الآثار القانونية لجائحة كورونا/ كوفيد ١٩ على حماية البيانات الشخصية

أ. إيمان خميس اليحيائي(*)
أ. د. عدنان إبراهيم سرحان(**)

الملخص

أدى انتشار جائحة كورونا/ كوفيد ١٩ والإجراءات المتبعة لمواجهته إلى الابتعاد عن التقارب الجسدي الملموس في تقديم مختلف الخدمات والأعمال في شتى الميادين، حيث فرضت إجراءات التباعد الاجتماعي المطبقة في مختلف دول العالم ومنها دولة الإمارات العربية المتحدة، الانتقال إلى العالم الرقمي أو الافتراضي. وقد استحدثت دولة الإمارات العديد من التقنيات والآليات الذكية لمواجهة فيروس كورونا المستجد، وذلك في سبيل الكشف عن الحالات المصابة بالفيروس والحالات المخالطة لها، وفرض الإجراءات اللازمة المتمثلة في الحجر الصحي للمصابين، وذلك لضمان عدم مخالطتهم لأفراد المجتمع بحيث يتم حصر الفيروس والحد من انتشاره، بالإضافة إلى استخدام التقنيات والآليات المستحدثة للاستمرار في تقديم خدمات الرعاية الصحية عن بعد . إلا أن التحول إلى الرقمية واستخدام التقنيات والآليات المستحدثة لمواجهة الفيروس أدى إلى زيادة المخاطر على البيانات الشخصية لمستخدي تلك التقنيات والآليات الحديثة والمستفيدين منها، لاسيما مرضى كورونا الذين توجب عليهم استخدام تلك التقنيات تحت طائلة العقوبة والمساءلة القانونية، بالإضافة إلى المخاطر المترتبة على تتبع ومراقبة الأفراد من خلال استخدام التطبيقات والآليات الذكية المستخدمة في تتبع مرضى كورونا ورصد أماكن تواجدهم بغرض التأكد من بقائهم في مكان العزل المقرر لهم وعدم مخالطة أشخاص آخرين، لاسيما وأن تقنيات الرصد الإلكتروني لا تقتصر على مرضى كورونا فحسب، وإنما دعت الجهات المعنية في الدولة كافة أفراد المجتمع إلى استخدام تلك التقنيات الحديثة. وفي ظل تزايد المخاطر على حماية البيانات الشخصية ارتأينا تسليط الضوء على القواعد القانونية المقررة لحماية البيانات الشخصية في ظل القانون الإماراتي، فبالرغم من عدم وجود قانون خاص بحماية البيانات الشخصية في الدولة إلا أن هنالك بعض القواعد

(*) الباحث الرئيسي: باحثة دكتوراه في القانون الخاص، جامعة الشارقة - دولة الإمارات العربية المتحدة.
(**) الباحث المشارك: أستاذ القانون المدني جامعة الشارقة - دولة الإمارات العربية المتحدة.

الحمائية الواردة في القواعد العامة للقانون، كما نصت التشريعات الصحية في الدولة على قواعد حمائية خاصة بالبيانات الشخصية للمرضى ومتلقي خدمات الرعاية الصحية، وهو ما يستوجب بيان تلك القواعد الحمائية ومدى كفايتها وفاعليتها في توفير الحماية القانونية للبيانات الشخصية لمرضى جائحة كورونا.

المقدمة

اجتاحت جائحة كورونا المستجد (كوفيد ١٩) العالم بأسره، وخلفت آثاراً واسعة على مختلف القطاعات في دولة الإمارات العربية المتحدة والعالم أجمع، وقد امتدت آثارها إلى كافة المجالات السياسية والاقتصادية والاجتماعية والقانونية، لاسيما في ظل الجهود المبذولة للسيطرة على الفيروس ومنع انتشاره.

وتتمثل أهم الآثار المترتبة على الجائحة في فرض إجراءات التباعد الاجتماعي وما نتج عنها من الانتقال إلى العالم الرقمي أو الافتراضي للتمكن من استمرارية تقديم الخدمات بمختلف أنواعها، وذلك دون الحاجة للتواصل الجسدي الملموس .

إلا أن الانتقال إلى العالم الافتراضي من خلال مختلف التقنيات والآليات المستحدثة في ظل الجائحة أدى إلى زيادة المخاطر على حماية خصوصية وسرية البيانات والمعلومات الشخصية، خصوصاً بيانات مرضى جائحة كورونا الذين توجب عليهم استخدام وسائل التقنية الحديثة لغايات العلاج أو التأكد من التزامهم بالإجراءات الاحترازية المطبقة عليهم في حال الحجر المنزلي، وغيرها من الإجراءات المقررة من الجهات الصحية المعنية في الدولة .

إشكالية البحث:

الظهور والانتشار الانفجاري لفيروس كورونا، والنتائج السلبية الجسيمة التي صاحبته على صحة الإنسان، وما استدعته من إجراءات الحجر والإغلاق التي اتخذتها جميع دول العالم لمنع انتشاره والتقليل من آثاره، دفعت أغلب المؤسسات العامة والخاصة، في سبيل الاستمرار في تقديم خدماتها، إلى الانتقال السريع إلى العالم الرقمي، دون أن تتاح لها الفرصة لاتخاذ المزيد من الاحتياطات لأمن مواقعها الإلكترونية، جاعلة من استمرار الخدمة أولوية على حساب أمن وسلامة المعلومات والبيانات التي تراجعت إلى المرتبة الثانية. كما إن مواجهة آثار الجائحة استدعى اللجوء إلى تقنيات وبرامج حديثة يستخدم بعضها لأول مرة، سواء أكان ذلك لأغراض العلاج أم مراقبة ومتابعة مرضى الفيروس ومخالطيهم، كل ذلك أدى إلى زيادة فرص الاعتداء على خصوصية البيانات الشخصية والاستخدام غير المشروع لهذه البيانات

على نحو ضار بأصحابها، مع وجود قصور في التشريعات القائمة للاستجابة لمتطلبات أمن المعلومات والبيانات الشخصية.

وعليه فإن إشكالية البحث الرئيسة تدور حول الإجابة عن التساؤل التالي:

ما هي الحماية القانونية التي وفرها المشرع الإماراتي لحماية البيانات الشخصية في ظل انتشار جائحة كورونا والانتقال السريع والمفاجئ إلى العالم الرقمي؟ وما مدى كفاية وفاعلية تلك الحماية في تحقيق خصوصية وسرية البيانات الشخصية للأفراد عموماً ولمرضى كورونا تحديداً ؟

أهمية البحث:

تبدو أهمية البحث في أنه يسلط الضوء على المخاطر التي تتعرض لها البيانات الشخصية في عصر كورونا، بشكل عام، وخصوصاً تلك المترتبة على اللجوء إلى تقنيات وبرامج حديثة لمواجهة آثاره، ومدى فاعلية التشريعات الاتحادية في دولة الإمارات في حماية تلك البيانات من الاعتداء أو التجاوز عليها. ويبين البحث في هذا الصدد عدم كفاية المنظومة التشريعية الإماراتية الحالية لتوفير الحماية الفعالة لتلك البيانات، مؤشراً على مواطن القصور، ومقترحاً التوصيات اللازمة لسد الخلل.

منهجية البحث:

اعتمدنا في إعداد هذا البحث على المنهجين الوصفي والتحليلي، من حيث وصف الحالة الراهنة الناتجة عن انتشار الفيروس والإجراءات التي اتخذتها دولة الإمارات العربية المتحدة لمواجهته، والتقنيات الحديثة التي لجأت إليها، وما رشح عن ذلك من مخاطر المساس بالبيانات الشخصية لمرضى الفيروس والاستخدام غير المشروع لهذه البيانات، مع تحليل التشريعات القائمة وبيان مدى كفايتها لمواجهة تلك المخاطر، وتقديم الحلول المناسبة للقصور في هذا المجال.

خطة البحث:

وقد وجدنا من المفيد تسليط الضوء على المخاطر التي تواجهها البيانات الشخصية في ظل جائحة كورونا.

وذلك من خلال بيان ماهية البيانات الشخصية محل الحماية، ومخاطر التقنيات الحديثة على حماية تلك البيانات والمعلومات الشخصية، والبحث في الحماية القانونية

للبيانات الشخصية لمرضى جائحة كورونا، وذلك من خلال النظر في القواعد الحمائية الواردة في القواعد العامة للقانون الإماراتي وتقييمها، بالإضافة إلى قواعد الحماية الواردة في التشريعات الصحية وبيان مدى كفايتها وفاعليتها في حماية البيانات الشخصية لمرضى جائحة كورونا. وسنبحث كل ذلك في مبحثين مستقلين، هما:

- المبحث الأول: المخاطر التي تواجهها البيانات الشخصية في ظل جائحة كورونا
- المبحث الثاني: الحماية القانونية للبيانات الشخصية لمرضى جائحة كورونا

المبحث الأول
المخاطر التي تواجهها البيانات الشخصية
في ظل جائحة كورونا

لبيان المخاطر التي تواجهها البيانات الشخصية في ظل انتشار فيروس كورونا المستجد (كوفيد ١٩)، يتوجب علينا بدايةً بيان ماهية البيانات الشخصية التي كفلت لها القوانين قواعد حمائية خاصة بها، وذلك من خلال تعريف تلك البيانات الشخصية محل الحماية وتحديد صورها.

كما يتوجب علينا تسليط الضوء على التقنيات والآليات المستحدثة في ظل انتشار الجائحة، لاسيما تلك المستخدمة في المجال الصحي، وبيان المخاطر المترتبة على استخدامها واللجوء إليها على حماية البيانات الشخصية، وعلى ذلك نقسم هذا المبحث إلى مطلبين:

- المطلب الأول: ماهية البيانات الشخصية محل الحماية
- المطلب الثاني: مخاطر التقنيات الحديثة على حماية البيانات الشخصية في ظل جائحة كورونا

المطلب الأول
ماهية البيانات الشخصية محل الحماية

تعد ماهية البيانات الشخصية محل الحماية من المسائل التي يفترض بيانها وتسليط الضوء عليها قبل الخوض في المخاطر المترتبة عليها والحماية القانونية الواردة بشأنها، حيث إن تحديد ماهية البيانات الشخصية يعد أمراً مبدئياً يجب أن يحدد ويوضع له إطار واضح لنتمكن بعدها من إبراز المخاطر التي تواجه تلك البيانات الشخصية وتحديد الأطر الحمائية التي وردت بخصوصها.

وللتفصيل في ماهية البيانات الشخصية محل الحماية سنتطرق لتعريف البيانات الشخصية وبيان أهم صورها، وذلك بتقسيم هذا المطلب إلى فرعين على النحو التالي:

- الفرع الأول: تعريف البيانات الشخصية
- الفرع الثاني: صور البيانات الشخصية

الفرع الأول
تعريف البيانات الشخصية

تعرف البيانات الشخصية بأنها: «المعلومات الخاصة بشخص طبيعي قابل للتعرف عليه»[١]، ويطلق على هذه البيانات شخصية أو خاصة كونها تتعلق بالشخص ذاته كإنسان، مثل الاسم والعنوان ورقم الهاتف وغيرها من المعلومات التي تأخذ شكل بيانات وثيقة الارتباط والالتصاق بكل شخص طبيعي معرف أو قابل للتعريف»[٢].

وقد تتعدد تسمية تلك المعلومات والبيانات فيطلق عليها البيانات الخاصة، أو البيانات الشخصية، أو المعلومات الاسمية[٣]، أو المعطيات الشخصية[٤] أو المعطيات ذات الطابع الشخصي[٥]، أو بيانات هوية الشخص[٦]، وكلها مرادفات للمعنى ذاته.

وفي ظل عدم صدور قانون خاص بحماية البيانات الشخصية في الدولة[٧]، فإنه يجدر بنا الرجوع، في شأن التعريفات التشريعية لهذه البيانات، إلى تعريفها وفقاً للقوانين المقارنة الخاصة بحماية البيانات الشخصية، فقد خصص المشرع الفرنسي تشريعاً لحماية البيانات الشخصية، وهو القانون رقم ٧ لسنة ١٩٧٨ المعدل بالقانون رقم

(١) حسام محمد نبيل الشنراقي، حماية البيانات الشخصية عبر الإنترنت، المجلة العربية للإدارة – المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، ملحق العدد ٢، مجلد ٣٨، ٢٠١٨، ص٩.

(٢) مصطفى بن قارة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، مجلة الندوة للدراسات القانونية، الجزائر، عدد ١٣، ٢٠١٧، ص ٧٦ .

(٣) المرجع السابق.

(٤) وردت هذه التسمية في قانون حماية المعطيات الشخصية التونسي رقم ٦٣ لسنة ٢٠٠٤.

(٥) وردت هذه التسمية في القانون المغربي رقم ٨–٩ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، صادر بتاريخ ١٨ فبراير ٢٠٠٩ .

(٦) وردت هذه التسمية في قرار مجلس الوزراء رقم ٣٢ لسنة ٢٠٢٠ بشأن اللائحة التنفيذية للقانون الاتحادي رقم ٢ لسنة ٢٠١٩ في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية، وذلك في المادة الأولى منه والتي تنص على: «بيانات هوية الشخص: البيانات أو المعلومات التي تدل على هوية الشخص سواء أكانت منفردة أم مجتمعة مع بيانات أو معلومات أخرى».

(٧) وفي هذا الصدد تجدر الإشارة إلى وجود مشروع قانون اتحادي لحماية البيانات الشخصية منذ عام ٢٠١٨، إلا أنه لم يصدر بعد، حيث أعلنت الهيئة العامة لتنظيم قطاع الاتصالات في الدولة عن إعداد مشروع قانون اتحادي جديد لحماية البيانات الشخصية للمستخدمين في دولة الإمارات يتكفل بحماية بيانات المستخدمين في الدولة . مقال بعنوان: مشروع قانون جديد لحماية البيانات الشخصية للمستخدمين، صحيفة الاتحاد، منشور بتاريخ ٢٢ يوليو ٢٠١٨، الموقع الإلكتروني للصحيفة: www.alittihad.ae، آخر زيارة للموقع: ١–١٠–٢٠٢٠.

٨٠١ لسنة ٢٠٠٤ الخاص بحماية البيانات الشخصية، وفي نطاق القوانين العربية فنجد بأن دولة تونس[١] وكذا المغرب[٢] قد أصدرتا قوانين خاصة بحماية البيانات الشخصية، كما أصدرت مؤخراً جمهورية مصر العربية قانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية. أما على صعيد القوانين الخليجية فقد انفردت دولة قطر بسن تشريع خاص لحماية البيانات الشخصية وذلك في القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية.

وبشأن تعريف البيانات الشخصية فقد ورد في المادة الثانية من القانون الفرنسي بأنه: «يعتبر بياناً شخصياً أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة، سواء تم تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه».[٣]

أما المشرع التونسي فقد أورد تعريف البيانات الشخصية تحت مسمى المعطيات الشخصية، وذلك بنصه على أن: «تعتبر معطيات شخصية على معنى هذا القانون كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصاً طبيعياً معرفاً أو قابلاً للتعريف بطريقة مباشرة أو غير مباشرة، باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانوناً»[٤].

---

(١) قانون حماية المعطيات الشخصية التونسي رقم ٦٣ لسنة ٢٠٠٤، صادر بتاريخ ٢٧ يوليو ٢٠٠٤، وهنالك مشروع قانون جديد متعلق بحماية المعطيات الشخصية رقم ٢٥ لسنة ٢٠١٨ إلا أنه لم يتم صدوره حتى الآن.

(٢) القانون المغربي رقم ٨-٩ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، صادر بتاريخ ١٨ فبراير ٢٠٠٩ .

(٣) المادة الثانية من القانون الفرنسي رقم ٧ لسنة ١٩٧٨ المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤ الخاص بحماية البيانات الشخصية. وتجدر الإشارة إلى أن المشرع الفرنسي تبنى الاتجاه الموسع لتعريف البيانات الشخصية في التعديل رقم ٨٠١ لسنة ٢٠٠٤، وبشأن القانون القديم رقم ٧ لسنة ١٩٧٨ فإنه يعطي للبيانات الشخصية تعريفاً ضيقاً، حيث عرفها بأنها : «أي معلومات تسمح بطريقة مباشرة أو غير مباشرة بتحديد هوية الأشخاص الطبيعيين»، فوفقاً للتعريف الحديث فإن البيانات الشخصية هي أي معلومة تتعلق بشخص طبيعي ما دام أن هذا الشخص محددة هويته، أو أنه من الممكن تحديد هويته بأية طريقة. أما وفقاً للتعريف القديم فإن البيانات الشخصية قاصرة فقط على المعلومات التي تسمح بتحديد هوية الشخص الطبيعي بطريقة مباشرة أو غير مباشرة. للتفاصيل أكثر حول هذا الموضوع، انظر: سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي، مجلة الحقوق، جامعة الكويت، مجلد ٣٥، عدد ٣، ٢٠١١، ص ٣٨٥ ومابعدها .

(٤) المادة الرابعة من قانون حماية المعطيات الشخصية التونسي رقم ٦٣ لسنة ٢٠٠٤ .

كما أورد المشرع المغربي تعريف البيانات الشخصية تحت مسمى المعطيات ذات الطابع الشخصي، وذلك بالنص على أن: « المعطيات ذات الطابع الشخصي هي كل معلومة كيفما كان نوعها بغض النظر عن دعامتها، بما في ذلك الصوت والصورة، والمتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه والمسمى بعده بالشخص المعني. ويكون الشخص قابلاً للتعرف عليه إذا كان بالإمكان التعرف عليه، بصفة مباشرة أو غير مباشرة، لاسيما من خلال الرجوع إلى رقم تعريف أو عنصر أو عدة عناصر مميزة لهويته البدنية أو الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية»[١].

وبشأن المشرع المصري فقد عرف البيانات الشخصية بأنها: «أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية»[٢].

أما فيما يتعلق بالمشرع القطري فقد عرف البيانات الشخصية بأنها: «بيانات عن الفرد[٣] الذي تكون هويته محددة، أو يمكن تحديدها بصورة معقولة، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى»[٤].

