المتقدمة، وفي إطار الحديث عن هذا الركن يجب التّويه بأن هذه الجريمة تعد من قبيل الجرائم العمدية الايجابية، وهي مثل سابقتها تأبى سلوكيات الامتناع، وعلى ضوء ذلك ولما كان القصد الجنائي مشكلاً من عنصر العلم والارادة، فإننا نفضل في هذا الخصوص كليهما، ثم نبين فيما إذا كانت هذه الجريمة من قبيل جرائم القصد العام أم الخاص، وهذا ما سنعرض له على النحو الآتي:

أولاً- عنصر العلم:

(١) لمزيد من التفاصيل، راجع: سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الأولى،

(القاهرة، دار النهضة العربية، ١٩٩٤م)، ص: ١٩٣ وما بعدها؛ راجع كذلك: هدى قشقوش، جرائم الحاسب

الإلكتروني في التشريع المقارن، الطبعة الأولى، (القاهرة، دار النهضة العربية، ١٩٩٢م)، ص: ١٢٢ وما بعدها.

(٢) راجع لمزيد من التفاصيل: نهلا عبد القادر المومني، الجرائم المعلوماتية، المرجع السابق، ص: ١٣٣؛ سامي الشوا،

ثورة المعلومات وانعكاساتها على قانون العقوبات، المرجع السابق، ص: ١٩٦ وما بعدها.

(٣) راجع: د/ جلال ثروت، نظم القسم العام في قانون العقوبات، المرجع السابق، ص ١٧٧ وما بعدها؛ د/ أمين مصطفى

محمد، قانون العقوبات - القسم العام، المرجع السابق، ص ٣٣٢ وما بعدها.

يعد علم الجاني مُتحققاً طالما كانت الجريمة عمديةً بالأمر الآتية:

١- علم الجاني بأن كافة السلوكيات المُقامة من جانبه، يستوي في ذلك إن كانت تعديلاً أو تغييراً أو إتلافاً، فجميعها سلوكيات يتولّى الجاني استخدامها وإعمالها دون وجه حقّ.

٢- علم الجاني بأن السلوكيات المُقامة من جانبه المقصد منها التعدي على حرية البيانات أو المعلومات الطبيّة.

٣- علم الجاني بأن عواقب فعلته وخيمة جداً؛ نظراً لأنّ تبديل أو تغيير تشخيص أو علاج بعينه قد يُؤدّي إلى اضطراب في الأنسجة وينتج عنه مرض قد ييأس الشفاء منه تجاه من يقصده "العلم بالنتيجة".

ثانياً- عنصر الإرادة:

والإرادة المقصودة - حسب تعبير الفقه - هي إرادة السلوك^(١)، أي لا بدّ حتى ينطبق النصّ المتقدّم أن يكون التغيير أو التعديل أو الإتلاف قد حصل بالفعل، بغضّ النظر عن مقدار جسامته، وبغضّ النظر عما إذا كانت الجريمة توقّفت عن حدّ الشروع من عدمه، طالما أنّ إرادة الجاني أو الجناة اتّجهت إلى إحداث ذلك، وفي هذا الصدد يثور التساؤل بصدد طبيعة الجريمة، ومدى اعتبارها من قبيل جرائم القصد العام من عدمه؟

وإزاء ذلك تعدّ جريمة تغيير أو إتلاف البيانات والمعلومات الطبيّة عمداً من جرائم القصد العام؛ نظراً لأنّ النصّ ذاته جاء خالياً من أيّ بيان يشير إلى قصدٍ خاصّ. ولكن لنا تجاه هذا الحديث رأيٌ جديرٌ بالاعتبار، ألا وهو أنّ الجريمة ينعقد لها القصد العام بتوافره، إلّا أنّنا نرى أنّ الهدف من سلوك الجاني الإجرامي لم يكن مجرد التوقّف عند عناصر القصد العامّ بحصول التعديل أو الإتلاف أو التغيير، فالجاني يُحاول الوصول من خلال هذه البيانات أو المعلومات الطبيّة بنية استعمالها والتعامل عليها، ممّا قد يُضفي عليها القصد الإجرامي الخاصّ، وهذا ما نودّ تأييده من جانب المشرّع.