ويتبين من تعريف البيانات الشخصية التي أوردتها القوانين المذكورة أعلاه بأن أية معلومة تتعلق بشخص طبيعي تعتبر من البيانات الشخصية الخاضعة للحماية القانونية، طالما أن هذا الشخص الطبيعي محدد الهوية، أو من الممكن تحديد هويته بأي طريقة مباشرة أو غير مباشرة، وهو ما يوفر نطاقاً واسعاً من الحماية القانونية للبيانات الشخصية؛ بحيث لا تقتصر الحماية على المعلومات أو البيانات التي تحدد هوية الشخص بشكل مباشر كاسم الشخص وعنوانه وموطنه، وإنما تمتد لتشمل كافة البيانات التي من الممكن أن يتم من خلالها تحديد هوية الشخص بشكل غير مباشر كرقم الهاتف أو عنوان البريد الإلكتروني وغيرها.

(١) المادة الأولى من القانون المغربي رقم ٨-٩ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، صادر بتاريخ ١٨ فبراير ٢٠٠٩ .

(٢) المادة الأولى من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠.

(٣) الفرد: الشخص الطبيعي الذي تتم معالجة بياناته الشخصية الخاصة به . المادة الأولى من القانون القطري رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية.

(٤) المادة الأولى من القانون القطري رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية.

كما يتضح من التعريفات السابقة بأن التشريعات الخاصة بالبيانات الشخصية كفلت الحماية للبيانات الشخصية المتعلقة بالشخص الطبيعي فحسب، دون الشخص المعنوي الذي يعد مستبعداً من تطبيق أحكام قوانين حماية البيانات الشخصية. ولعل السبب في ذلك يعود إلى أن هذه القوانين توفر الحماية للبيانات الشخصية في إطار نظرية الحقوق الملازمة للشخصية، وتلك النظرية وجدت أساساً لحماية الشخص الطبيعي أي الإنسان، أما حماية حقوق الشخص المعنوي فتتم في حدود القواعد العامة للمسؤولية المدنية، بحيث يجب المحافظة على سرية الأعمال وأن تكون البيانات صحيحة وإلا انعقدت المسؤولية المدنية[1].

و تجدر الإشارة هنا إلى ضرورة الأخذ بتعريفات مرنة عند بيان معنى البيانات الشخصية، وهو ما سارت عليه غالبية التشريعات التي تضمنت تعريفاً خاصاً بالبيانات الشخصية، بحيث تسمح بتطبيق الحماية القانونية على أية صورة حديثة ومستجدة من صور البيانات الشخصية، لاسيما وأن التطور الذي نشهده بصورة مستمرة وتحديداً في المجال التقني والتكنولوجي ينبئ بظهور صور جديدة ومستحدثة للبيانات الشخصية .

كما نشيد بتوجه التشريعات المذكورة أعلاه في توسيع نطاق حماية البيانات الشخصية وذلك من خلال حماية البيانات الشخصية التي تؤدي بطريقة غير مباشرة إلى تحديد هوية الشخص، لاسيما وأن اقتصار الحماية القانونية على البيانات الشخصية التي يمكن من خلالها تحديد هوية الشخص بصورة مباشرة قد يؤدي إلى انتهاك خصوصية الأشخاص والتعدي على البيانات الخاصة بهم، وذلك لوجود بيانات شخصية لا تحدد هوية الشخص بطريقة مباشرة ومنفردة إلا أنه يمكن تحديد هوية الشخص من خلال جمع تلك البيانات وربطها ببعضها بعضاً.

ونأمل أن يحذو المشرع الإماراتي حذو التشريعات التي أوردت تعريفات مرنة وواسعة للبيانات الشخصية عند إصدار قانون حماية البيانات الشخصية – لاسيما في مشروع قانون حماية البيانات الشخصية الذي نرتقب صدوره قريباً –، وذلك لضمان توفير الحماية القانونية لكافة البيانات الشخصية التي يمكن من خلالها تحديد هوية الأشخاص سواء بصورة مباشرة أو غير مباشرة، وذلك لكافة صور البيانات الشخصية سواء المتعارف عليها في الوقت الراهن أو تلك التي من الممكن أن يتم استحداثها مستقبلاً.

(١) حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، العدد الأول، ١٩٩٠، ص ٢٠ .

الفرع الثاني
صور البيانات الشخصية

لا شك أن تحديد صور البيانات الشخصية على سبيل الحصر ليس بالأمر الممكن، ذلك أن البيانات الشخصية محل الحماية تتغير وتتطور بحيث قد يتم استحداث بيانات شخصية تخضع للحماية القانونية لم تكن كذلك من قبل، فعلى سبيل المثال أدى ظهور شبكة الإنترنت إلى اعتبار الرقم الخاص بالكمبيوتر الشخصي (IP)[١] ضمن البيانات الشخصية محل الحماية[٢]، وهو ما لم يكن كذلك في السابق لأنه لم يكن معروفاً أساساً؛ لذا فإن تحديد صور البيانات الشخصية محل الحماية يجب أن يأتي دائماً على سبيل المثال فقط لا الحصر، وفي هذا الصدد يجدر التأكيد على ضرورة وضع تعريفات تشريعية مرنة للبيانات الشخصية تسمح بإضافة البيانات الشخصية المستحدثة ضمن نطاق حماية البيانات الشخصية.

فيعد من قبيل البيانات الشخصية الخاضعة للحماية القانونية للشخص اسمه[٣] ولقبه، فالاسم هو الوسيلة المستخدمة لتفريد الأشخاص وتمييزهم عن غيرهم[٤]، وينقسم

---

(١) يعرف (IP) بأنه : «عنوان بروتوكول الإنترنت، وهو سلسة من أربعة أرقام (بين الرقم ٠ و ٢٥٥) تستخدم لتحديد جهاز الكمبيوتر المتصل بالإنترنت». محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، بحث منشور على الموقع الإلكتروني لجامعة بنها، جمهورية مصر العربية، الموقع الرسمي للجامعة: www.bu.edu.eg، آخر زيارة للموقع: ١٢-١٠-٢٠٢٠، ص ١٤ .

(٢) بالرغم من وجود خلاف حول مدى اعتبار الرقم الخاص بالكمبيوتر الشخصي (IP) بياناً شخصياً، انظر: الاتجاه المؤيد لاعتباره بياناً خاصاً: سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي، مرجع سابق، ص ٣٨٨ . ويميل الاتجاه الآخر إلى عدم اعتباره بياناً شخصياً لأنه لا يعرف إلا جهاز الحاسوب الذي يستخدمه الشخص ولا يمكن عن طريقه تحديد هوية المشترك عبر موقع الإنترنت إلا بعد الرجوع إلى السلطة المختصة، وهو ما أكدته محكمة النقض الفرنسية في حكمها الصادر بتاريخ ١٣ يناير ٢٠٠٩ . انظر: طارق جمعة السيد، الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، عدد ٢، ٢٠١٧، ص٩٤ .

(٣) وقد اعتبرت المذكرة الإيضاحية لقانون المعاملات المدنية الاتحادي أن اسم الشخص يعد حقاً من الحقوق الملازمة بصاحبه، وقد يتحول الاسم الشخصي إلى اسم تجاري له قيمة مالية وهذا أيضاً يحميه القانون». المذكرة الإيضاحية لقانون المعاملات المدنية الصادر بالقانون الاتحادي رقم ٥ لسنة ١٩٨٥ المعدل بالقانون الاتحادي رقم ١ لسنة ١٩٨٧، ص ٦٤.

(٤) وفاء حلمي، محاضرات في نظرية الحق، منشورات جامعة الزقازيق، مصر، ٢٠٠٧، ص ٦٨ .

إلى الاسم الأصلي[١] واسم الشهرة[٢] والاسم المستعار[٣]. ولا تقتصر الحماية القانونية على اسم الشخص فحسب وإنما تمتد لتشمل لقبه، ويعرف اللقب بأنه «اسم الأسرة أو العائلة التي ينتمي إليها الشخص وتنحدر أصوله منها»[٤]؛ إذ لا يكفي اسم الشخص وحده لتمييزه عن غيره من الأشخاص في المجتمع.

كما يعد صوت الشخص وصورته من قبيل البيانات الشخصية المكفولة بالحماية القانونية[٥]، فالتكنولوجيا الرقمية سمحت بأن تتم معالجتهما باستخدام برامج الكمبيوتر، بالإضافة إلى إمكانية إضافة نص إلى صورة معينة أو إضافة صوت لنص معين، فكل ذلك يؤدي إلى اعتبار الصوت والصورة بيانات شخصية يمكن معالجتها، ومن ثم فإنها تخضع للحماية القانونية[٦]. كما أن صوت الشخص وصورته يتمتعان بحماية قانونية باعتبار أن الحق في حماية الصوت والصورة يعتبر أحد مظاهر الحق في الخصوصية[٧]. والصوت والصورة يعدان من البيانات الشخصية التي تحتاج في عصرنا الحالي إلى الحماية أكثر من أي وقت مضى، لإمكان معالجتها والتلاعب بها على نحو ضار بصاحبها.

(١) «هو الاسم الرسمي الذي يتم ذكره في شهادة الميلاد والبطاقة الشخصية، وهو الاسم الذي يظهر في المعاملات الرسمية». سهير منتصر، النظرية العامة للحق، منشورات جامعة الزقازيق، مصر، ٢٠٠٦، ص ٦٦ .

(٢) «اسم يختلف عن الاسم الأصلي ويشتهر به الشخص بين الناس، ولا يرد ذكره في شهادة الميلاد أو البطاقة الشخصية». المرجع السابق .

(٣) «اسم يتخذه الإنسان لنفسه، غير اسمه الأصلي، وذلك بمناسبة نشاط معين مهني أو فني أو أدبي، وغالباً ما يكون الهدف من الاسم المستعار هو إخفاء الشخصية الحقيقية للإنسان، كالفنان أو الكاتب الناشئ الذي يريد اختبار مدى نجاح عمله قبل الكشف عن شخصيته الحقيقية». المرجع السابق.

(٤) حسام محمد نبيل الشنراقي، مرجع سابق، ص١٤.

(٥) وهو ما أكدته المادة ٢١ من مرسوم بقانون رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات والتي اعتبرت كل من الصوت والصورة من البيانات الشخصية الواقعة في نطاق الحماية .

(٦) وهو ما أكدته محكمة نقض أبو ظبي باعتبار صورة الشخص من البيانات الشخصية المكفولة بالحماية القانونية. محكمة نقض أبو ظبي، طعن رقم ٣٢ لسنة ٢٠١٧، تاريخ الجلسة ٧-٣-٢٠١٧، مشار إليه في: شبكة قوانين الشرق، www.eastlaws.com، آخر زيارة للموقع: ٩-١٠-٢٠٢٠ .

(٧) انظر أكثر حول هذا الموضوع: حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دار النهضة العربية، من دون سنة نشر، ص ٧٦ ومابعدها، وتجدر الإشارة إلى أن مفهوم البيانات الشخصية كان يقتصر على البيانات الاسمية للشخص، أما الصوت والصورة فقد بدأ اعتبارهما من البيانات الشخصية في توجه للجنة الحريات الفرنسية مستندة في ذلك إلى التوجيه الأوروبي الخاص بحماية البيانات الشخصية الصادر في ٢٤ أكتوبر ١٩٩٥، والذي اعتبر أن صوت الإنسان وصورته بيانات شخصية يمكن معالجتها وتستوجب حمايتها قانوناً. حسام محمد نبيل الشنراقي، حماية البيانات الشخصية عبر الإنترنت، مرجع سابق، ص١٤.

كما يعد من قبيل البيانات الشخصية للأفراد، عنوان الشخص، وحالته الاجتماعية، وخصائصه الجسمانية، وأرقامه الشخصية، وجنسيته وأصوله العرقية، وبيانات حساباته المصرفية وكافة المعلومات المتعلقة بأي وسيلة من وسائل الدفع الإلكتروني(١).

كما تعد البيانات البيومترية من قبيل البيانات الشخصية ونعني بها تلك البيانات التي تتعلق بجسم الإنسان وتختلف من شخص لآخر(٢)، كبصمة الأصابع، والخطوط العريضة لكف اليد، وتحليل الشبكية، وقزحية العين، والشبكة الوريدية للأصابع واليد، و شكل الوجه، وكذلك الحمض النووي. حيث تستطيع البيانات البيومترية أن تحدد بطريقة تقنية وفنية هوية الشخص من خلال تحويل صفة أو سمة سلوكية لشخص معين إلى بصمة رقمية، وتهدف هذه البيانات إلى إثبات انفراد الشخص بمظاهر ثابتة وغير قابلة للتغيير على جسده(٣).

كما تعد المعلومات الخاصة بالحالة الصحية للشخص من البيانات الشخصية المكفولة بالحماية القانونية، وتشمل كافة المعلومات أو البيانات المتعلقة بالفحوصات الطبية والتشخيص الطبي، وكذلك البيانات المتعلقة بأي نوع من أنواع العلاج أو الرعاية الطبية، بالإضافة إلى البيانات الواردة في السجلات الطبية المستخدمة في المجال الصحي.

وقد شددت بعض قوانين حماية البيانات الشخصية على حماية البيانات الصحية للأشخاص(٤)، واعتبرتها ذات طبيعة خاصة نظراً لأهميتها وحساسيتها وخصوصيتها؛

---

(١) للمزيد حول صور البيانات الشخصية، انظر: سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي، مرجع سابق، ص ٣٨٨ وما بعدها، وللمؤلف نفسه، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها، دراسة في القانون الإماراتي، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، كلية الحقوق، مصر، عدد ٦٧، ٢٠١٨، ص ٦٢٦ وما بعدها. وكذلك: حسام محمد نبيل الشنراقي، مرجع سابق، ص١٥ وما بعدها.

(٢) جبالي أبو هشيمة كامل، حماية البيانات الشخصية في البيئة الرقمية، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق، جامعة آسيوط، مصر، ١٢-١٣ أبريل ٢٠١٦، ص ٤ .

(٣) انظر أكثر حول هذا الموضوع: محمد أحمد المعداوي، مرجع سابق، ص ١٣ .

(٤) ومنها قانون حماية البيانات الشخصية القطري، وذلك في المادة ١٦ منه والتي تنص على أنه: «تعد بيانات شخصية ذات طبيعة خاصة، البيانات المتعلقة بالأصل العرقي، والأطفال، والصحة أو الحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقة الزوجية، والجرائم الجنائية». كما قد أفرد لها المشرع الفرنسي نصاً خاصاً وذلك في المادة ٨ من قانون البيانات الشخصية، والتي نصت على أنه: « البيانات الشخصية التي ترتبط بشكل مباشر أو غير مباشر بالأصول العرقية أو الجينية أو بالآراء السياسية أو الفلسفية أو الدينية أو النقابية أو الصحة أو الحياة الجنسية للأفراد». كما نص قانون حماية البيانات الشخصية المصري على أن البيانات المتعلقة بالحالة الصحية للشخص تعد من البيانات الشخصية الحساسة، وذلك في المادة الأولى منه، والتي نصت على أنه: (البيانات الشخصية الحساسة هي البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية).

لأنها تعد من البيانات الشخصية السرية التي غالباً ما يرفض الأشخاص أن يتم الاطلاع عليها من قبل الآخرين .

المطلب الثاني

مخاطر التقنيات الحديثة على حماية البيانات الشخصية في ظل جائحة كورونا

انتشار جائحة كورونا وفرض إجراءات التباعد الاجتماعي أوجب الانتقال من العالم الحقيقي إلى العالم الافتراضي أو الرقمي، وهو ما استتبع إنتاج كميات هائلة من البيانات الشخصية، وتعاظمت على إثره المخاطر التي تترتب على إدارتها والحفاظ على سريتها وخصوصيتها. لاسيما في ظل تطور الوسائل المستخدمة لاختراق أنظمة المعلومات واستحداث طرق ووسائل قادرة على اختراق الأنظمة ونقل كميات هائلة من البيانات في غضون ثوان معدودة، فقد أثبتت الدراسات إمكانية نقل ما يقارب ١٧٨ تيرابايت من البيانات والمعلومات خلال ثانية واحدة فقط[١].

وقد أثبتت الإحصائيات بأن ما يقارب مليونين ونصف مستخدم من مستخدمي شبكة الإنترنت في دولة الإمارات العربية المتحدة قد وقعوا ضحية للجرائم المرتكبة عبر وسائل تقنية المعلومات في غضون عام واحد[٢].

أضف إلى ذلك فإن التحول إلى الرقمية لم يقتصر على جانب أو مجال معين، فالتقنيات ووسائلها الحديثة تستخدم في كافة القطاعات، سواء على مستوى العمل عن بعد في الجهات والمؤسسات الحكومية والخاصة، والتعليم عن بعد في كافة مدارس الدولة وجامعاتها، بالإضافة إلى أعمال الشركات والمؤسسات الخاصة التي تتم عن بعد باستخدام مختلف وسائل التقنية الحديثة.

---

(١) حيث حقق فريق من المهندسين في جامعة كوليدج لندن رقماً قياسياً عالمياً في سرعة نقل البيانات، بمعدل ١٧٨ تيرابايت في الثانية الواحدة، وذلك بعدما نجحوا في استخدام تقنيات مكبر الصوت في تعزيز قوة الإشارة وتسريع الإرسال، ويشبه ذلك تنزيل كل مكتبة مسلسلات نتفليكس في أقل من ثانية، وهو ما حطم الرقم القياسي لأسرع معدل نقل بيانات في العالم. مقال بعنوان: فريق بريطاني يبتكر أسرع شبكة إنترنت، صحيفة البيان، منشور بتاريخ: ٢٤ أغسطس ٢٠٢٠، الموقع الإلكتروني للصحيفة: www.albayan.ae ، آخر زيارة للموقع: ١٠-١٠-٢٠٢٠ .

(٢) وذلك في تقرير نورتن لعام ٢٠١٥ والذي تمت الإشارة إليه في: محمد خليفة الغفلي، ندوة الجرائم الإلكترونية في فترة التعقيم الوطني، غرفة تجارة وصناعة عجمان، بتاريخ ٢٣ سبتمبر ٢٠٢٠، ندوة إلكترونية عبر برنامج زوم: zoom .

كما شمل التحول إلى الرقمية والعالم الافتراضي جانب الرعاية الصحية والخدمات الطبية، وهو ما سنسلط عليه الضوء في هذه الدراسة، حيث اتجهت الجهات الصحية المعنية في الدولة إلى استحداث وسائل وتقنيات إلكترونية حديثة لمواجهة جائحة كورونا. وهذا يستوجب منا بيان تلك التقنيات والآليات المستحدثة في ظل جائحة كورونا، ومخاطر تلك التقنيات الحديثة على حماية البيانات الشخصية، وعلى ذلك نقسم هذا المطلب إلى فرعين على النحو الآتي:

- الفرع الأول: التقنيات والآليات المستحدثة في ظل جائحة كورونا
- الفرع الثاني: مخاطر التقنيات الحديثة على حماية البيانات الشخصية

الفرع الأول

التقنيات والآليات المستحدثة في ظل جائحة كورونا

لجأت العديد من دول العالم إلى استحداث تقنيات وآليات ذكية لاستخدامها في ظل انتشار جائحة كورونا، وذلك بهدف الكشف عن المرضى المصابين بالفيروس، أو مراقبتهم وتحديد موقعهم وضمان عدم مخالطتهم لأشخاص آخرين، أو غيرها من المتطلبات التي دعت إلى استحداث تقنيات وآليات تعتمد على استخدام الذكاء الاصطناعي. وقد كانت دولة الإمارات العربية المتحدة من الدول السباقة في هذا المجال[1]، وذلك باللجوء إلى العديد من الحلول الذكية للكشف عن حالات الإصابة بفيروس كورونا المستجد، وتتبعه، والسيطرة على انتشاره. وكان من أهم التقنيات والآليات المستحدثة في الدولة ما يعرف بتطبيقات الرصد الإلكتروني وهي تطبيقات ذكية يتم تحميلها عبر الهواتف المحمولة ليتم من خلالها مراقبة المستخدم وتحديد المخالطين له باستخدام خاصية البلوتوث .

كما لجأت الدولة إلى استحداث تقنيات تتمثل في ساعات وأساور إلكترونية يتم من خلالها مراقبة المرضى المصابين بفيروس كورونا المستجد ممن تقرر خضوعهم للعزل الصحي المنزلي؛ وذلك بهدف مراقبتهم وتتبعهم من قبل الجهات الصحية المعنية وضمان عدم مغادرتهم لمنازلهم ومخالطة أفراد المجتمع مما يجعلهم عرضة للإصابة بالفيروس .

أضف إلى ذلك استحدثت الدولة تقنيات وآليات ذكية لتشخيص وعلاج الحالات المرضية في ظل انتشار جائحة كورونا، وقد تم تخصيص بعض منها لتشخيص أعراض

(١) الموقع الإلكتروني للبوابة الرسمية لحكومة دولة الإمارات، https://u.ae/ar-AE#/، آخر زيارة للموقع: ١٢-١٠-٢٠٢٠ .

الإصابة بفيروس كورونا المستجد تحديداً، وذلك على خلاف بعض التقنيات والتطبيقات الذكية الأخرى التي تم إطلاقها لكافة أفراد المجتمع لتشخيص وعلاج مختلف الأمراض التي يعانون منها .

وتجدر الإشارة إلى أن مرضى كورونا الذين انطبقت عليهم شروط استخدام التقنيات الحديثة، ملزمون باستخدامها بذات الشروط والإجراءات المعتمدة من الجهات الصحية المختصة، لاسيما من كان منهم مشمولاً بالعزل المنزلي والذين يتوجب عليهم تحميل برنامج أطلق عليه مسمى « الحصن»، واستخدام سوار الرصد الإلكتروني لضمان بقائهم في منازلهم وعدم تعريض الآخرين لخطر العدوى بالفيروس(١).

الفرع الثاني

مخاطر التقنيات الحديثة على حماية البيانات الشخصية

لاشك أن لجوء الدول – وتحديداً دولة الإمارات العربية المتحدة – إلى استخدام الوسائل التكنولوجية والتقنية الحديثة، قد أسهم بشكل إيجابي في تطوير العديد من القطاعات والأنشطة على الصعيدين الداخلي والخارجي، لاسيما في ظل توجه سياسة دولة الإمارات إلى تطوير القطاع التكنولوجي والتقني واستخدامه في مختلف المجالات والقطاعات في الدولة، ومنها التوجه نحو الحكومة الذكية(٢)، والعمل والدراسة عن بعد، وإدخال تطبيقات الذكاء الاصطناعي في مختلف القطاعات، وغيرها من وسائل وأساليب التحول إلى الرقمية في مختلف المجالات. وقد تجلت الحاجة إلى التقنيات الحديثة والوسائل التكنولوجية الذكية في ظل انتشار جائحة كورونا، وهو ما جعل الدولة تستحدث تقنيات وآليات حديثة – كما سبق بيانه – لمواجهة فيروس كورونا المستجد والحد من انتشاره.

إلا أن التحول إلى الرقمية واستخدام التقنيات والآليات الحديثة لمواجهة الفيروس أدى إلى زيادة المخاطر على البيانات الشخصية لمستخدي تلك التقنيات والآليات

(١) المرجع السابق .

(٢) «الانتقال إلى الحكومة الذكية هو من المصطلحات الجديدة على المستوى المحلي والعربي، حيث نادى به سمو الشيخ محمد بن راشد رئيس مجلس الوزراء حاكم دبي باتجاه حكومة دبي نحو تطبيقات الحكومة الذكية والتي تقدم خدماتها للمواطنين على مدار الساعة دون توقف، ونقصد هنا بالحكومة الذكية تحويل العمل الإلكتروني للحكومة إلى تطبيقات إلكترونية على أجهزة الهواتف النقالة الحديثة، وتعتبر هذه النقلة بمثابة المواكبة للدول المتقدمة إلكترونياً ومنها ماليزيا التي أعدت سبعة مشاريع خاصة بتطبيقات الحكومة الذكية». سرحان حسن المعيني، جرائم التطبيقات الذكية، أكاديمية العلوم الشرطية، الشارقة، دولة الإمارات العربية المتحدة، ٢٠١٦، ص ١٨ .

المستحدثة والمستفيدين منها، لاسيما مرضى كورونا الذين توجب عليهم استخدام تلك التقنيات الحديثة تحت طائلة العقوبة والمساءلة القانونية.

ومن الملاحظ في هذا الصدد وجود تناقض بين حق الدولة في استخدام التقنيات الحديثة لمواجهة فيروس كورونا المستجد والحد من انتشاره من جهة، وحق مستخدمي تلك التقنيات وتحديداً المصابين بالفيروس في حماية بياناتهم الشخصية والحفاظ على سريتها من جهة أخرى. أضف إلى ذلك وجود تناقض بين حق الشخص في حماية بياناته الشخصية وعدم الإفصاح عنها، وبين التزامه من جهة ومصلحته في كشف تلك البيانات لاستخدام التقنيات المستحدثة والاستفادة من مزاياها وفاعليتها في مواجهة الفيروس، فنجد على سبيل المثال مصلحة الأفراد في تحميل تطبيق الحصن والمتمثلة في تمكنهم من معرفة نتائج اختبارات الكشف عن الفيروس التي يتم الاطلاع عليها من خلال التطبيق بعد مدة زمنية معينة من إجراء الاختبار، كما يمكن للأفراد الاستفادة من التطبيق من خلال تتبع الحالات المصابة ومعرفة ما إن كان الفرد قد خالط أحد المصابين بما يجعله عرضة للإصابة بالفيروس. إلا أن الاستفادة من تلك التقنيات الحديثة يستوجب الإفصاح عن البيانات الشخصية وذلك من خلال التسجيل في التطبيق الذكي باستخدام رقم الهوية الإماراتية ورقم الهاتف المحمول، ومن ثم يتم استخراج كافة البيانات المتعلقة بالفرد من خلال البيانات المسجلة لدى الجهات المعنية والمرتبطة بالهوية الإماراتية، فيجد الشخص صورته الشخصية وكافة البيانات الخاصة به قد ظهرت على التطبيق الذكي.

كما يشترط كذلك للاستفادة من تطبيق الحصن أن يتم تشغيل خاصية البلوتوث لتحديد موقع المستخدم ورصد تحركاته ومعرفة الأفراد الذين يكونون على قرابة منه، بالإضافة إلى السماح للتطبيق بالولوج لكاميرا الهاتف والميكروفون لضمان عمل التطبيق بالشكل الأمثل.

في ظل وجود هذه التناقضات يمكن أن توجد العديد من المخاطر التي تواجه البيانات الشخصية في ظل استخدام التقنيات والآليات الذكية، وتحديداً المستحدثة في ظل انتشار جائحة كورونا، ففرصة الوصول إلى البيانات الشخصية بطريقة غير مشروعة أصبحت أكثر سهولة وإمكانية في ظل توافر قواعد البيانات وبنوك المعلومات وغيرها من مصادر المعلومات التي يتم استخدامها في التقنيات الحديثة، أضف إلى ذلك الخطورة المتمثلة في تتبع الأشخاص ومراقبتهم باستخدام الآليات المستحدثة لتتبع مرضى كورونا ورصد تحركاتهم.

الغصن الأول: المخاطر المترتبة على استخدام البيانات الشخصية بطريقة غير مشروعة:

خلقت التقنيات والآليات الحديثة تحديات جديدة في مواجهة حماية البيانات الشخصية، من خلال زيادة كمية البيانات وإتاحة وعولمة المعلومات والاتصالات، وبالتالي زيادة احتمالية فقدان المركزية وآليات السيطرة والتحكم من قبل الجهات المعنية، وهو ما جعل تهديد التطور التكنولوجي أو المعلوماتي للبيانات الخاصة للأفراد واقعاً ملموساً، استطاع التغلب على الموانع المادية وعوائق المسافة(١).

فالتقنيات الحديثة مرتبطة بقواعد البيانات وبنوك المعلومات الموجودة لدى الجهات الحكومية المعنية بتلك التقنيات والآليات المستحدثة، سواء أكان ذلك في القطاع الصحي أو القطاع الأمني أو غيرها من الجهات المختصة، وهو ما أدى إلى أن المعلومات الشخصية التي كانت منعزلة ومتفرقة يصعب التوصل إليها، غدت مجمعة ومتوافرة بشكل يتيح الوصول إليها واستخدامها بسهولة، بطريقة مشروعة وغير مشروعة، فالبيانات الشخصية الموجودة في قواعد البيانات المرتبطة بالأجهزة الذكية المتصلة بشبكة الإنترنت، تكون هدفاً سهلاً لعمليات القرصنة التي تتم عبر النظم المعلوماتية، بحيث يمكن الولوج إلى تلك القواعد وسرقة البيانات الشخصية الموجودة فيها واستخدامها بشكل غير مشروع أو بيعها لجهات أخرى والاستفادة منها، كلما كان تأمين تلك القواعد ضعيفاً(٢).

ومن المخاطر التي تتعرض لها البيانات الشخصية إمكانية الاطلاع على البيانات السرية من قبل الغير دون وجود تصريح بذلك، كما قد يصاحب الاطلاع غير المشروع على تلك البيانات مخاطر إجراء العديد من التدخلات التي تتم على البيانات الشخصية كالإلغاء، والحذف، والتدمير، والإفشاء، والإتلاف، والتغيير، والنسخ، والنشر، وغيرها(٣).

أضف إلى ذلك المخاطر المتمثلة في أن المعلومات الرقمية ليس لها وقت نهائي فهي لا تتقادم ولا تنتهي، وهو ما يمكنها من معاودة الظهور في أي وقت لاحق على تجميعها أو

(١) أحمد جاد منصور، ضمانات الحق في حرمة الحياة الخاصة في المواثيق الدولية لحقوق الإنسان والقوانين الوطنية، المجلة العربية للإدارة – المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، إصدار خاص، ٢٠١٣، ص٨٩.

(٢) سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي، مرجع سابق، ص٤٠٥.

(٣) المادة ٣ من قانون مكافحة جرائم تقنية المعلومات.

تخزينها، بالرغم من أن حياة الشخص الذي تتعلق به تلك البيانات من المحتمل أن تكون قد تغيرت ولم تعد بياناته صالحة للظهور(١).

وفيما يتعلق تحديداً بالتقنيات والآليات المستحدثة لمواجهة فيروس كورونا، فإن الانتقال السريع لاستخدامها كان له دور بارز في زيادة المخاطر على البيانات الشخصية، ذلك أن الانتقال السريع لاستخدمها لم يتح المجال للجهات المعنية لتوفير بنية تحتية كافية لضمان سرية البيانات الشخصية وعدم السماح باختراقها لغايات الغش والاحتيال، فالحاجة إليها تعاظمت بصورة فجائية وسريعة لمواجهة تداعيات الجائحة، الأمر الذي وضع الاستمرار في تقديم الخدمة في المقام الأول لتتراجع خلفه مسألة أمن المعلومات.

كما سبق وأن شهدت محاكم الدولة العديد من عمليات اختراق الأجهزة الذكية والأنظمة المعلوماتية التابعة لمختلف الجهات والمؤسسات الحكومية والخاصة في الدولة، فقد تم اختراق نظام المعلومات الخاص بإحدى الجامعات الطبية الخاصة في الدولة وسرقة المعلومات والبيانات السرية الخاصة بها(٢).

وفي نطاق الجهات والمؤسسات الحكومية فقد تعرضت مؤسسة الإمارات للاتصالات لعملية قرصنة تم خلالها الاطلاع على البيانات الشخصية الخاصة بعدد من موظفي المؤسسة والاستيلاء على نسخ من تلك البيانات السرية(٣). كما تم اختراق الشبكة المعلوماتية الداخلية بوزارة شؤون الرئاسة في أبو ظبي، وذلك باستخدام أدوات وبرمجيات تسمح باختراق الشبكة والاطلاع على البيانات السرية الموجودة بداخلها(٤).

وعليه يمكن القول بأن استخدام التقنيات والوسائل الإلكترونية المستحدثة في ظل جائحة كورونا والمرتبطة بقواعد البيانات والشبكات المعلوماتية تشكل خطورة كبيرة على حماية البيانات الشخصية، حتى وإن كانت تلك القواعد التي تحوي المعلومات الشخصية تابعة لجهات ومؤسسات حكومية كتلك التابعة للقطاع الصحي أو القطاع الأمني أو

(١) وليد السيد سليم، ضمانات الخصوصية في الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، ٢٠١٢، ص٢١٩.

(٢) المحكمة الاتحادية العليا، طعن رقم ٦٦٧ لسنة ٢٠١٦، تاريخ الجلسة ١٠-٤-٢٠١٧، مشار إليه في: شبكة قوانين الشرق، www.eastlaws.com، آخر زيارة للموقع: ٩-٩-٢٠٢٠ .

(٣) محكمة تمييز دبي، طعن رقم ٢٣٠ لسنة ٢٠٠١، تاريخ الجلسة ٨-١٢-٢٠٠١، مشار إليه في: شبكة قوانين الشرق، www.eastlaws.com، آخر زيارة للموقع: ٩-٩-٢٠٢٠ .

(٤) محكمة نقض أبو ظبي، طعن رقم ٧٦٩ لسنة ٢٠١٠، تاريخ الجلسة ٩-١١-٢٠١٠، مشار إليه في: شبكة قوانين الشرق، www.eastlaws.com، آخر زيارة للموقع: ٩-٩-٢٠٢٠ .

غيرها من الجهات المعنية بمكافحة جائحة كورونا، فتلك البيانات الشخصية ليست بمنأى عن مخاطر اختراقها واستغلالها بطريقة غير مشروعة.

الغصن الثاني: المخاطر المترتبة على تتبع ومراقبة مرضى كورونا:

استخدمت العديد من الدول، ومنها دولة الإمارات العربية المتحدة، تطبيقات وآليات ذكية لتتبع مرضى كورونا ورصد أماكن تواجدهم، بغرض التأكد من بقائهم في مكان العزل المقرر لهم، وعدم مخالطة أفراد المجتمع مما يعرضهم للإصابة بالفيروس. كما استخدمت الدولة أساور وساعات إلكترونية تعزز نظام التتبع المرتبط بتلك التطبيقات الذكية، ولم تقتصر تطبيقات الرصد الإلكتروني على مرضى كورونا فحسب، فقد دعت الجهات الحكومية المعنية في الدولة بمكافحة فيروس كورونا المستجد كافة أفراد المجتمع لتحميل تطبيق الحصن. ويتم تفعيل تلك التقنيات بالتعاون مع شركات الاتصالات الهاتفية والشركات المصنعة للهواتف الذكية الذين يملكون الوسائل التقنية لمتابعة تحركات الأفراد عبر التتبع الجغرافي من خلال تطبيقات رقمية فائقة السرعة، وبناء على طلب الجهات الحكومية المعنية في الدولة فإنه يمكن تفعيل تلك البرامج والتطبيقات لمراقبة وتتبع الأفراد[1].

وبالرغم من مميزات تطبيقات التتبع والرصد الإلكتروني في مجال تعقب حالات الإصابة بفيروس كورونا المستجد والتحذير منها، إلا أن الخطر في تلك التطبيقات يكمن في أنه بمجرد تحميل الشخص للتطبيق والتسجيل فيه، فإنه بذلك يكون قد أعطى موافقة ضمنية على تتبعه ورصد تنقلاته وأماكن تواجده على مدى أربع وعشرين ساعة . وفي هذا الصدد بينت منظمة حقوق الإنسان بأن هنالك مخاطر ومخاوف بشأن انتهاك حقوق الإنسان من خلال استخدام الحكومات وشركات القطاع الخاص في العديد من الدول لتطبيقات تتبع ورصد تحركات الأفراد بهدف احتواء انتشار جائحة كورونا، وقد أشارت إلى أن الخطورة تكمن في استخدام برامج تحديد التموضع الجغرافي للأشخاص، مشيرة إلى أن ذلك قد يقود إلى انتهاكات جسيمة، نظراً لأنه يجعل العديد من المعلومات الشخصية الحساسة متاحة للعديد من الجهات، وهو ما يمكن معه استغلال تلك البيانات ضد الأشخاص في مرحلة ما[2].