(١) د/ جلال ثروت، نظم القسم العام في قانون العقوبات، نظرية الجريمة، المرجع السابق، ص ١٨١.

الفرع الثاني

العقوبات المقررة للجريمة

في نطاق الحديث عن العقوبة المقررة، بصدد جريمة التعدي على البيانات الشخصية، نرى أن المشرع الاتحادي الإماراتي في نطاق المادة (٢/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية عدّ المساس بهذه البيانات الطبية بمثابة ظرفٍ مُشدّد يتم على ضوءه تشديد العقاب، إلا أن الظرف المُشدّد الذي أورده النص يختلف عن الظروف المُشدّدة التي عرضت لها المادة (٦٠) من قانون مكافحة الشائعات والجرائم الإلكترونية^(١)، وعليه إزاء تفصيل الحديث بصدد هذه العقوبات نفرّق بين فرضين:

الفرض الأول: طائفة العقوبات التبعية المنصوص عليها بالمادة (٥٦) من قانون مكافحة الشائعات والجرائم الإلكترونية سالف الإشارة إليها، وكذلك ما في حكمها بموجب نص المادة (٥٩) بصدد التدابير الاحترازية^(٢)، إذ إنهما يتم تطبيقهما بقوة القانون دون حاجة إلى ضرورة إقرار ذلك في نطاق ما عولت عليه المادة (٢/٦) من ذات القانون سالف الإشارة إليه.

(١) تنص المادة (٦٠) من قانون مكافحة الشائعات والجرائم الإلكترونية على أنه "في تطبيق أحكام هذا المرسوم بقانون يعدّ ظرفاً مُشدّداً:

١- ارتكاب الجاني لأيّ جريمة منصوص عليها في هذا المرسوم بقانون بمناسبة أو بسبب تأدية عمله.
٢- استخدام الجاني شبكة المعلومات أو أيّ نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أيّ جريمة لم ينص عليها هذا المرسوم بقانون.

٣- ارتكاب الجاني أيّ جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو أيّ جماعة معادية أو جماعة إرهابية أو تنظيم غير مشروع.

(٢) تنص المادة (٥٩) من قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي الإماراتي على أنه: "التدابير الجزائية: يجوز للمحكمة عند الحكم بالإدانة في أيّ جريمة من الجرائم المنصوص عليها بهذا المرسوم بقانون أن تقضي بأيّ من التدابير الآتية:

١- الأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية أو حرمانه من استخدام أيّ شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أيّ وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة.

٢- إغلاق الموقع المخالف إغلاقاً كلياً أو جزئياً متى أمكن ذلك فنياً.

٣- حجب الموقع المخالف حجاً كلياً أو جزئياً للمدة التي تُقررها المحكمة.

الفرض الثاني: طائفة العقوبات الأصلية المتمثلة في عقوبتي الحبس والغرامة، والمنصوص عليهما في المادة (١/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية، والتي عدّها المشرّع في حالة المساس بالبيانات الطبية ظرفاً مُشدداً، بالرجوع إلى القواعد العامة، يُضاعف الحد الأقصى للعقوبة المقررة للجريمة، معنى ذلك أنّ عقوبة الحبس في القانون الإماراتي تصل إلى ٦ سنوات، كل ما هنالك أنه عوّل على المساس بالبيانات الشخصية الطبية، واعتبر أية صورة من صور التعدي عليها ظرفاً مُشدداً، لذلك فإننا نرى في هذا الخصوص أنّ العقوبات الواردة في نصّ المادة (١/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي الإماراتي تعدّ بمثابة حدّ أدنى يُعوّل عليه بصدد التعدي على البيانات الشخصية الطبية، مفاد ذلك اعتبار الحد الأقصى المنصوص عليه بالمادة (١/٦) من هذا القانون، حدّاً أدنى للتطبيق على حكم المادة (٢/٦) من ذات القانون، أو أنّ المشرّع يتفضّل متدخلًا بمعالجة هذا النصّ المتقدّم، أمّا المشرّع المصري فلم يتعرّض لمثل هذا التنظيم العقابي.

يُعاقب بالحبس مدّة لا تزيد على سنة أو بغرامة لا تزيد على (٥٠٠٠) خمسة آلاف درهم، كل من خالف أيّ تدبير من التدابير المحكوم بها، وللمحكمة أن تأمر بإطالة التدابير مدّة لا تزيد على نصف المدّة المحكوم بها ولا تزيد في أية حال على (٣) ثلاث سنوات أو أن تستبدل به تدبيراً آخر ممّا ذكر.

الخاتمة

أولتُ تشريعاتُ وقوانينُ دولة الإمارات العربية المتحدة اهتماماً كبيراً بحماية حقِّ الأفراد في الخصوصية بجميع أشكالها؛ نظراً لاعتماد الدولة على أنماط التكنولوجيا الرقمية والبنى التكنولوجية في الإدارة والاتصال والتي نتجَ عنها استحوادُ المؤسسات الحكومية والخاصة على كمياتٍ من البيانات الشخصية ينتجُ عنها إساءة الاستخدام بانتهاك الخصوصية، مما استدعى نظرَ المشرِّع في سنِّ التشريعات وتعديلاتها لمواكبة التقدم وتحديد الكيفية التي يتمُّ بها جمعُ وحفظُ ومعالجة البيانات التي يمكنُ أن تحتوي على معلوماتٍ خاصة بالأفراد بما يضمنُ حماية خصوصية المواطنين ويجرِّم جمع البيانات الشخصية بطرقٍ غير مشروعة في قانون مكافحة الشائعات والجرائم الإلكترونية رقم (٣٤) لسنة ٢٠٢١.

فقد جرِّم معالجة البيانات ونقلها وإفشاءها؛ بما قد يُعرضُ المواطنين لانتهاك حُرمة حياتهم الخاصة وحقيهم في الخصوصية، وبما يوضحُ أن المشرِّع قد وُفق في إيجاد التوازن للعلاقة المزدوجة بين حماية البيانات الشخصية للإنسان وحمايته من انتهاك الحقوق كمستخدم أو مُستهلك للأنظمة الإلكترونية، وأوجب على الشركات تنفيذَ مستوى مناسبٍ من الأمان، يشملُ عناصرَ التحكم في الأمان التقنية والتنظيمية؛ لمنع فقدان البيانات أو تسريب المعلومات أو عمليات معالجة البيانات غير المصرَّح بها الأخرى. كما يُشجِّع القانون العام لحماية البيانات (GDPR) الشركات على دمج مُتطلبات التشفير وإدارة الحوادث وسلامة الشبكة والنظام والتوافر والمرونة في برنامج الأمان الخاص بها.

أولاً: النتائج:

توصَّلَ الباحثُ من خلال الدراسة إلى النتائج التالية:

١- جاءت القوانين الاتحاديَّة الإماراتية في بيانها للبيانات الشخصية مقصورةً على الأشخاص الطبيعيين فقط دون الأشخاص الاعتباريين.

٢- جاء نصُّ المادة (١/٦) من قانون مكافحة الشائعات والجرائم الإلكترونية خالياً من النصِّ على سلوك "التغيير" ضمن السلوكيات التي أوردتها المشرِّع، على الرغم من أهمية هذا الاصطلاح في الواقع العملي.

٣- لم تُنظَّم السلطة التنفيذية لائحةً تنفيذيةً لقانون حماية البيانات الشخصية الاتحادي الإماراتي على الرغم من أن الزمنَ المخصَّص لإصدارها قد انقضى.