---

(١) التطبيقات الذكية حين تسهم في ردع كورونا وتخترق خصوصيتنا، مقال منشور على موقع أخبارنا، www.arabic.euronews.com، بتاريخ: ٢٥ مارس ٢٠٢٠، آخر زيارة للموقع: ٥-٨-٢٠٢٠.

(٢) الموقع الرسمي لمنظمة حقوق الإنسان، www.hrw.org، اخر زيارة للموقع: ٩-٩-٢٠٢٠.

وعلى الرغم من تأكيد العديد من السلطات والجهات الحكومية التي لجأت إلى استخدام تطبيقات الرصد الإلكتروني، على أن المعلومات المسجلة عن الأفراد والتي تتيحها تلك البرامج و التطبيقات، ستبقى سرية ولن يسمح بالكشف عنها لأي جهة غير مختصة، إلا أنه لا يمكن ضمان سرية البيانات والمعلومات بشكل تام؛ ذلك أن الأنظمة المعلوماتية والتطبيقات الذكية معرضة دوماً لعمليات السرقة والاحتيال[١].

المبحث الثاني

الحماية القانونية للبيانات الشخصية لمرضى جائحة كورونا

اهتم المشرع الإماراتي بتوفير الحماية القانونية للبيانات الشخصية، فبالرغم من عدم وجود قانون خاص بحماية البيانات الشخصية في الدولة، إلا أن هنالك بعض القواعد الحمائية الواردة في القواعد العامة للقانون، والتي تناولت مسألة حماية البيانات الشخصية في مجال معين من مجالات التعامل مع هذه البيانات. كما نصت التشريعات الصحية في الدولة على قواعد حمائية خاصة بالبيانات الشخصية للمرضى والمستفيدين من خدمات الرعاية الصحية، وهو ما يستوجب معه تسليط الضوء على تلك القواعد الحمائية وبيان مدى كفايتها وفاعليتها في توفير الحماية القانونية للبيانات الشخصية لمرضى جائحة كورونا.

وعليه سيتم بيان الحماية القانونية للبيانات الشخصية لمرضى جائحة كورونا الواردة في القواعد العامة، وذلك في المطلب الأول، ثم سنتبعه بمطلب ثان يتعلق بالحماية القانونية المقررة في التشريعات الصحية.

المطلب الأول

حماية البيانات الشخصية وفقاً للقواعد العامة

أوردت القواعد العامة في القانون الإماراتي قواعد حمائية للبيانات الشخصية، حيث تفرقت تلك القواعد القانونية في مختلف القوانين الاتحادية والمحلية على مستوى الدولة، كما تدرجت الحماية القانونية في توفير الحماية للحق في الخصوصية بشكل عام وصولاً إلى توفير حماية قانونية خاصة بالبيانات الشخصية. وعليه سيتم تسليط الضوء على قواعد الحماية القانونية الواردة في القواعد العامة للقانون الإماراتي، ومن ثم تقييمها وبيان مدى فعاليتها في توفير الحماية القانونية اللازمة للبيانات الشخصية، وعلى ذلك نقسم هذا المطلب إلى فرعين على النحو التالي:

(١) هل تمثل تطبيقات الرصد الإلكتروني انتهاكاً لحقوق الإنسان، مقال منشور على الموقع الإلكتروني لأخبار بي بي سي، www.bbc.com، بتاريخ: ١٩مايو ٢٠٢٠، آخر زيارة للموقع: ٥-٨-٢٠٢٠.

- الفرع الأول: قواعد حماية البيانات الشخصية
- الفرع الثاني: تقييم فعالية قواعد الحماية القانونية
- الفرع الأول: قواعد حماية البيانات الشخصية

تضمنت القواعد العامة في القانون الإماراتي العديد من القواعد الحمائية للبيانات الشخصية، فنجد بأن الدستور الإماراتي تضمن أحكاماً توفر حماية فعالة للبيانات الشخصية، وإمعاناً في هذه الحماية قرر المشرع الإماراتي بمقتضى قانون العقوبات، جزاء يوقع على من يعتدي على خصوصية هذه البيانات، كما ألزمه بالتعويض وفقاً لقانون المعاملات المدنية، أضف إلى ذلك بأن المشرع الإماراتي قرر غطاءً قانونياً لتلك البيانات الشخصية، وذلك بمقتضى قانون مكافحة جرائم تقنية المعلومات. ولتوضيح ذلك نقسم هذا الفرع إلى أربعة غصون على النحو التالي:

- الغصن الأول: الدستور
- الغصن الثاني: قانون العقوبات
- الغصن الثالث: قانون المعاملات المدنية
- الغصن الرابع: قانون مكافحة جرائم تقنية المعلومات

الغصن الأول: الدستور

اهتم الدستور الإماراتي بحماية الخصوصية للأفراد، فقد كفل الحماية للعديد من الحقوق والحريات الشخصية والفكرية التي تتصل بشخص الإنسان وفكره[1]، فهي حقوق أصلية للإنسان سواء من حيث الشخصية الإنسانية وما يلازمها من حريات أخرى، أم من حيث ما يتصل بذهن الإنسان وفكره من رأي وخصوصية وغيرها من الحقوق اللصيقة به[2].

(١) فقد نصت المادة ٢٦ من دستور دولة الإمارات على أنه: «الحرية الشخصية مكفولة لجميع المواطنين ولا يجوز القبض على أحد أو تفتيشه أو حجزه إلا وفق أحكام القانون، ولا يعرض أي إنسان للتعذيب أو المعاملة الحاطة بالكرامة»، كما نصت المادة ٢٨ من الدستور ذاته على أنه: «العقوبة شخصية، والمتهم بريء حتى تثبت إدانته في محاكمة قانونية وعادلة، وللمتهم الحق في أن يوكل من يملك القدرة للدفاع عنه أثناء المحاكمة . ويبين القانون الأحوال التي يتعين فيها حضور محام عن المتهم، وإيذاء المتهم جسمانياً أو معنوياً محظور».

(٢) إعاد علي القيسي، مبادئ القانون الدستوري وأنظمة الحكم، دراسة تحليلية مقارنة لدستور الإمارات العربية المتحدة، الطبعة الأولى، ٢٠١٣، ص ٢٥٧.

ومن الخصوصيات التي نص الدستور الإماراتي على حمايتها صراحةً؛ خصوصية المراسلات بحيث تعد الرسائل بمختلف أنواعها من المسائل الخاصة المرتبطة بأفكار الإنسان وشخصيته، وهو ما يستوجب ضمان سرية المراسلات بمختلف أنواعها وذلك من خلال عدم السماح بالاطلاع عليها من قبل الآخرين أو إفشائها أو التصريح بها أو الاعتداء على سريتها، فقد نصت المادة ٣١ من دستور دولة الإمارات على أن: «حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال وسريتها مكفولة وفقاً للقانون».

ونشيد بالحماية القانونية التي كفلها الدستور للمراسلات، لاسيما المراسلات البريدية، بما تشمله من مراسلات البريد الإلكتروني، التي برزت أهمية حمايتها وضمان سريتها في الوقت الراهن، وذلك نتيجة لزيادة استخدامها والتواصل من خلالها في مختلف القطاعات والجهات، سواء على المستوى الشخصي للأفراد أو على مستوى الأعمال في القطاعات والمؤسسات الحكومية والخاصة. وفي هذا الصدد نشير إلى العملية التي تمت من خلال اختراق أنظمة المعلومات واستخدام المراسلات البريدية والتي ترتب عليها الاستيلاء على ما يقارب ٤,٣ مليون درهم إماراتي، وهو ما يبين أهمية حماية سرية عناوين البريد الإلكتروني والمراسلات التي تتم من خلاله[١].

الغصن الثاني: قانون العقوبات

أورد قانون العقوبات الاتحادي[٢] نصوصاً خاصة بحماية الحياة الخاصة للأفراد، وخصص بعض أنواع البيانات الشخصية بالحماية، فنجد بأن المادة ٣٧٨ من القانون ذاته قد نصت على أن: «يعاقب بالحبس والغرامة كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه: أ- استرق السمع أو سجل أو نقل عن طريق جهاز

(١) حيث تعود تفاصيل القضية والتي تعد من قضايا الاحتيال الإلكتروني المعروضة أمام المحكمة الاتحادية العليا إلى قيام خليجي باختراق مراسلات بريدية إلكترونية لشركتين، إحداهما في الشارقة والأخرى في السعودية، وتوصل إلى فحوى العلاقة التجارية الطويلة بينهما، فقام بإرسال رسالة من بريد إلكتروني مشابه كلياً لبريد موظفة بالشركة الأولى، يطلب فيه من الشركة الثانية مبالغ مستحقة تقدر بنحو أربعة ملايين و٣٧٠ ألف درهم إماراتي، وأدرج رقم حساب مختلف لشركته، بحجة أنه قام بتغيير الحساب، فانطلت الخدعة على الشركة الموجودة في السعودية وحولت الأموال إلى الجاني، ثم اكتشفت لاحقاً أنها كانت ضحية عملية احتيال متقنة . مقال بعنوان: خليجي يخترق مراسلات شركتين ويستولي على ٤,٣ ملايين درهم، صحيفة الإمارات اليوم، منشور بتاريخ: ٢٦ سبتمبر ٢٠٢٠، الموقع الرسمي للصحيفة: www.emaratalyoum.com، آخر زيارة للموقع: ٢-١٠-٢٠٢٠.

(٢) قانون العقوبات الاتحادي رقم ٣ لسنة ١٩٨٧ وتعديلاته.

من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف أو أي جهاز آخر. ب- التقط أو نقل بجهاز أياً كان نوعه صورة شخص في مكان خاص»[1]. «فإذا صدرت الأفعال المشار إليها في الحالتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضاً، كما يعاقب بالعقوبة ذاتها من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة. ويعاقب بالحبس مدة لا تزيد على سبع سنوات وبالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها».

ويقصد بأسرار الحياة الخاصة أو العائلية الواردة في المادة المذكورة ما تتميز به حياة الأفراد من أسرار شخصية ومشاعر ذاتية وغيرها من الخصوصيات التي يحق للفرد الاحتفاظ بها لنفسه وعدم السماح بالاطلاع عليها من قبل الغير، فقد ذهب البعض إلى أن الحياة الخاصة هي: «الحياة العائلية والشخصية والداخلية للإنسان عندما يعيش وراء بابه المغلق ويكون له الحق في المحافظة عليها ضد التدخل»[2].

أما في نطاق حماية البيانات الشخصية فنجد بأن المشرع في قانون العقوبات الاتحادي قد سلط الضوء على حماية إحدى صور البيانات الشخصية والمتمثلة في صورة الشخص، حيث كفلت المادة المذكورة أعلاه الحماية القانونية بشكل صريح للصورة الشخصية، وذلك من خلال تجريم التقاط أو نقل الصور الشخصية في الأماكن الخاصة.

إلا أن الحماية القانونية للصورة في هذا الصدد تقتصر على الصور التي تم التقاطها أو نقلها من أماكن خاصة، أما تلك التي تم التقاطها في الأماكن العامة فلا تدخل في نطاق الحماية لصراحة نص المادة بتحديد الحماية للصور التي تم التقاطها أو نقلها من الأماكن الخاصة، وفي هذا الصدد أكدت محكمة نقض أبو ظبي بأن الخصوصية قد تكون مستمدة من المكان المتواجد فيه الشخص الواقع عليه الاعتداء، بأن يكون مكاناً

(١) المادة ٣٧٨ معدلة بموجب القانون الاتحادي رقم ٣٤ لسنة ٢٠٠٥، حيث كانت المادة قبل التعديل تنص على أنه: «يعاقب بالحبس مدة لا تزيد على سنة والغرامة التي لا تجاوز عشرة آلاف درهم في الحالتين أو بإحدى هاتين العقوبتين من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة».

(٢) محمد محرم محمد، خالد محمد المهيري، قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقهاً وقضاءً، دار الفتح للطباعة والنشر، الطبعة الثانية، ١٩٩٢، ص ١٠٠١ .

خاصاً به، أو يتوقف دخوله على إذن لدائرة محددة صادر ممن يملك الحق فيه.[١] كما أن تحديد نطاق الحماية على الصور الملتقطة في الأماكن الخاصة يفيد اقتصار الحماية على الصور الملتقطة بطريقة غير مشروعة، أما الصور الملتقطة أو التي تم الحصول عليها بطريقة مشروعة فلم يورد المشرع في قانون العقوبات الاتحادي أية حماية قانونية لها حتى وإن تمت معالجتها أو نشرها أو استخدامها بطريقة غير مشروعة .

وقد نص قانون العقوبات الاتحادي على حماية البيانات في نصوص أخرى منها المادة ٣٨٠ مكرر[٢]، والتي ورد فيها بأنه: «يعاقب بالحبس كل من نسخ أو وزع أو زود الغير من دون وجه حق فحوى اتصال أو رسالة أو معلومات أو بيانات أو غيرها اطلع عليها بحكم عمله»، وبالرغم من الحماية القانونية التي وفرها المشرع للبيانات والمعلومات في هذه المادة إلا أن الحماية مخصصة للبيانات التي تم الاطلاع عليها بحكم عمل الشخص، أما ما يخرج عن نطاق العمل فلا يدخل في إطار الحماية المقررة وفقاً لهذه المادة.

الغصن الثالث: قانون المعاملات المدنية

نصت المادة ٩٠ من قانون المعاملات المدنية الاتحادي[٣] على أنه: «لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر»، وبذلك يكون المشرع قد حمى الشخص ضد الغير إذا تعدى على أي حق من الحقوق الملازمة للشخصية، كالتعدي على حرية الشخص أو سلامة جسمه أو سمعته الأدبية أو حرمة موطنه، فإذا وقع من الغير شيء من ذلك كان للشخص أن يطلب وقف هذا التعدي والتعويض عن الضرر. ويعد الاعتداء على البيانات الشخصية للشخص اعتداءً على حق من حقوقه الملازمة للشخصية، فتعدي الغير على بيانات الشخص ومنازعته في استعمالها دون مبرر يستوجب وقف الاعتداء والتعويض[٤].

كما خص القانون ذاته بعض البيانات الشخصية بالحماية القانونية، ومنها اسم الشخص ولقبه، حيث ورد في المادة ٩١ منه أنه: «لكل من نازعه غيره في استعمال

---

(١) محكمة نقض أبو ظبي، طعن رقم ٢٩٥ لسنة ٢٠١٧، تاريخ الجلسة ٢٦-٤-٢٠١٧، مشار إليه في: شبكة قوانين الشرق، www.eastlaws.com ،آخر زيارة للموقع: ١٨-٩-٢٠٢٠.

(٢) المادة ٣٨٠ مكرر أضيفت بمرسوم بقانون اتحادي رقم ٧ لسنة ٢٠١٦.

(٣) قانون اتحادي رقم ٥ لسنة ١٩٨٥ بإصدار قانون المعاملات المدنية لدولة الإمارات العربية المتحدة المعدل بالقانون الاتحادي رقم ١ لسنة ١٩٨٧.

(٤) المذكرة الإيضاحية لقانون المعاملات المدنية الصادر بالقانون الاتحادي رقم ٥ لسنة ١٩٨٥ المعدل بالقانون الاتحادي رقم ١ لسنة ١٩٨٧، ص ٦٤.

اسمه أو لقبه أو كليهما بلا مبرر، أو انتحل اسمه أو لقبه أو كليهما دون حق، أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر». أضف إلى ذلك بأنه يحق للمتضرر من عدم حماية بياناته الشخصية واستخدامها بطريقة غير مشروعة كنشرها أو استخدامها أو غيرها من وسائل الاعتداء على سرية وخصوصية البيانات الشخصية، أن يطالب بالتعويض وفقاً لقواعد المسؤولية الواردة في المادة ٢٨٢ من قانون المعاملات المدنية الاتحادي، والتي تنص على أنه: «كل أضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر»، وعليه يحق لصاحب البيانات الشخصية المطالبة بالتعويض عن الضرر الذي أصابه نتيجة التعدي على خصوصية بياناته الشخصية واستخدامها بطريقة غير مشروعة، وذلك من خلال إثبات وجود فعل الإضرار والضرر والعلاقة السببية بينهما[١].

الغصن الرابع: قانون مكافحة جرائم تقنية المعلومات

نص المشرع الإماراتي في قانون مكافحة جرائم تقنية المعلومات[٢] على العديد من القواعد الحمائية للبيانات الشخصية[٣]، فنجد بأن المادة الثانية منه قد فرضت عقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين، على كل من تسبب بإلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات شخصية، وذلك من خلال الدخول إلى أي موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات من دون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة.

فهذه المادة تجرم الاعتداء على البيانات الشخصية سواء أكانت هذه البيانات موجودة على موقع إلكتروني على شبكة الإنترنت أم موجودة على نظام معلوماتي غير مرتبط بشبكة الإنترنت، كما قد تكون تلك البيانات الشخصية موجودة على شبكة معلومات

(١) للتفصيل أكثر حول المسؤولية التقصيرية عن معالجة البيانات الشخصية في قانون المعاملات المدنية الاتحادي، انظر: سامح عبد الواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها، دراسة في القانون الإماراتي، مرجع سابق، ص ٦٤٣ وما بعدها.

(٢) المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، المعدل بقانون اتحادي رقم ١٢ لسنة ٢٠١٦.

(٣) تعد دولة الإمارات العربية المتحدة أول دولة خليجية وثاني دولة عربية – بعد المملكة المغربية – تصدر قانوناً خاصاً بمكافحة جرائم تقنية المعلومات والذي يختص بتجريم الأفعال المرتكبة عبر شبكة الإنترنت أو أية وسيلة من وسائل تقنية المعلومات. محمد خليفة الغفلي، مرجع سابق .