- ٤- تعدُّ علاقة السببية رابطةً غائيةً بصدد جرائم التّعديّ على البيانات الشخصية، وهي مُتحقّقة دائماً كون الجريمة المُتقدّمة من قبيل الجرائم العمديّة.
- ٥- أحسن المُشرّع الاتّحاديّ الإماراتُ صنعاً في تنظيم أحكام جريمة التّعديّ على البيانات الشخصية الطبيّة والمصرفيّة تنظيمًا كاملاً على غرار ما هو معمولٌ به في التّشريع المصريّ، لا سيّما وأنّ هذا الأخير لم ينظّم الجريمة المُتقدّمة بصورة كاملة.
- ٦- تعدُّ جريمة التّعديّ على البيانات الشخصية الطبيّة والمصرفيّة من قبيل جرائم القصد العامّ، وهي تتماثلُ في هذا المقام مع جريمة التعامل/ التّعديّ على البيانات الشخصية.
- ٧- عدم تشديد المُشرّع الإماراتيّ لعقوبة البيانات الشخصية لمُرتكبيها وعدّها من الجرائم الجنح، إضافةً إلى أنه اكتفى بتحديد حدّها الأدنى ولم يضع حدّاً أقصى للعقوبة.

ثانياً: التوصيات:

تتجلى توصيات الدّراسة في هذا المقام في الآتي:

١. نقترحُ على المُشرّع الاتّحاديّ الإماراتيّ تعديل نصّ المادة (١/٣) من قانون مكافحة الشائعات والجرائم الإلكترونيّة، وإدراج اصطلاح التغيير ضمن المُصطلحات التي قدّمها النصّ في هذا الخصوص.
٢. نقترحُ على السّلطة التنفيذيّة ممثّلةً في مجلس الوزراء ضرورة إصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية؛ نظراً لفوات الزمن المُحدّد لإصدارها.
٣. نقترحُ على المُشرّع الاتّحاديّ الإماراتيّ النّظر في مسألة البيانات الشخصية ومدى قصرها على الأشخاص الطبيعيين، لا سيّما وأنّ الشخص الاعتباري له من الخواصّ التي تتطابق مع الشخص الطبيعيّ، الأمر الذي نراه في حاجةٍ إلى تدخّل تشريعيّ للمعالجة.
٤. توعية الأفراد بضرورة الحفاظ على بياناتهم الشخصية واستعمالها بحذرٍ في الفضاء الرقميّ وتنبههم بالمخاطر التي تُحيط بها، والأضرار التي قد تُصيبهم من الإفراط في تداولها واستعمالها العشوائيّ، وذلك عن طريق مُختلف الوسائل التكنولوجيّة وإقامة الندوات العلميّة والدّراسات حول مضمون الحقّ في الخصوصية، والتمكين منه، وآليات حمايته واحترامه، ولا سيّما في البيئة الرقميّة.
٥. تشديد تجريم استخدام التّطبيقات من قبل العامّة وتطوير التّقنيّات وإتاحتها دون ضوابط أو تقنين.

٦. رغم خطورة الجرائم الماسة بالبيانات وتهديدها لحياة الأفراد، ورغم حجم الأضرار المادية والمعنوية التي تخلفها، فإنّ المشرّع أعطاهما وصفَ الجنحة وعقوبتها بسيطة؛ لهذا وجبَ مراجعة سياسة العقاب وتوقيع أشدها على بعض السلوكيات الخطيرة الماسة بالبيانات حتى يتحقّق نوعٌ من الردع.
٧. وضع حدودٍ لمعالجة البيانات الشخصية وحركتها إلى الخارج وتأمين ملفاتها وأصولها من خطر الانتهاك بفرض حقّ ملكيةٍ على المعطيات ذات الطابع الشخصي.
٨. وضع آلياتٍ منضبطةٍ تضمنُ عدمَ حدوثِ اختراقاتٍ واستخداماتٍ للبيانات الشخصية المعالجة تقنياً، وتكفل التصديّ للأخطار الناجمة عن تلك الاستخدامات غير المشروعة أو الانتهاكات لسريّتها.