داخلية خاصة بمنشأة معينة، بحيث يخترق أحدهم الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة الداخلية لإحدى المؤسسات أو الهيئات، ويقوم بإحدى العمليات المحظورة على البيانات الشخصية، كإلغائها أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغييرها أو نسخها أو نشرها[١].

وقد نصت المادة ٢١ من القانون ذاته على تجريم نشر المعلومات أو البيانات الشخصية حتى وإن كانت صحيحة وحقيقية؛ وذلك لضمان حماية سرية تلك البيانات والمعلومات، فقد ورد بأنه: «يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بنشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية».

ويلاحظ أن المشرع جرم الاعتداء على خصوصية الأشخاص دون تحديد معنى تلك الخصوصية وحدودها، وهو ما يجعل من الصعب تحديد الحد الفاصل بين الحياة الخاصة للأفراد والحياة العامة التي من الممكن الاطلاع عليها من قبل الآخرين. إلا أنه يمكن القول بأن خصوصية الأشخاص تعني الحياة الخاصة بهم، والتي تشمل كافة الأمور الشخصية التي لا يرغب الشخص بمشاركتها أو إطلاع الغير عليها دون رضاه. فالخصوصية هي حق كل شخص في الاحتفاظ بشؤونه الخاصة التي لا يرغب أن يطلع عليها الآخرون[٢]، ويرجع ذلك إلى الشخص نفسه، فقد لا يتوافر للشؤون التي يرى الشخص حجبها عن الآخرين صفة السرية غير أنها تنتمي مع ذلك إلى الحياة الخاصة،

(١) سامح عبد الواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها، دراسة في القانون الإماراتي، مرجع سابق، ص ٦٣٧.

(٢) ويتوجب حماية خصوصية الأفراد في مواجهة الآخرين حتى وإن كانوا أقرب الناس إليهم، كمن تربطهم علاقات أسرية أو اجتماعية، وفي هذا الصدد نشير إلى القضية التي شهدتها محاكم عجمان بهذا الخصوص والتي تعود وقائعها إلى ما قامت به إحدى الزوجات بفتح هاتف زوجها دون علمه والاطلاع على بعض المراسلات والصور الموجودة فيه، وقامت بتصوير تلك المراسلات والصور باستخدام هاتفها المحمول، فما كان من الزوج إلا أن قام بإبلاغ الجهات المعنية بفعل الزوجة حيث اعترفت بالتهم المنسوبة إليها، فتم الحكم عليها بالحبس والإبعاد والغرامة وفقاً لقانون مكافحة جرائم تقنية المعلومات . زايد الشامسي، الضوابط القانونية لاستخدام وسائل التواصل الاجتماعي، منتدى نحو مجتمع رقمي آمن، جمعية أم المؤمنين، عجمان، بتاريخ ٢٣ سبتمبر ٢٠٢٠، عبر تطبيق زوم zoom .

فالخصوصية في هذا الصدد لا تعني السرية و إنما تعد الخصوصية ذات مدى أوسع بحيث تشمل أموراً قد لا تكون سرية[١].

ولم يكتف المشرع بحماية المعلومات والبيانات الشخصية فحسب، بل شمل بالحماية أنظمة المعلومات الإلكترونية ووسائل تقنية المعلومات التي تحوي تلك البيانات الشخصية، فقد ورد في المادة العاشرة من القانون ذاته بأنه : «يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً ومن دون تصريح برنامجاً معلوماتياً إلى الشبكة المعلوماتية أو نظام معلومات إلكترونياً أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات».

فقد جاء هذا النص نتيجة اهتمام المشرع بأن تقوم الشبكة المعلوماتية وأنظمة المعلومات الإلكترونية ووسائل تقنية المعلومات بأداء مهامها من دون معوقات وبطريقة طبيعية، ويتم ذلك من خلال حمايتها وحماية البيانات والمعلومات المحفوظة فيها من السلوكيات التي تؤدي إلى الإضرار بها.

كما خص القانون بعض صور البيانات الشخصية بالحماية القانونية نظراً لأهميتها وضرورة الحفاظ على سريتها وخصوصيتها، ومنها البيانات الشخصية المتعلقة بأرقام البطاقات الائتمانية أو الإلكترونية، وأرقام وبيانات الحسابات المصرفية، بالإضافة إلى البيانات الشخصية المتعلقة بأية وسيلة من وسائل الدفع الإلكتروني[٢]، وكذلك البيانات الشخصية المتمثلة في الأرقام السرية وكلمات المرور أو الشفرات المستخدمة للدخول إلى وسائل تقنية المعلومات أو المواقع الإلكترونية أو الأنظمة المعلوماتية الإلكترونية أو الشبكة المعلوماتية[٣].

---

(١) عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، جمهورية مصر العربية، ٢٠٠٤، ص ٥٩٤ .

(٢) المادة ١٢ من قانون مكافحة جرائم تقنية المعلومات . ومن أهم قضايا الاحتيال على الأرقام الخاصة بالبطاقات الائتمانية ما شهدته محكمة عجمان في قضية متعلقة بمكتب سياحي في الإمارة، حيث تعود تفاصيل القضية إلى تواصل أحد موظفي المكتب السياحي مع شخص في سنغافورة عبر البريد الإلكتروني ليقوم الأخير بحجز تذاكر سفر للمتعاملين مع المكتب السياحي، حيث تبين بأنه كان يقوم بحجز تذاكر السفر من خلال بطاقات ائتمانية مسروقة، وهو ما أدى بشركات الطيران إلى إلغاء كافة التذاكر المحجوزة لعملاء المكتب السياحي عن طريق تلك البطاقات المسروقة، فما كان من المكتب السياحي إلا أن قام بشراء تذاكر سفر جديدة لكافة العملاء وهو ما كبده خسارة مالية بلغت مليون ونصف درهم إماراتي، محمد خليفة الغفلي، مرجع سابق.

(٣) المادة ١٤ من قانون مكافحة جرائم تقنية المعلومات .

وفيما يتعلق بحماية الصورة باعتبارها إحدى البيانات الشخصية، فقد كفل لها المشرع الحماية القانونية وجرم الاعتداء عليها، إذ «يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكترونياً، أو إحدى وسائل تقنية المعلومات، في غير الأحوال المصرح بها قانوناً بالتقاط صور الغير أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها»[١].

كما «يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، كل من استخدم نظام معلومات إلكترونياً، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها»[٢].

وبذلك يكون المشرع قد وفر الحماية القانونية للصور الشخصية في مواجهة كافة العمليات التي قد ترد عليها، كالتقاط صور الغير وإعداد الصور الإلكترونية ونقلها وكشفها ونسخها والاحتفاظ بها، كما جرم تعديل الصور ومعالجتها بقصد الاعتداء على الخصوصية أو انتهاكها. ونعني بتغيير الصور إحداث تغيير فيها، أما معالجة الصور فتتم من خلال عمليات تقنية تقوم بتحويل الصورة إلى شكل معين يمكن للحاسوب أو أية وسيلة تقنية أخرى أن يتعامل معه ويفهمه[٣].

وفي تفسيرها للحماية القانونية الواردة في المادة ٢١ بخصوص الصورة، فقد اشترطت محكمة نقض أبو ظبي أن يتم التقاط الصورة في أماكن خاصة، أما تلك الصور الملتقطة في أماكن عامة فلا تشملها الحماية القانونية الواردة في هذا الصدد، حيث أكدت بأن تصوير الأشخاص في مكان عام ومطروق لكافة العاملين فيه وللجمهور لا يمثل اعتداء على الخصوصية الوارد في المادة ٢١ من قانون مكافحة جرائم تقنية المعلومات[٤]،

(١) المادة ٢١ من قانون مكافحة جرائم تقنية المعلومات.

(٢) المرجع السابق .

(٣) عبدالرازق الموافي عبداللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، الكتاب الأول، سلسلة الدراسات القانونية والقضائية، عدد ١٥، معهد دبي القضائي، دبي، ٢٠١٦، ص ٣١ .

(٤) محكمة نقض أبو ظبي، طعن رقم ١١٠٦ لسنة ٢٠١٨، تاريخ الجلسة ٢٢-١-٢٠١٩ . مشار إليه في: خالد المسلمي، المستحدث من الأحكام الصادرة من محكمة النقض، مجلة القضاء والقانون، مركز البحوث والدراسات القضائية بدائرة القضاء – أبو ظبي، عدد خاص بفيروس كورونا (كوفيد ١٩)، السنة السادسة، يوليو ٢٠٢٠، ص٣٠٩.

وقضت في أحد أحكامها بأن: «تصوير موظفات مكتب الإمارات للهوية قسم السيدات بمركز بلدية العين أثناء تأدية عملهن في مقر العمل لا يعد اعتداء على الخصوصية الشخصية للموظفات، حيث إن الواقعة حدثت في مكتب الإمارات للهوية وهو ليس مكاناً خاصاً ولا يتوقف الدخول إليه على إذن من المجني عليهم – موظفات المكتب – وهو ما يعني أن الواقعة حدثت في مكان عام ومطروق لكافة العاملين فيه وللجمهور، فمن ثم أضحت الأوراق خالية من دليل يقيني على قيام الطاعنين بالاعتداء على الخصوصية الشخصية للعاملين بذلك المكان»[١].

كما بينت في حكم آخر لها بأن تصوير الشخص على متن الطائرة لا يعد اعتداء على خصوصيته، حيث قضت بأن: «الخصوصية تكون مستمدة من المكان المتواجد فيه الشخص الواقع عليه الاعتداء، بأن يكون مكاناً خاصاً به، أو يتوقف دخوله على إذن لدائرة محددة صادر ممن يملك الحق فيه، أما تصوير المجني عليه في الطائرة وهو مكان مطروق لطاقم الطائرة ولجميع المسافرين على متنها فلا تتوافر به جريمة الاعتداء على خصوصيته في معنى المادة ٢١ من المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٤ في شأن مكافحة جرائم تقنية المعلومات».[٢]

إلا أننا لا نؤيد ما اتجهت إليه محكمة نقض أبو ظبي من تخصيص الحماية القانونية الواردة في المادة ٢١ على الصور التي تم التقاطها في الأماكن الخاصة؛ ذلك أن المشرع لم يقصر الحماية على الصور الملتقطة في الأماكن الخاصة، وإنما كفل الحماية لكافة الصور الملتقطة للغير باستخدام شبكة معلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وهو ما يعني بأن الحماية القانونية للصورة تشمل تلك الصور الملتقطة في الأماكن العامة والخاصة.

أضف إلى ذلك أنه في حال أراد المشرع اقتصار الحماية على الصور الملتقطة في الأماكن الخاصة لنص على ذلك صراحةً، كما هو الحال في المادة ٣٧٨ من قانون العقوبات الاتحادي والتي نصت على أنه: «يعاقب بالحبس والغرامة كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه: ب- التقط أو نقل بجهاز أياً كان نوعه صورة شخص في مكان خاص».

(١) محكمة نقض ابو ظبي، طعن رقم ١١٨٢ لسنة ٢٠١٥، تاريخ الجلسة ٢٢-٢-٢٠١٦، مشار إليه في شبكة قوانين الشرق، www.eastlaws.com، آخر زيارة للموقع: ٣-١٠-٢٠٢٠.

(٢) محكمة نقض أبو ظبي، طعن رقم ٢٩٥ لسنة ٢٠١٧، تاريخ الجلسة ٢٦-٤-٢٠١٧، مشار إليه في شبكة قوانين الشرق ، www.eastlaws.com، آخر زيارة للموقع: ٣-١٠-٢٠٢٠.

ومن ناحية أخرى فقد اهتم المشرع الإماراتي في قانون مكافحة جرائم تقنية المعلومات بتوفير حماية قانونية خاصة للمعلومات والبيانات المتعلقة بالمجال الطبي، باعتبارها أحد أهم أنواع البيانات الشخصية، وتشمل كافة البيانات الشخصية المتعلقة بالفحوصات أو التشخيص الطبي، وكذلك المعلومات المتعلقة بعلاج الأشخاص وسجلاتهم الطبية. فقد نصت المادة السابعة من قانون مكافحة جرائم تقنية المعلومات على أنه: «يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى بغير تصريح بيانات أي مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات، وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي، أو علاج أو رعاية طبية أو سجلات طبية».

ويثور التساؤل بشأن مدى انطباق الاعتداء على سرية البيانات والمعلومات الشخصية المستخدمة في الوسائل الإلكترونية والتقنيات المستحدثة لمواجهة فيروس كورونا المستجد على الحماية التي فرضها المشرع في المادة السابعة من القانون؟ وهذا التساؤل يرجع إلى أن المشرع قد نص على وسائل محددة يلزم الاعتداء على البيانات الشخصية من خلالها، والمتمثلة في الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات؛ أي عن طريق الحاسب الآلي أو الإنترنت أو الأقراص المحفوظ عليها البيانات والمعلومات الطبية الخاصة بالمريض(١).

لا شك أن تحديد مدى انطباق الحماية القانونية الواردة في هذا النص على التقنيات والآليات المستحدثة لمواجهة فيروس كورونا المستجد، يقوم على بيان ما إذا كانت تلك الآليات والتقنيات من قبيل الوسائل التي حددها المشرع الإماراتي والمتمثلة في الشبكة المعلوماتية، والمواقع الإلكترونية، وأنظمة المعلومات الإلكترونية، ووسائل تقنية المعلومات. ونحن نرى بأن هذه التقنيات والآليات المستحدثة والمتمثلة في تطبيقات الرصد الإلكتروني، ووسائل التتبع الإلكترونية، والمنصات الإلكترونية المخصصة لتشخيص وعلاج الحالات المرضية، وغيرها من التقنيات والوسائل الإلكترونية المستحدثة لمواجهة فيروس كورونا، لا تخرج عن نطاق الوسائل التي حددها المشرع؛ بحيث يمكن تصنيفها بأنها أنظمة معلومات إلكترونية وهي: «مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك»(٢).

(١) عبد الرازق الموافي عبد اللطيف، مرجع سابق، ص٩٧.
(٢) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات .

كما يمكن تصنيفها بأنها وسيلة من وسائل تقنية المعلومات، لاسيما وأن المشرع قد وسع في تعريف وسائل تقنية المعلومات باعتبارها: «أية أداة إلكترونية[1] مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين»[2]. وبالرغم مما نراه بأن التقنيات والآليات المستحدثة لمواجهة فيروس كورونا تعد من ضمن نطاق الوسائل الإلكترونية التي أشار إليها المشرع الإماراتي في المادة المذكورة أعلاه، وشمولية النص لكافة وسائل تقنية المعلومات بمختلف أنواعها وصورها، إلا أن تحديد ما إذا كانت التقنيات المستحدثة و التطبيقات الإلكترونية تدخل ضمن نطاق الحماية المقررة في هذا الصدد من عدمه تعد من المسائل المعروضة أمام المحاكم المختصة بنظر النزاع.

الفرع الثاني
تقييم فعالية قواعد الحماية القانونية

يتضح من القواعد القانونية العامة اهتمام المشرع الإماراتي بحماية الخصوصية للأفراد، ويمكن القول بأن خصوصية المعلومات والبيانات الشخصية جزء من الخصوصية على إطلاقها، وتتعلق بمواجهة الاعتداءات على البيانات الشخصية، في حين أن الخصوصية على إطلاقها تنطوي على خصوصية البيانات والاتصالات، وأيضاً خصوصية المكان والمراسلات العادية والإلكترونية، وكل هذه المفاهيم ترتبط معاً في نطاق واحد هو الحق في الخصوصية[3].

وقد اهتم المشرع الإماراتي بدايةً بحماية خصوصية الأفراد وحياتهم الخاصة بشكل عام، ثم توالت القوانين التي وفرت الحماية القانونية الخاصة ببعض جزئيات الخصوصية والحياة الخاصة ومنها حماية المعلومات والبيانات الشخصية محل الدراسة، فنجد أن حماية الخصوصية في القانون الإماراتي بدأت من حماية الدستور للحقوق والحريات الشخصية والفكرية التي تتصل بشخص الإنسان وفكره، وذلك من خلال حرمة المسكن وخصوصية المراسلات وحق الكرامة والأمن وغيرها مما يدخل في

(١) الإلكتروني: ما يتصل بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية أو المؤتمتة أو الضوئية أو ما شابه ذلك . المادة الأولى من قانون مكافحة جرائم تقنية المعلومات.

(٢) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات .

(٣) مصطفى بن قارة، مرجع سابق، ص ٧٨ .

نطاق توفير الحياة الخاصة للإنسان، وهو ما سار عليه المشرع الإماراتي في قانون العقوبات الاتحادي بتوفير الحماية القانونية للحياة الخاصة بشكل عام، وذلك بنصه على أنه: «يعاقب بالحبس والغرامة كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد[١]»، فلم يورد المشرع حماية خاصة بالمعلومات أو البيانات الشخصية على وجه الخصوص، وقد استمر المشرع الإماراتي على النهج ذاته في قانون المعاملات المدنية الاتحادي الذي نص على أنه: « لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر»[٢].

ويثور التساؤل بشأن مدى اعتبار حماية البيانات الشخصية جزءاً من حماية الحياة الخاصة للأفراد ؟ وهل يمكن اعتبار كافة البيانات الشخصية من قبيل الحياة الخاصة للأفراد التي تدخل في نطاق الحماية القانونية المقررة في هذا الصدد ؟

من الملاحظ أن القوانين التي كفلت الحماية للخصوصية أو الحياة الخاصة للأفراد لم تبين معنى تلك الخصوصية، ولم ترسم الحد الفاصل بين الحياة الخاصة للأفراد والحياة العامة، وسبق أن أشرنا إلى صعوبة الفصل بين الحياة العامة للأفراد والحياة الخاصة التي تتمتع بالحماية القانونية، وبشأن مدى اعتبار حماية البيانات الشخصية جزءاً من حماية الحياة الخاصة، يرى جانب من الفقه[٣] بأن الحياة الخاصة للأفراد تشمل بياناتهم الشخصية، بحيث تعتبر أية بيانات أو معلومات متعلقة بشخص طبيعي من البيانات الشخصية التي تقع ضمن إطار الحياة الخاصة، وبالتالي تدخل في نطاق الحماية القانونية المقررة في هذا الصدد.

كما تشير غالبية القوانين التي أوردت القواعد الحمائية للحياة الخاصة، إلى أن البيانات الشخصية للأفراد تدخل في نطاق الحياة الخاصة، وذلك بالنص صراحة على بعض أنواع البيانات الشخصية ضمن النصوص القانونية المعنية بحماية الحياة الخاصة ومنها الصورة الشخصية، فقد نصت المادة ٣٧٨ من قانون العقوبات الاتحادي على أن: «يعاقب بالحبس والغرامة كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني

(١) المادة ٣٧٨ من قانون العقوبات الاتحادي.
(٢) المادة ٩٠ من قانون المعاملات المدنية الاتحادي.
(٣) حول هذا الرأي، انظر: سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي، مرجع سابق، ص٣٧٩.

عليه: ب- التقط أو نقل بجهاز أياً كان نوعه صورة شخص في مكان خاص»، وهو ما يؤكد بأن الصورة الشخصية وهي أحد أنواع البيانات الشخصية تدخل في نطاق الحياة الخاصة.

وبخصوص قانون المعاملات المدنية الاتحادي فقد اعتبر البيانات الشخصية جزءاً من الحقوق الملازمة للشخصية، وهو ما أكدته المذكرة الإيضاحية للقانون بحيث اعتبرت الاعتداء على البيانات الشخصية للشخص اعتداءً على حق من حقوقه الملازمة للشخصية، فاعتداء الغير على بيانات الشخص ومنازعته في استعمالها دون مبرر يستوجب وقف الاعتداء والتعويض[1].

وبالرغم من تأييدنا للاتجاه القائل بدخول البيانات الشخصية ضمن نطاق الحياة الخاصة في بعض الأحيان، إلا أن ذلك لا يعني اعتبار كافة البيانات الشخصية من قبيل الحياة الخاصة للأفراد، إذ إن هنالك بيانات شخصية تعد من عناصر الحياة الخاصة للأفراد وتدخل ضمن نطاق الحماية المقررة لخصوصية الأفراد والحق في حماية الحياة الخاصة، وهنالك أنواع أخرى من البيانات الشخصية التي لا تعد من قبيل الحياة الخاصة للأفراد وبالتالي لا تدخل ضمن الحماية القانونية المقررة لها، فلا تعد كل معلومة أو بيان شخصي من قبيل الحياة الخاصة التي تستوجب الحماية.

وهذا الواقع يبرر ضرورة سن تشريعات خاصة بحماية البيانات الشخصية وعدم الاكتفاء بالحماية المقررة لحق الخصوصية أو الحياة الخاصة في القواعد العامة، بحيث يتم توفير الحماية الفاعلة لكافة صور البيانات الشخصية سواء أكانت تدخل ضمن نطاق الحياة الخاصة أم لا، بالإضافة إلى توفير الحماية القانونية لمعالجة البيانات الشخصية لاسيما تلك التي لا تمثل اعتداءً على الحياة الخاصة لصاحب تلك البيانات.

وقد خطا المشرع الإماراتي الخطوة الأولى في هذا الصدد، وذلك بتوفير قواعد حمائية خاصة للبيانات الشخصية، حيث نص صراحة على تجريم الاعتداء على البيانات الشخصية في قانون مكافحة جرائم تقنية المعلومات، إلا أن هذه الخطوة لم تعد كافية لتوفير الحماية اللازمة للبيانات الشخصية، لاسيما في ظل العولمة وسهولة الحصول على البيانات وتداولها، بحيث تتضاعف أهمية إرساء نظام فاعل للحماية، وفرض إجراءات قانونية صارمة ضد إساءة استخدام البيانات الشخصية والاعتداء على خصوصيتها. وعليه فإنه يجدر بالمشرع الإماراتي أن ينتقل للخطوة التالية والمتمثلة في سن تشريع

(١) المذكرة الإيضاحية لقانون المعاملات المدنية الصادر بالقانون الاتحادي رقم ٥ لسنة ١٩٨٥ المعدل بالقانون الاتحادي رقم ١ لسنة ١٩٨٧، ص ٦٤.

خاص لحماية البيانات الشخصية، وفعلاً يوجد مشروع قانون اتحادي لحماية البيانات الشخصية منذ عام ٢٠١٨[١]، إلا أنه لم يتم إصداره حتى الآن، وهو ما نأمل أن يقوم به المشرع الإماراتي لضمان توفير الحماية القانونية للبيانات الشخصية.

وقد أكد القضاء الإماراتي على ضرورة سن تشريع خاص بحماية البيانات الشخصية، وذلك من خلال دراسة أعدتها دائرة القضاء بأبو ظبي منذ أواخر عام ٢٠١٩، حيث أوضحت بأن المشرع الإماراتي جرم التعرض إلى الخصوصية عموماً، وإلى بعض جوانب البيانات الشخصية خصوصاً، بالإضافة إلى بعض المبادئ القضائية التي أقرتها المحاكم العليا في الدولة، ويمكن اعتبارها أساساً لحماية قضائية للبيانات الشخصية، إلا أنها لم تعد كافية في الوقت الراهن، وهو ما يستوجب سن قانون لحماية البيانات الشخصية يراعي مختلف التجارب العالمية في هذا المجال، ويؤسس بناءً على أفضل الممارسات العالمية ذات الصلة[٢].

وإلى حين صدور ذلك القانون ينبغي الرجوع إلى الحماية التي وردت في قانون مكافحة جرائم تقنية المعلومات، حيث أورد العديد من القواعد الحمائية التي يمكن الاستناد إليها لحماية خصوصية البيانات الشخصية، لاسيما المادة ٢١ منه والتي كفلت الحماية القانونية للبيانات الشخصية من مختلف العمليات التي قد ترد عليها، بالإضافة إلى الحماية المقررة لمعالجة البيانات الشخصية، كما يمكن الرجوع أيضاً إلى قواعد ضمان الفعل الضار في قانون المعاملات المدنية الإماراتي وفقاً للمادة ٢٨٢، بحيث يتم تعويض من تم الاعتداء على بياناته الشخصية إذا تسبب هذا الاعتداء في الإضرار به. ومما لا شك فيه بأن الرجوع

(١) حيث أعلنت الهيئة العامة لتنظيم قطاع الاتصالات في الدولة عن إعداد مشروع قانون اتحادي جديد لحماية البيانات الشخصية للمستخدمين في دولة الإمارات، وفق أعلى المعايير العالمية في هذا المجال، وبينت أن القانون الإماراتي الجديد يتكفل بحماية بيانات المستخدمين في الإمارات، وسيكون نطاق تطبيقه داخل الدولة، لينضم بذلك إلى القوانين النافذة في هذا الشأن المعنية بحماية البيانات، وشددت على أن مسؤولية تطبيق بنود قانون حماية بيانات المستخدمين تعود على الشركات والمؤسسات التي تمتلك البيانات أو تخزنها أو تعالجها، كما أفادت بأن هذه النوعية من التشريعات تنظم بشكل عام علاقة العمل بين الشركات والمؤسسات التي تعالج وتخزن البيانات، من جهة، وأصحاب تلك البيانات من جهة أخرى، كما أنها توفر مبادئ ومفاهيم من شأنها أن توضح وتيسر أطر العمل والتنسيق. مقال بعنوان: مشروع قانون جديد لحماية البيانات الشخصية للمستخدمين، صحيفة الاتحاد، منشور بتاريخ ٢٢ يوليو ٢٠١٨، الموقع الإلكتروني للصحيفة: www.alittihad.ae، آخر زيارة للموقع: ١-١٠-٢٠٢٠.

(٢) مقال بعنوان: قضاء أبو ظبي يوصي بسن قانون لحماية البيانات الشخصية، صحيفة الإمارات اليوم، منشور بتاريخ ٢٥ يوليو ٢٠١٩، الموقع الإلكتروني للصحيفة: www.emaratalyoum.com، آخر زيارة للموقع: ١-١٠-٢٠٢٠.

للقواعد العامة لن يوفر الحماية المرجوة للبيانات الشخصية لاسيما في ظل أساليب الاختراق والمعالجة المستحدثة التي أوجدها التقدم العلمي والتكنولوجي في الآونة الأخيرة.

المطلب الثاني

حماية البيانات الشخصية وفقاً للتشريعات الصحية

اهتمت التشريعات الصحية في الدولة بحماية حقوق وحريات المرضى ومتلقي خدمات الرعاية الصحية على مستوى الدولة، وتتمثل أهم تلك الحقوق في حماية سرية و خصوصية البيانات والمعلومات الشخصية لمتلقي تلك الخدمات الصحية، حيث وردت بعض القواعد الحمائية للبيانات الشخصية في التشريعات الصحية.

وتتمثل أهمية حماية البيانات الشخصية لمرضى جائحة كورونا فيما يشهده العالم من زيادة عمليات الاختراق لأنظمة المعلومات الخاصة بالجهات الصحية، لاسيما وأن تهديدات الهجمات الإلكترونية قد تتسبب بشلل الأنظمة التقنية الطبية بالكامل وإلحاق ضرر كبير بها[1].

أضف إلى ذلك فإن قطاع الرعاية الصحية يعد في المرتبة الأولى من ضمن القطاعات التي تم استهدافها بعمليات الاختراق والهجمات السيبرانية، وذلك منذ بداية انتشار جائحة كورونا[2]. وعليه سنهتم في بحثنا هذا ببيان قواعد الحماية القانونية للبيانات الشخصية

(١) حيث إن الهجمات الإلكترونية على قطاع الرعاية الطبية مستمرة، ومن أهمها هجوم قراصنة إنترنت باستخدام برمجيات «الفدية الخبيثة» التي استهدفت عدداً من المؤسسات في مختلف أنحاء العالم، حيث أدّت هجماتها إلى تعطيل معظم المستشفيات البريطانية، كما أصابت تلك الهجمات دولاً عظمى مثل الصين وروسيا. مقال بعنوان: التقنية الطبية .. فوائد صحية ومخاوف أمنية، صحيفة الخليج، منشور بتاريخ: ٢-٩-٢٠١٧، الموقع الإلكتروني للصحيفة: www.alkhaleej.ae، آخر زيارة للموقع: ١٠-٩-٢٠٢٠. أضف إلى ذلك ما وقع في الولايات المتحدة الأمريكية من قيام أحد الأشخاص باختراق نظام المعلومات الخاص بالمشفى الذي تتلقى فيه زوجته الرعاية الطبية اللازمة، حيث قام بتغيير الوصفة الطبية التي تحوي الأدوية التي يتم إعطاؤها لزوجته من قبل المشفى، وهو ما أدى إلى وفاتها نتيجة تغييره للوصفة الطبية الخاصة بها. محمد خليفة الغفلي، مرجع سابق.

(٢) وجدير بالذكر في هذا الصدد بأنه لم يتم تسجيل أي استهداف بشأن أية منشأة طبية في الدولة منذ بداية انتشار الجائحة، حيث تم تصنيف دولة الإمارات العربية المتحدة كرابع أفضل دولة من حيث توفير أفضل بيئة إلكترونية تعنى بتوفير بنية تحتية أمنية للخدمات الإلكترونية. عبيد صالح المختن، طرق الوقاية من أساليب الاختراق الإلكتروني، منتدى نحو مجتمع رقمي آمن، جمعية أم المؤمنين، عجمان، بتاريخ ٢٣ سبتمبر ٢٠٢٠، عبر تطبيق زوم zoom .. كما أكدت مباركة إبراهيم، مديرة إدارة نظم المعلومات الصحية في وزارة الصحة ووقاية المجتمع بأن وزارة الصحة ووقاية المجتمع لم تشهد أي خلل في الحماية الأمنية خلال السنوات العشر الأخيرة. مقال بعنوان: التقنية الطبية .. فوائد صحية ومخاوف أمنية، صحيفة الخليج، منشور بتاريخ: ٢-٩-٢٠١٧، الموقع الإلكتروني للصحيفة: www.alkhaleej.ae، آخر زيارة للموقع: ١٠-٩-٢٠٢٠.

الواردة في التشريعات الصحية، ومن ثم سيتم تقييمها وبيان مدى كفاية وفاعلية الحماية القانونية المقررة في هذه التشريعات للبيانات الشخصية الخاصة بالمرضى.

وذلك من خلال تقسيم هذا المطلب إلى فرعين على النحو التالي:

- الفرع الأول: القواعد الحمائية للبيانات الشخصية في التشريعات الصحية
- الفرع الثاني: تقييم فعالية قواعد الحماية القانونية

الفرع الأول

القواعد الحمائية للبيانات الشخصية في التشريعات الصحية

اهتم المشرع الإماراتي بحماية البيانات الشخصية للمرضى ومتلقي خدمات الرعاية الصحية في الدولة، فقد أورد العديد من القواعد الحمائية في مختلف التشريعات الصحية؛ وذلك لضمان سرية وخصوصية البيانات الشخصية الخاصة بالمرضى، ولتسليط الضوء على الحماية القانونية الواردة في تلك التشريعات الصحية سيتم تقسيم هذا الفرع إلى ثلاثة غصون على النحو التالي:

- الغصن الأول: قانون مكافحة الأمراض السارية
- الغصن الثاني: قانون المسؤولية الطبية
- الغصن الثالث: قانون استخدام تقنية المعلومات والاتصالات في المجالات الصحية

الغصن الأول

قانون مكافحة الأمراض السارية

يهدف قانون مكافحة الأمراض السارية[١] إلى حماية الصحة العامة وتعزيز جهود الدولة في تنفيذ استراتيجية مكافحة الأمراض السارية ومنع انتشارها، وذلك بالموازنة بين مقتضيات الصحة العامة وحقوق الأفراد وفق اللوائح الصحية الدولية. وتسري أحكام هذا القانون داخل حدود دولة الإمارات العربية المتحدة، وعلى جميع الأمراض السارية الواردة في جدول الأمراض السارية المرفق بالقانون[٢].

وقد سلط القانون الضوء على حماية بعض أنواع البيانات الشخصية الخاصة بالمرضى المصابين بأمراض سارية، حيث نصت المادة ٢٩ منه على أنه: «يحق للأشخاص

(١) قانون اتحادي رقم ١٤ لسنة ٢٠١٤ في شأن مكافحة الأمراض السارية.

(٢) مقال بعنوان: مكافحة الأمراض السارية، البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة، https://u.ae/ar-AE#/، آخر زيارة للموقع بتاريخ ١-١٠-٢٠٢٠.

المصابين بأمراض سارية حماية سرية المعلومات الخاصة بهم والتي لها علاقة بالمرض، ولا يجوز إفشاء هذه المعلومات إلا في الحالات المقررة قانوناً»[١]، بحيث تلتزم الجهات الصحية المعنية بحماية سرية أية بيانات أو معلومات خاصة بالحالة الصحية للمريض المصاب بأحد الأمراض السارية المنصوص عليها في القانون، وهو ما يعد أحد أهم الحقوق التي ينبغي توفيرها وحمايتها للمرضى، فالمعلومات والبيانات الخاصة بحالة المريض الصحية تعد من الأمور الخاصة به والتي قد لا يرغب باطلاع الغير عليها، كما قد لا يرغب أن يعلم الغير بإصابته أساساً بالمرض، لاسيما إن كانت تلك الإصابة قد تؤثر على جانب من جوانب حياته، كالجانب الأسري أو الوظيفي أو غيرها مما قد يتأثر سلباً بإصابة الشخص بأحد الأمراض السارية[٢].

وتجدر الإشارة إلى أن نطاق تطبيق الحماية الواردة في المادة المذكورة أعلاه يقتصر على البيانات والمعلومات الشخصية المتعلقة بالمرضى المصابين بأحد الأمراض السارية الواردة في الجدول المرفق بالقانون، ولا تسري الحماية على البيانات والمعلومات المتعلقة بالمرضى المصابين بغيرها من الأمراض مهما بلغت خطورة تلك الأمراض أو شدة الإصابة بها. كما لا تشمل المادة المذكورة كافة البيانات الشخصية الخاصة بالمريض، بل تقتصر الحماية القانونية الواردة فيها على البيانات والمعلومات الشخصية المتعلقة بالمرض فحسب؛ كنتائج التحاليل والاختبارات التي تبين مدى إصابة الشخص بالمرض من عدمه، ومدى خطورة الإصابة، والخطة العلاجية التي سيخضع لها، وغيرها من المعلومات المتعلقة بالمرض الساري الذي يعاني منه المريض.

(١) وبالرغم من الحماية المقررة في هذه المادة إلا أننا نرى بأن صياغتها اللغوية بحاجة إلى تعديل؛ حيث إن النص على أنه: «يحق للأشخاص» قد يبين أو يبادر إلى الأذهان بأن الأمر جوازي أو اختياري في حين أن حماية سرية البيانات والمعلومات الخاصة بالمرضى من المسائل الهامة التي يجب النص عليها بطريقة صريحة وواضحة لا تثير أية إشكاليات أو لبس في مدى إلزاميتها ووجوب الالتزام بها، فحبذا لو يتم النص على أنه: «يجب حماية سرية المعلومات الخاصة بالأشخاص المصابين بأمراض سارية والتي لها علاقة بالمرض، ولا يجوز إفشاء هذه المعلومات إلا في الحالات المقررة قانوناً».

(٢) وننوه بضرورة التأكد من نتائج التحاليل والفحوصات الطبية التي تبين الإصابة بأحد الأمراض السارية، وذلك لما في الأمر من خطورة وتبعات عديدة في حال الخطأ في نتائج تشخيص الإصابة بالأمراض السارية، وفي هذا الصدد أيدت محكمة استئناف أبوظبي حكماً صادراً من المحكمة الابتدائية بإلزام مستشفى بتعويض مريض بمبلغ ٥٠ ألف درهم نتيجة تشخيصه خطأً بإصابته بأحد الأمراض السارية، ما ترتب عليه عزله لمدة ١٦ يوماً وإلزامه ببرنامج علاجي مدته ثمانية أشهر بواقع ١٢ حبة دواء يومياً. مقال بعنوان: ٥٠ ألف درهم تعويضاً لمريض عزل ١٦ يوماً بسبب تشخيص خاطئ، صحيفة الإمارات اليوم، منشور بتاريخ ٢٨ سبتمبر ٢٠٢٠، الموقع الإلكتروني للصحيفة: www.emaratalyoum.com ،آخر زيارة للموقع: ٢٨-٩-٢٠٢٠.