قائمة المراجع والمصادر

أولاً: الكتب العامة:

١. جلال ثروت، نظم القسم العام في قانون العقوبات، نظرية الجريمة، (مصر، دار الجامعة الجديدة، ٢٠١٠م).
٢. فتوح عبد الله الشاذلي، علم الإجرام وعلم العقاب (الإسكندرية: دار المطبوعات الجامعية، ٢٠١٧م).
٣. فتوح عبد الله الشاذلي، شرح قانون العقوبات، القسم العام، الكتاب الأول، (مصر، دار المطبوعات الجامعية، ٢٠١٨م).
٤. فتوح عبد الله الشاذلي، شرح قانون العقوبات، القسم العام، الكتاب الأول، (الإسكندرية: دار المطبوعات الجامعية، ٢٠١٨م).
٥. محمد عبد الرحمن عنانزة، القصدُ الجرميُّ في الجرائم الإلكترونية، الطبعة الأولى، (عمان: دار الأيام للنشر والتوزيع، ٢٠١٧م).

ثانياً: الكتب المتخصصة:

١. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت - دراسة مقارنة، ط١، القاهرة، دار النهضة العربية، ٢٠٠٩م.
٢. روسكو باوند، ضمانات الحرية في الدستور الأمريكي، ترجمة: د/ لبيب شنب، ط١، الإسكندرية، منشأة المعارف، ١٩٧٣م.
٣. سارة شريف، خصوصية البيانات الرقمية، القاهرة: مركز دعم لتقنية المعلومات، ٢٠١٨.
٤. سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الأولى، (القاهرة، دار النهضة العربية، ١٩٩٤م).
٥. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي - دراسة مقارنة، (دار الجامعة الجديدة، الإسكندرية، ٢٠١٨م).
٦. ممدوح خليل البحر، حماية الحياة الخاصة في القانون الجنائي - دراسة مقارنة، ط١، القاهرة، دار النهضة العربية، سنة ١٩٨٣م.

٧. منى كامل تركي، الذكاء الاصطناعي والأنظمة الرقمية، دورها في العمل الأمني والعلاقات التعاقدية الدولية - دراسة تحليلية في تشريعات دولة الإمارات العربية المتحدة والقوانين المقارنة، دبي، الدولية للكتب القانونية والنشر والتوزيع، ط١، ٢٠٢٢.
٨. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، (عمان - دار الثقافة للنشر والتوزيع)، ٢٠١٠م.
٩. هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الأولى، (القاهرة، دار النهضة العربية، ١٩٩٢م).
١٠. وسيم شفيق الحجار: النظام القانوني لوسائل التواصل الاجتماعي، بيروت: المركز العربي للبحوث القضائية، ٢٠١٧م.
١١. يونس عرب: دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، عمان: ورقة عمل، نادي المعلومات العربي، ٢٠٠٢.

ثالثاً: الرسائل العلمية:

١. بارق منتظر عبد الوهاب، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني (رسالة ماجستير)، كلية الحقوق، الأردن: جامعة الشرق الأوسط، ٢٠١٧.
٢. خلود عبد الرحمن العبادي، العقوبات المجتمعية في التشريعات الجزائية الأردنية - واقع وطموح، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٥م.
٣. سليم جلد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقهاء الإسلاميين، مذكرة لنيل شهادة الماجستير في الشريعة والقانون، ٢٠١٢ - ٢٠١٣م، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران.
٤. ماجد رجب، التواصل الاجتماعي (رسالة ماجستير)، كلية أصول الدين، غزة: الجامعة الإسلامية، ٢٠١١.

رابعاً: المنشورات والأوراق العلمية والأبحاث:

١. أحمد بن محمد بن مشيع الثبيتي، المسؤولية الجنائية للصغير والمكروه والمجنون، بحث منشورٌ بمجلة الدراسات العربية، كلية دار العلوم، جامعة المنيا، ٢٠١٨م.
٢. أحمد فتحي سرور، الحق في الحياة الخاصة، بحثٌ مُقدمٌ لمؤتمر الحق في الحياة الخاصة بكلية الحقوق، جامعة الإسكندرية، سنة ١٩٨٧م.
٣. تومي يحيى: الحماية القانونية للمعطيات ذات الطابع الشخصي - دراسة تحليلية، مجلة الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد ٤، العدد ٢، ٢٠١٩.
٤. ثاني بن علي آل ثاني، الرقمنة وقانون حماية المعطيات ذات الطابع الشخصي، بحثٌ مُقدمٌ في المؤتمر العلمي الدولي: الرقمنة والقانون تطلعات المستقبل في الدول العربية، المُعقد يوم الجمعة والسبت ١٥ و١٦ يوليو ٢٠٢٢ بمدرج المُختار السوسي، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش.
٥. حيدر غازي فيصل، الحق في الخصوصية وحماية البيانات، مجلة كلية الحقوق، جامعة النهريين، ٢٠١٧م.
٦. خدوجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الإلكترونية - دراسة مقارنة، الأستاذ الباحث للدراسات القانونية والسياسية، ٢٠١٧م.
٧. سامية عبد الرازق خلف، التعدي على حرمة الحياة الخاصة باستخدام التكنولوجيا الحديثة، الدراسات القانونية - جامعة بغداد، ٢٠١٤م.
٨. سينثيا شاسينيو: الإطار القانوني لمعالجة البيانات الشخصية على مواقع التجارة الإلكترونية، باريس، ٢٠٠١م.
٩. شيماء عبد الغني عطا الله، تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية، بحثٌ منشورٌ بمجلة كلية القانون الكويتية العالمية، يونيو ٢٠١٥، العدد ١٠، السنة الثالثة.
١٠. أ.م. د. صباح سامي داود، صابرين إبراهيم رضا، عقوبة الغرامة البديلة لسلب الحرية، بحثٌ منشورٌ بعددٍ خاصٍ لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الثاني، المجلد (٣٦)، أيلول ٢٠٢١م، منشورٌ إلكتروني.

<https://jols.uobaghdad.edu.iq/index.php/jols/article/download/434/356/763>

١١. طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي - دراسة مقارنة، مجلة القانون والاقتصاد - ملحق خاص، العدد (الثاني والتسعون).
١٢. عزري الزين، العلاقة السببية كشرط لمسؤولية الإدارة في مجال العمران، بحث منشور بمجلة العلوم الإنسانية، العدد (٢٢)، جامعة منتوري، قسنطينة، الجزائر، ديسمبر ٢٠٠٤م.
١٣. علاء الدين عبد الله الخصاونة، فراس الكساسبة، نافي محمد درادكة، الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد رقم (٨)، العدد (٢)، جمادى الآخرة ١٤٣٢هـ/ يونيو ٢٠١١م.
١٤. فايز علي الأسود، القصد الجنائي في القانون والشريعة الإسلامية - فقه الإمام الشافعي كنموذج، مؤتمر الإمام الشافعي، منشور على الإنترنت.
١٥. فتيحة حزام، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لتمنراست، المجلد ٨، العدد ٤، لسنة ٢٠١٩.
١٦. فطيمة نساخ، حماية المعطيات ذات الطابع الشخصي في ظل العصر التكنولوجي والرقمي وفق قانون ٢٠٠٧/١٨ الجزائري، مجلة الاقتصاد والصحافة، المجلد (٨)، العدد ٢.
١٧. كيث غولدستين، أوهاد شيم توف، والسيد دان برازيريس، الحق في الخصوصية في العصر الرقمي، تقرير المفوض السامي لحقوق الإنسان، ٩ أبريل ٢٠١٨.
١٨. منى كامل تركي، جرائم انتهاك الخصوصية عبر وسائل التواصل الاجتماعي في التشريعات الاتحادية لدولة الإمارات العربية المتحدة - المؤتمر العلمي الدولي الثالث للإعلام عبر الوسائط الإلكترونية - الحق في الخصوصية ومواقع شبكات التواصل الاجتماعي.
١٩. منى كامل تركي، رقمنة الهوية الوطنية بين حماية المعطيات ذات الطابع الشخصي وتصميم النظام، بحث مقدم في المؤتمر العلمي الدولي - الرقمنة والقانون: تطلعات المستقبل في الدول العربية، المنعقد يومي الجمعة والسبت ١٥ و١٦ يوليو ٢٠٢٢ بمدرج المختار السوسي، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض، مراكش.