الغصن الثاني
قانون المسؤولية الطبية

أورد قانون المسؤولية الطبية[١] العديد من الأحكام القانونية التي تسري على كل من يزاول إحدى المهن الطبية أو المرتبطة بها في الدولة بهدف توفير البيئة الآمنة لمقدم الخدمة الطبية ومتلقيها في الوقت ذاته[٢]، إلا أنه فيما يتعلق بحماية البيانات الشخصية للمرضى فإنه لم ينص على حماية قانونية صريحة ومباشرة للبيانات، ولم يبين المسؤولية المترتبة على الاعتداء على خصوصية البيانات والمعلومات الشخصية المتعلقة بالمريض أو بحالته الصحية، إلا أنه وبالرغم من ذلك نجد بأن المادة ٧ من قرار مجلس الوزراء رقم ٤٠ لسنة ٢٠١٩ في شأن اللائحة التنفيذية للمرسوم بقانون اتحادي رقم ٤ لسنة ٢٠١٦ بشأن المسؤولية الطبية نصت على أنه: «يجوز للجهات الصحية وضع نظام لتقديم الخدمات الصحية عن بعد، وفقاً للضوابط والشروط الواردة في الملحق المرفق بهذا القرار». فقد أتاح المشرع المجال للجهة الصحية التي ترغب بتقديم خدمات صحية عن بعد وضع نظام خاص لتلك الخدمات، بحيث يبين آلية تقديم الخدمات الصحية عن بعد وكيفية ضمان فعالية تلك الخدمات. وتتمثل الجهات الصحية في وزارة الصحة ووقاية المجتمع وأية جهة حكومية اتحادية أو محلية تعنى بالشؤون الصحية في الدولة[٣].

وتعد البيانات الشخصية للمرضى الخاضعين للعلاج عن بعد من أهم الأولويات التي ينبغي توفير الحماية اللازمة والفاعلة لها، بحيث تتكفل الجهة الحكومية المعنية بوضع نظام تقديم الخدمات الصحية عن بعد ببيان آلية حماية خصوصية البيانات الشخصية للمرضى. وفي هذا الصدد صدرت العديد من الأنظمة واللوائح الخاصة بتقديم الخدمات الصحية عن بعد، ومن أهمها القرار الإداري رقم ٣٠ لسنة ٢٠١٧ باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد[٤]، والتي تهدف إلى توضيح

(١) مرسوم بقانون اتحادي رقم ٤ لسنة ٢٠١٦ بشأن المسؤولية الطبية .

(٢) مقال بعنوان: ورشة تعريفية لشرح مرسوم بقانون اتحادي بشأن المسؤولية الطبية، أصدره صاحب السمو رئيس الدولة، الموقع الرسمي لوزارة الصحة ووقاية المجتمع، www.mohap.gov.ae، منشور بتاريخ ٢٤ سبتمبر ٢٠١٦ .

(٣) المادة الأولى من مرسوم بقانون اتحادي رقم ٤ لسنة ٢٠١٦ بشأن المسؤولية الطبية.

(٤) تشريع محلي خاص بإمارة دبي، صادر عن حميد القطامي المدير العام لهيئة الصحة بدبي، تم نشره في العدد رقم ٤١٢ من الجريدة الرسمية – دبي، تاريخ التوقيع ٢١-٢-٢٠١٧، تاريخ النشر ٩-٣-٢٠١٧ .

المتطلبات الأساسية لتقديم خدمات الرعاية الصحية عن بعد وتوفير أعلى مستويات السلامة والجودة في رعاية المرضى عن بعد[١]، وقد أوردت اللائحة التنفيذية لقانون المسؤولية الطبية[٢] بعض القواعد الحمائية للبيانات الشخصية للمرضى، بحيث ورد فيها بأنه يجب على المهني التأكد من أن مكان مزاولة المهنة آمن، ويضمن توفير الخصوصية، وعازل للصوت، وذلك للحفاظ على سرية معلومات المريض[٣]. كما يجب على المنشأة الصحية توفير معلومات عن خدمات الرعاية الصحية عن بعد المقدمة من خلال البرامج الإلكترونية أو أي وسائل اتصال أخرى، على أن تكون هذه المعلومات صحيحة، وأن توضح حقوق المريض فيما يتعلق بالمعلومات الصحية المتعلقة به[٤]. وفي حال استخدام البريد الإلكتروني كوسيلة من وسائل الاتصال يجب أن يكون ذلك بشكل آمن يضمن خصوصية المريض وسرية معلوماته[٥]. كما ألزمت هذه اللائحة الجهات الصحية المعنية بخدمات الرعاية الصحية عن بعد بوضع لائحة داخلية لتحديد نظام العمل داخل المنشأة الصحية بحيث تتضمن الأسس المتبعة لتوثيق معلومات المرضى بالملف الصحي وأساليب الاحتفاظ بها، وأسس نقل وتخزين البيانات، وكذلك بيان كيفية وصول الطاقم الطبي المختص إلى الملف الصحي للمريض، وتبادل المعلومات والبيانات الخاصة به بما في ذلك استخدام الملفات الطبية الإلكترونية[٦]. ويجب على المنشأة الصحية توفير سياسات وإجراءات موثقة لضمان دقة تدوين خدمات الرعاية الصحية عن بعد، تتضمن منهجية لتوثيق كامل المعلومات والبيانات المتعلقة بالمريض والإرشادات الطبية والعلاج الموصى به في الملف الصحي وفقاً للقوانين الاتحادية واللوائح التنظيمية المعمول بها[٧]. ويتضح

(١) المادة ٣ من القرار الإداري رقم ٣٠ لسنة ٢٠١٧ باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد.

(٢) قرار مجلس الوزراء رقم ٤٠ لسنة ٢٠١٩ في شأن اللائحة التنفيذية للمرسوم بقانون اتحادي رقم ٤ لسنة ٢٠١٦ بشأن المسؤولية الطبية.

(٣) الفقرة الثانية من المادة ١١ من القرار الإداري رقم ٣٠ لسنة ٢٠١٧ باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد.

(٤) الفقرة الثالثة من المادة ٧ من القرار الإداري رقم ٣٠ لسنة ٢٠١٧ باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد.

(٥) الفقرة السابعة من المادة ١٢ من القرار الإداري رقم ٣٠ لسنة ٢٠١٧ باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد.

(٦) المادة ٥ من القرار الإداري رقم ٣٠ لسنة ٢٠١٧ باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد.

(٧) الفقرة الأولى من المادة ١٠ من القرار الإداري رقم ٣٠ لسنة ٢٠١٧ باعتماد اللائحة التنظيمية لخدمات الرعاية الصحية عن بعد.

من هذا أن اللائحة التنظيمية نصت على القواعد العامة والأطر الحمائية الأساسية لتقديم الخدمات الصحية عن بعد، ومن ثم ألزمت المنشآت الصحية المختصة بتقديم تلك الخدمات بوضع السياسات والإجراءات الخاصة بها والتي تضمن حسن سير الخدمات الصحية المقدمة عن بعد بما فيها حماية المعلومات والبيانات الخاصة بالمرضى.

وبالرغم من القواعد الحمائية الخاصة بحماية البيانات والمعلومات الشخصية الواردة في اللائحة التنظيمية، إلا أنها من التشريعات المحلية التي تنطبق على الجهات الصحية التابعة لهيئة الصحة بدبي حصراً دون باقي الجهات المحلية والاتحادية الأخرى. ونرى ضرورة سن تشريعات وقوانين اتحادية تنظم خدمات الرعاية الصحية عن بعد لاسيما في ظل انتشار جائحة كورونا والتي تعاظمت خلالها الحاجة لخدمات الرعاية الصحية عن بعد، فقد شهدت دولة الإمارات العديد من تلك الخدمات المتمثلة في المنصات الإلكترونية المخصصة لتشخيص وعلاج الحالات المرضية، كمنصة الدكتور الافتراضي ومنصة الرعاية الصحية عن بعد وخدمة طبيب لكل مواطن، وغيرها من خدمات التشخيص الطبي والعلاج عن بعد[١].

كما نأمل أن تتم الإشارة في قانون المسؤولية الطبية إلى مسؤولية مقدمي الرعاية الصحية في حال الإخلال بحماية خصوصية البيانات والمعلومات الشخصية المتعلقة بالمرضى، وذلك في حالات تقديم الرعاية الصحية بشكل مباشر أو عن طريق المنصات والخدمات الإلكترونية عن بعد.

الغصن الثالث

قانون استخدام تقنية المعلومات والاتصالات في المجالات الصحية

أصدر المشرع الإماراتي قانوناً اتحادياً ينظم استخدام تقنية المعلومات ووسائل الاتصال الحديثة في المجالات الصحية[٢]، وهو ما يعد خطوة إيجابية وفعالة في ظل تطور

(١) وتجدر الإشارة إلى أنه قد تم الإعلان منذ عام ٢٠١٧ عن قانون اتحادي لتنظيم التطبيب عن بعد، بحيث يحدد اللوائح والأطر التنظيمية للتطبيب عن بعد وتقديم العلاج باستخدام الأجهزة الذكية، إلا أنه لم يتم صدور القانون حتى الآن، وهو ما نأمل أن يتم إصداره بشكل عاجل نظراً لتعاظم الحاجة لقانون اتحادي ينظم العلاج عن بعد، لاسيما في ظل انتشار جائحة كورونا والازدياد الملحوظ في استخدام منصات الرعاية الصحية والعلاج عن بعد. مقال بعنوان: قانون اتحادي يحدد لوائح تنظيم التطبيب عن بعد، صحيفة البيان، منشور بتاريخ ١٣ مايو ٢٠١٧، الموقع الإلكتروني للصحيفة: www.albayan.ae، آخر زيارة للموقع: ١٨-٩-٢٠٢٠.

(٢) قانون اتحادي رقم ٢ لسنة ٢٠١٩ في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية.

الأساليب المستخدمة في المجالات الصحية سواء لتشخيص الحالات المرضية أو علاجها أو غيرها من مراحل تقديم الرعاية الصحية للمريض. وتزداد أهمية هذا القانون في المجالات الصحية في ظل انتشار جائحة كورونا، بحيث تعددت أساليب تقنية المعلومات والاتصالات المستخدمة في المجال الطبي أثناء تفشي الجائحة. وتتمثل أهم أهداف القانون في ضمان الاستخدام الأمثل لتقنية المعلومات والاتصالات في المجالات الصحية، بالإضافة إلى ضمان أمن وسلامة البيانات والمعلومات الصحية[١]، ويسري هذا القانون على جميع أساليب واستخدامات تقنية المعلومات والاتصالات في المجالات الصحية في الدولة[٢].

ومن أهم القواعد الحمائية للبيانات الشخصية للمريض الواردة في هذا القانون، ما ورد في المادة ٤ منه والتي تنص على أنه: «يتعين عند استخدام تقنية المعلومات والاتصالات في المجالات الصحية الالتزام بما يأتي:١- المحافظة على سرية البيانات والمعلومات الصحية، وذلك بعدم السماح بتداولها في غير الأحوال المصرح بها. ٢- ضمان صحة ومصداقية البيانات والمعلومات الصحية، وذلك بالمحافظة على سلامتها من التخريب أو التعديل أو التحوير أو الحذف أو الإضافة غير المصرح بها». كما نصت المادة ١٦ من القانون ذاته على أنه: «يجب على كل من يتداول المعلومات الخاصة بالمرضى المحافظة على سريتها، وعدم استخدامها لغير الأغراض الصحية، دون موافقة خطية من المريض». وقد اشترط القانون تدريب وتأهيل الكوادر البشرية وتوفير الإمكانيات والبيئة الملائمة بهدف ضمان أمن وسلامة البيانات والمعلومات الصحية بما يتوافق مع أفضل الممارسات الدولية[٣]، أضف إلى ذلك ما ورد في القانون بشأن إنشاء المنظومة المركزية[٤] من قبل وزارة الصحة ووقاية المجتمع بالتنسيق مع الجهات الصحية المعنية، والتي تختص بحفظ وتبادل وتجميع البيانات والمعلومات الصحية[٥].

(١) المادة الثالثة من قانون اتحادي رقم ٢ لسنة ٢٠١٩ في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية.

(٢) المادة الثانية من قانون اتحادي رقم ٢ لسنة ٢٠١٩ في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية.

(٣) المادة ١٩ من قانون اتحادي رقم ٢ لسنة ٢٠١٩ في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية.

(٤) وقد عرفها القانون في المادة الأولى منه بأنها: «مجموعة عمليات للتبادل الإلكتروني للبيانات والمعلومات الصحية، وتشمل مجموعة الأجزاء أو العناصر الإلكترونية التي تربط بعضها ببعض علاقات تعمل معاً، نحو تحقيق هدف معين».

(٥) المادة ٥ من قانون اتحادي رقم ٢ لسنة ٢٠١٩ في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية . للمزيد حول المنظومة المركزية انظر: المواد ٦-١٥ من القانون ذاته، وكذلك: قرار مجلس الوزراء رقم ٣٢ لسنة ٢٠٢٠ بشأن اللائحة التنفيذية للقانون الاتحادي رقم ٢ لسنة ٢٠١٩ في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية.

ويثور التساؤل في هذا الصدد عما إذا كانت التقنيات والآليات المستحدثة لمواجهة فيروس كورونا تدخل ضمن نطاق تطبيق قانون استخدام تقنية المعلومات والاتصالات في المجالات الصحية ؟ ومما نراه بأن التقنيات والآليات المستحدثة لمواجهة فيروس كورونا تدخل ضمن نطاق تطبيق القانون لاسيما وأنه كما أسلفنا فإن المادة الثانية من القانون قد نصت صراحة على سريان القانون على جميع أساليب واستخدامات تقنية المعلومات والاتصالات في المجالات الصحية في الدولة. ويجب توافر شرطين لذلك؛ يتمثل أولهما في وجوب دخول تلك الوسائل والآليات المستحدثة في نطاق تعريف القانون لتقنية المعلومات والاتصالات، فقد جاء في المادة الأولى من القانون أن تقنية المعلومات والاتصالات تعني: «الأدوات أو النظم التقنية والإلكترونية أو الوسائل الأخرى التي تتيح إمكانية معالجة المعلومات والبيانات بكافة أنواعها، ويشمل ذلك إمكانية تخزينها واسترجاعها ونشرها وتبادلها»، أما الشرط الثاني، فيتمثل في وجوب استخدام تلك التقنيات والآليات المستحدثة لمواجهة فيروس كورونا في المجالات الصحية.

الفرع الثاني
تقييم فعالية قواعد الحماية القانونية

اهتم المشرع الإماراتي بسن تشريعات خاصة بالمجال الصحي في الدولة، وقد تجلى هذا الاهتمام في ظل انتشار جائحة كورونا، فنجد أن التشريعات الصحية مواكبة للتغيرات والتطورات التي تمر بها دول العالم عامة ودولة الإمارات العربية المتحدة خاصة، وقد أجرت الدولة تعديلاً على الجدول المرفق بقانون مكافحة الأمراض السارية بمجرد تفشي جائحة كورونا[١]، وذلك بإضافة فيروس كورونا المستجد إلى جدول الأمراض السارية الوارد في اللائحة التنفيذية لقانون مكافحة الأمراض السارية، وذلك وفقاً للقرار الوزاري رقم ٢٣٢ لسنة ٢٠٢٠ بشأن تعديل جدول الأمراض السارية المرفق باللائحة التنفيذية للقانون الاتحادي رقم ١٤ لسنة ٢٠١٤[٢].

كما صدرت العديد من التشريعات والقرارات لمواجهة فيروس كورونا المستجد، من أهمها قرار النائب العام للدولة رقم ٣٨ لسنة ٢٠٢٠ وتعديلاته للحد من انتشار فيروس كورونا المستجد (كوفيد ١٩)، وذلك من خلال قائمة بالمخالفات والغرامات

(١) وذلك بتاريخ ٣٠-٣-٢٠٢٠ .

(٢) نصت المادة الأولى من القرار على أنه: «يضاف إلى الجدول (د) المرفق بقرار مجلس الوزراء رقم ٣٣ لسنة ٢٠١٦ باللائحة التنفيذية للقانون الاتحادي رقم ١٤ لسنة ٢٠١٤ بشأن مكافحة الأمراض السارية ما يلي: فيروس كورونا المستجد (كوفيد ١٩)، متلازمة الشرق الأوسط التنفسية».

التي تم الإعلان عنها والبدء بتطبيقها منذ ٢٦ مارس ٢٠٢٠ والمتعلقة بمخالفة إجراءات الصحة والسلامة المطبقة للسيطرة على انتشار فيروس كورونا في الدولة. ومنها المخالفات والغرامات المترتبة على عدم الالتزام بالتعليمات الخاصة بالتباعد الاجتماعي، وعدم الالتزام بالقرارات الصادرة بشأن العزل الصحي والحجر المنزلي، والخروج من المنازل دون مقتضى أو ضرورة في أوقات التعقيم الوطني، وغيرها من المخالفات والغرامات لمخالفي الإجراءات الضرورية المتبعة لاحتواء الفيروس والحد من انتشاره(١).

إلا أنه فيما يتعلق بالقواعد الحمائية المتعلقة تحديداً بحماية البيانات والمعلومات الشخصية لمرضى كورونا في التشريعات الصحية، نجد أن التشريعات الصحية قد نصت على بعض قواعد حماية البيانات الشخصية للمرضى، إلا أنها متفرقة في العديد من القوانين واللوائح التشريعية ومخصصة لبيانات ومعلومات خاصة ومحددة.