خامساً: الأحكام القضائية:

أحكام المحكمة الاتحادية العليا الإماراتية:

١. الطّعن رقم ١٢٣ لسنة ٢٢ قضائية، الأحكام الجزائية، بتاريخ ٣/١١/٢٠٠١م.
 ٢. الطّعن رقم ٨٢ لسنة ٢٦ قضائية، الأحكام الجزائية، بتاريخ ٨/١/٢٠٠٥م.
 ٣. الطّعن رقم ١٨ لسنة ٢٠١٦ قضائية، الدائرة الجزائية بتاريخ ٢١/٣/٢٠١٦م.
 ٤. الطّعن رقم ١٣٥٧ لسنة ٢٠٢١ قضائية، الدائرة الجزائية، بتاريخ ٢٢/٣/٢٠٢٢م.
- أحكام محكمة النقض المصرية:**

١. الطّعن رقم ١٨٨٠٧ لسنة ٨٥ قضائية، الدوائر الجنائية، جلسة ٢٠/١٢/٢٠١٧م.
٢. الطّعن رقم ١٢١٩٦ لسنة ٩٠ قضائية، الدوائر الجنائية، جلسة ٤/١٢/٢٠٢١م.
٣. الطّعن رقم ٢٠٦٦ لسنة ٨٩ قضائية، الدوائر الجنائية، جلسة ٦/٦/٢٠٢١م.

سادساً: القوانين والتشريعات:

١. الإعلان العالمي لحقوق الإنسان الصادر في ١٠/١٢/١٩٤٨ من الجمعية العامة للأمم المتحدة.
٢. التوجيه الأوروبي رقم ٤٦/٩٥ الصادر بتاريخ ٢٤ تشرين الأول ١٩٩٥ الخاص بحماية الأشخاص الطبيعيين تجاه معالجة البيانات الشخصية والانتشار الحر لهذه البيانات.
٣. القانون الاتحادي رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية الصادر بتعديل المرسوم بقانون اتحادي رقم ١٢ لسنة ٢٠١٦ والصادر بتعديل المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، والمعدل على القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات.
٤. مرسوم القانون الاتحادي رقم ٤٥/٢٠٢١ بشأن حماية البيانات الشخصية، دخل حيز التنفيذ بتاريخ ٢ يناير ٢٠٢٢.

الفهرس

٢	مُلخَص الدِّراسة.....
٤	مُقَدِّمة:.....
٥	أهمِّية الدِّراسة:.....
٥	إشكالِيَّة الدِّراسة.....
٦	أهداف الدِّراسة.....
٧	منهجِيَّة الدِّراسة.....
٧	خطة الدِّراسة.....
٧	المبحث الثاني: الحقوق والالتزامات المُتَّصلة بالبيانات.....
٨	المبحث الأول: ماهيَّة خصوصيَّة البيانات الشخصيَّة والمبادئ الأساسيَّة لحمايتها.....
٩	المطلب الأول: ماهيَّة خصوصيَّة المعلومات والبيانات الشخصيَّة وتطوُّرها.....
١٤	المطلب الثاني: المبادئ الأساسيَّة لحماية البيانات الشخصيَّة.....
١٧	المبحث الثاني: حقوق الشخص صاحب البيانات والتزامات المسؤول عن مُعالجتها.....
١٧	المطلب الأول: حقوق الشخص صاحب البيانات الخاضعة للمُعالجة.....
٢٢	المطلب الثاني: التزامات المسؤول عن مُعالجة البيانات الشخصيَّة.....
٢٦	المبحث الثالث: صور الحماية الجنائيَّة لخصوصيَّة البيانات الشخصيَّة.....
٢٦	المطلب الأول: التَّعدي على البيانات الشخصيَّة.....
٢٦	الفرع الأول: أركان الجريمة.....
٣٦	الفرع الثاني: العقوبات المُقرَّرة للجريمة.....
٤٠	المطلب الثاني: التَّعدي على البيانات الشخصيَّة الطبيَّة أو المصرفيَّة.....
٤١	الفرع الأول: أركان الجريمة.....

٤٧.....	الفرع الثاني: العقوبات المُقرَّرة للجريمة
٤٨.....	الخاتمة
٤٩.....	المراجع والمصادر
٥٧.....	الفهرس