فقانون مكافحة الأمراض السارية كفل الحماية لبيانات المرضى المصابين بأحد الأمراض السارية المحددة في الجدول المرفق بالقانون فحسب، بحيث إن الحماية لا تشمل بيانات المرضى المصابين بغيرها من الأمراض، كما أن الحماية المقررة في هذا الصدد لا تنطبق على كافة المعلومات والبيانات الشخصية للمرضى وإنما تقتصر تحديداً على البيانات المتعلقة بالمرض الساري الذي تأكدت إصابتهم به.

أما فيما يتعلق بقانون المسؤولية الطبية فلم يتطرق إلى مسؤولية مقدمي الرعاية الصحية في حال الإخلال بالتزامهم بحماية سرية المعلومات والبيانات الخاصة بالمرضى، علاوة على ذلك فإن اللائحة التنفيذية للقانون لم تشر إلى تلك المسؤولية بحيث إنها لم تنص أساساً على الالتزام بحماية سرية البيانات والمعلومات الخاصة بالمرضى . واكتفى قانون المسؤولية الطبية ولائحته التنفيذية بإناطة مسؤولية وضع الأنظمة واللوائح الخاصة بتقديم الخدمات الصحية، بالجهات الصحية المتمثلة في وزارة الصحة ووقاية المجتمع، وأية جهة حكومية اتحادية أو محلية تعنى بالشؤون الصحية في الدولة.

إلا أننا نرى بأنه من الأجدر أن يتم رسم أطر الحماية القانونية الأساسية في القوانين الاتحادية، ومن ثم ترك المسائل التفصيلية للجهات الصحية المعنية في الدولة، فعلى سبيل المثال، لو سلطنا الضوء على تقديم خدمات الرعاية الصحية عن بعد، نجد

(١) تشريعات مكافحة فيروس كورونا المستجد (كوفيد ١٩)، البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة، https://u.ae/ar-AE#/ ، آخر زيارة للموقع: ١-١٠-٢٠٢٠.

بأنه لا يوجد قانون اتحادي ينظم تقديم الخدمات الصحية عن بعد في الدولة، وإنما تقتصر التشريعات في هذا الصدد على القرارات الإدارية والقوانين المحلية الخاصة بكل إمارة على حدة، وهو ما يثير إشكالية تعدد القوانين المطبقة على خدمات الرعاية الصحية عن بعد بحسب الإمارة التي يتم تقديم الخدمة من خلالها، لاسيما في تزايد تقديم الخدمات الصحية عن بعد في ظل انتشار جائحة كورونا. كما تتجلى الإشكالية في وجود خدمات مشتركة بين عدد من الجهات الحكومية الاتحادية والمحلية في الدولة، كتطبيق الحصن الذي يعد مبادرة مشتركة بين وزارة الصحة ووقاية المجتمع، ودائرة الصحة بأبو ظبي، وهيئة الصحة بدبي.

ونحن نعتقد إن في وجود قانون اتحادي ينظم تقديم الخدمات الصحية عن بعد، ما يكفل الحماية القانونية اللازمة في هذا الصدد، وتحديداً حماية البيانات والمعلومات الخاصة بالمرضى المستفيدين من تلك الخدمات، ويزيل كافة الملابسات والإشكاليات التي تقع بسبب تحديد القانون المحلي الواجب التطبيق على التقنيات والآليات المستخدمة في المجال الصحي، بالإضافة إلى توحيد قواعد الحماية على مستوى الدولة دون وجود مغايرات واختلافات بين القوانين المحلية.

وفيما يتعلق بقرارات النائب العام لمواجهة فيروس كورونا المستجد، فهي قد تطرقت لمخالفات حماية البيانات الشخصية للمصابين بفيروس كورونا والخاضعين للعلاج أو الفحص، بحيث ورد في قرار النائب العام رقم ٣٨ لسنة ٢٠٢٠ وتعديلاته غرامة مقدارها ٢٠٠٠٠ درهم لكل من يقوم بجمع أو نسخ أو نقل أو تداول بيانات أو معلومات صحية عن المصابين بالفيروس الذين يتلقون علاجاً لدى الجهات الصحية، أو إلغاء أو حذف أو دمج تلك البيانات أو المعلومات، بالإضافة إلى غرامة مقدارها ٥٠٠٠ درهم عند عدم الالتزام بمعايير أمن المعلومات المعتمدة في المنشآت الصحية الحكومية أو الخاصة أو الإخلال بها.

وبشأن قانون استخدام تقنية المعلومات والاتصالات في المجالات الصحية فنشيد بما ورد فيه من أحكام حماية البيانات والمعلومات الشخصية للمريض، لاسيما وأن القانون يسري على كافة أساليب واستخدامات تقنية المعلومات والاتصالات في المجالات الصحية في الدولة. إلا أنه تثار في هذا الصدد بعض التساؤلات المتعلقة بالتقنيات والآليات المستحدثة لمواجهة فيروس كورونا المستجد، فهل تسري القواعد الحمائية الواردة في قانون استخدام تقنية المعلومات والاتصالات في المجالات الصحية واللوائح الخاصة بتقديم الرعاية الصحية عن بعد على تلك التقنيات والآليات المستحدثة؟ الإجابة عن هذا التساؤل

تتم من خلال تحديد نوع وطبيعة عمل تلك التقنيات والآليات المستحدثة لمواجهة الفيروس، ففيما يتعلق بالمنصات الإلكترونية المخصصة لتشخيص وعلاج الحالات المرضية عن بعد، فهي تدخل في نطاق تطبيق تلك القوانين لاسيما فيما يتعلق بالقرارات الإدارية واللوائح المتعلقة بتنظيم تقديم خدمات الرعية الصحية عن بعد، وذلك وفقاً لنطاق تطبيق تلك القرارات واللوائح. كما تدخل في نطاق تطبيق هذا القانون تطبيقات الرصد الإلكتروني والمتمثلة في تطبيق الحصن، وتطبيق تتبع (كوفيد ١٩)، وتطبيق ابق في المنزل، لاسيما أن القانون يسري على جميع أساليب واستخدامات تقنية المعلومات والاتصالات في المجالات الصحية في الدولة[١]. ونشيد بشمول نطاق تطبيق القانون على كافة المجالات الصحية وعدم اقتصار نطاق تطبيقه على العلاج أو المسائل الطبية المتخصصة، فاستخدام مصطلح المجالات الصحية يوسع من نطاق تطبيق القانون بحيث يشمل كافة ما يتعلق بالمجال الصحي حتى وإن لم يتطرق لعلاج المرضى كما هو الحال في تطبيقات الرصد الإلكتروني.

على إن الإشكال يثور بشأن وسائل التتبع الإلكترونية المستخدمة لمراقبة المصابين بفيروس كورونا ممن تقرر إلزامهم بالعزل المنزلي، وذلك لتحديد أماكن تواجدهم وضمان عدم مخالطتهم لأفراد المجتمع، كسوار المراقبة الإلكتروني والساعة الإلكترونية الذكية، فهل تعد تلك الآليات والوسائل من قبيل التقنيات المستخدمة في المجال الصحي بحيث تدخل ضمن نطاق تطبيق قانون استخدام تقنية المعلومات والاتصالات في المجالات الصحية؟ نحن نرى بأنه يمكن اعتبار وسائل التتبع الإلكتروني من قبيل التقنيات المستخدمة في المجال الصحي التي تدخل ضمن نطاق تطبيق القانون؛ ذلك أنها من التقنيات التي تخدم المجال الصحي وتم استحداثها لغايات مراقبة المرضى المصابين، فهي وإن كانت لا تستخدم للعلاج أو العمليات والتقنيات الطبية بشكل صريح، إلا أنها تخدم المجال الصحي ولا تخرج عن نطاقه، أضف إلى ذلك أن غالبية وسائل التتبع الإلكترونية مزودة بخاصية قياس ومراقبة الوظائف الحيوية لجسم الإنسان، كقياس حرارة الجسم ومعدل نبضات القلب وغيرها من الخاصيات والعمليات التي تدخل ضمن نطاق المجال الصحي.

وعليه نرى بأنه يمكن تطبيق قانون استخدام تقنية المعلومات والاتصالات في المجالات الصحية على وسائل التتبع الإلكترونية، وذلك إلى حين سن تشريعات خاصة تنظم طبيعة عمل وسائل التتبع الإلكترونية المستخدمة لمراقبة المرضى، كتلك القوانين والتشريعات التي

(١) وذلك في المادة الثانية من القانون.

تنظم عمل السوار الإلكتروني المستخدم في نظام المراقبة الإلكترونية المستحدث بالمرسوم بقانون اتحادي رقم ١٧ لسنة ٢٠١٨ بتعديل بعض أحكام قانون الإجراءات الجزائية[١].

وفي هذا الصدد تجدر الإشارة إلى أن رأينا في تصنيف الآليات والتقنيات المستحدثة لمواجهة فيروس كورونا وتحديد القوانين الواجبة التطبيق عليها ما هي إلا اجتهادات فقهية دعت إليها الحاجة في ظل غياب التشريعات الصريحة التي تبين الإطار القانوني الذي يحكم تطبيق تلك الآليات والتقنيات الحديثة، وهو ما يتوجب معه سن قوانين تحسم أية نزاعات قد تصدر بخصوص تلك التقنيات، وتبين طبيعة عملها، والقانون الواجب التطبيق عليها، والمسؤولية المترتبة في حال سوء استخدامها أو اختراق أنظمتها أو غيرها مما قد تتعرض له تلك التقنيات والآليات المستحدثة، لاسيما وأن التقنيات والآليات لا تقتصر على ما تم بحثه وتسليط الضوء عليه في هذه الدراسة، وإنما تستحدث تقنيات ووسائل إلكترونية جديدة بشكل مستمر ومتواصل.

وبشأن حماية المعلومات والبيانات الشخصية لمستخدمي تلك التقنيات، فإننا نؤكد على ضرورة استحداث قانون خاص بحماية البيانات الشخصية بحيث يوفر حماية وتنظيم شامل لكافة البيانات والمعلومات الشخصية بمختلف أنواعها ومصادرها.

الخاتمة

بعد أن بينا المخاطر التي تواجهها البيانات الشخصية في ظل انتشار جائحة كورونا، لاسيما مع الانتقال والتحول السريع والمفاجئ إلى العالم الرقمي، واستخدام العديد من الآليات والتقنيات الحديثة لغايات العلاج أو مراقبة مرضى فيروس كورونا ومخالطيهم، فقد تبين بأن المشرع الإماراتي أورد حماية قانونية للبيانات الشخصية لمرضى كورونا، إلا أنها حماية قاصرة وغير كافية لتفادي المخاطر التي تتعرض لها البيانات الشخصية في ظل انتشار الجائحة.

---

(١) وذلك في المادة الثانية من المرسوم والتي تقضي بإضافة فصل بعنوان الوضع تحت المراقبة الإلكترونية (المواد ٣٥٥ – ٣٨٥)، وذلك في الباب الثالث المعنون بالإجراءات الجزائية الخاصة في الكتاب الخامس من القانون الاتحادي رقم ٣٥ لسنة ١٩٩٢ بإصدار قانون الإجراءات الجزائية وتعديلاته. كما صدر في هذا الشأن قرار مجلس الوزراء رقم ٥٣ لسنة ٢٠١٩ بشأن تنفيذ المراقبة الإلكترونية، والتعميم الصادر من النائب العام للدولة رقم ١١ لسنة ٢٠١٩ بشأن إرشادات تنفيذ النظام من الناحية العملية. انظر أكثر حول هذا الموضوع: جيهان العرفاوي، العقوبات البديلة في القانون الجزائي الإماراتي، المراقبة الإلكترونية نموذجاً، مقال منشور على موقع مكتب السويدي ومشاركوه للمحاماة والاستشارات القانونية، بتاريخ ١٣ فبراير ٢٠٢٠، www.alsuwaidi.ae، آخر زيارة للموقع: ١-٨-٢٠٢٠.

وعليه فقد توصلنا في نهاية هذا البحث إلى بعض النتائج والتوصيات نوردها على النحو التالي:

أولاً- النتائج:

من المؤكد أن ظهور جائحة كورونا وفرض الإجراءات اللازمة لمواجهتها والحد من انتشارها أدى إلى الانتقال السريع إلى العالم الرقمي أو الافتراضي دون أن يصاحب ذلك تقدم موازٍ في وسائل الأمن والحماية للبيانات والمعلومات المتداولة، وهو ما أدى بدوره إلى زيادة المخاطر على البيانات الشخصية للأفراد، لاسيما مرضى كورونا ممن تحتم عليهم استخدام بعض الآليات والتقنيات الذكية المستحدثة لمواجهة الفيروس، وذلك تحت طائلة العقوبة والمسائلة القانونية.

وقد زاد من المخاطر التي تعرضت لها البيانات الشخصية في ظل انتشار جائحة كورونا (كوفيد ١٩) والانتقال إلى العالم الرقمي، استخدام هذه البيانات على نطاق واسع في مختلف التقنيات والآليات المستحدثة لمواجهة الفيروس، مما عرضها لمخاطر الاستخدام غير المشروع، بالإضافة إلى المخاطر المترتبة على تتبع ومراقبة الأفراد – وتحديداً المصابين بالفيروس – وذلك نتيجة لاستخدام برامج الرصد الإلكتروني.

في ظل المخاطر المتزايدة على البيانات الشخصية نجد بأن المشرع الإماراتي جرم التعرض إلى الخصوصية عموماً، وإلى بعض جوانب البيانات الشخصية خصوصاً، حيث أوردت القواعد العامة في القانون الإماراتي أحكاماً حمائية للبيانات الشخصية، تفرقت في مختلف القوانين الاتحادية والمحلية على مستوى الدولة.

بالرغم من اهتمام المشرع الإماراتي ببعض جوانب حماية البيانات والمعلومات الشخصية، إلا أن هذا الاهتمام يبقى محدوداً ولا يلائم الأهمية التي تحظى بها البيانات الشخصية، ومستوى المخاطر التي تتعرض لها، خصوصاً في العالم الافتراضي. وظل النظام القانوني الإماراتي خلواً من تشريع خاص بحماية البيانات الشخصية، رغم ظهور العديد من التشريعات في القانون المقارن يمكن الاستفادة منها في إصدار تشريع ينظم الموضوع.

ثانياً - التوصيات:

ضرورة إصدار قانون اتحادي خاص بحماية البيانات الشخصية في الدولة، يستلهم من التشريعات المقارنة أفضل ما تضمنته، مع إضافة ما يلائم المنظومة التشريعية في دولة الإمارات العربية المتحدة، لاسيما وأن المخاطر المترتبة على البيانات الشخصية

في تزايد مستمر في ظل أساليب الاختراق والمعالجة المستحدثة التي أوجدها التقدم العلمي والتكنولوجي في الآونة الأخيرة. ولحين صدور قانون خاص بحماية البيانات الشخصية ينبغي الرجوع للحماية المقررة وفقاً لقانون مكافحة جرائم تقنية المعلومات، الذي نص على بعض القواعد الحمائية التي يمكن الاستناد إليها لحماية خصوصية البيانات الشخصية. كما يمكن الرجوع أيضاً إلى قواعد ضمان الفعل الضار في قانون المعاملات المدنية الإماراتي، بحيث يتم تعويض من تم الاعتداء على بياناته الشخصية إذا تسبب هذا الاعتداء في الإضرار به.

ضرورة مواكبة التشريعات الصحية في الدولة للآليات والتقنيات المستحدثة لمواجهة مختلف الجوائح المرضية، ومنها فيروس كورونا المستجد/ (كوفيد ١٩)، وبيان الإطار القانوني لتلك الآليات والتقنيات الحديثة، لاسيما تلك المستخدمة في قطاع الرعاية الصحية، بحيث يتم بيان طبيعة عملها والقانون الواجب التطبيق بشأنها والمسؤولية المترتبة في حال سوء استخدامها أو اختراق أنظمتها أو غيرها مما قد تتعرض له تلك التقنيات والآليات المستحدثة، لاسيما وأن التقنيات والآليات المستخدمة في المجال الصحي تستحدث بشكل مستمر ومتواصل.

ضرورة أن تطور المؤسسات المختلفة في الدولة وسائل الأمن والحماية لمختلف البرامج والتقنيات التي تستخدمها في تقديم خدماتها، وأن لا يكون هدفها الأول تقديم الخدمة وتسيير الأعمال، على حساب أمن المعلومات والبيانات الشخصية التي تتراجع في أولوياتها إلى المرتبة الثانية.

المراجع

أولاً- الكتب القانونية:

- إعاد علي القيسي، **مبادئ القانون الدستوري وأنظمة الحكم**، دراسة تحليلية مقارنة لدستور الإمارات العربية المتحدة، الطبعة الأولى، ٢٠١٣ .
- حسام الدين كامل الأهواني، **الحق في احترام الحياة الخاصة**، الحق في الخصوصية، دار النهضة العربية، دون سنة نشر.
- سرحان حسن المعيني، **جرائم التطبيقات الذكية**، أكاديمية العلوم الشرطية، الشارقة، دولة الإمارات العربية المتحدة، ٢٠١٦ .
- سهير منتصر، **النظرية العامة للحق**، منشورات جامعة الزقازيق، مصر، ٢٠٠٦ .
- عبد الرازق الموافي عبد اللطيف، **شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة**، الكتاب الأول، سلسلة الدراسات القانونية والقضائية، عدد ١٥، معهد دبي القضائي، دبي، ٢٠١٦ .
- عمر محمد أبو بكر يونس، **الجرائم الناشئة عن استخدام الإنترنت**، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، جمهورية مصر العربية، ٢٠٠٤ .
- محمد محرم محمد، خالد محمد المهيري، **قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقهاً وقضاءً**، دار الفتح للطباعة والنشر، الطبعة الثانية، ١٩٩٢ .
- وفاء حلمي، **محاضرات في نظرية الحق**، منشورات جامعة الزقازيق، مصر، ٢٠٠٧.
- وليد السيد سليم، **ضمانات الخصوصية في الإنترنت**، دار الجامعة الجديدة، الإسكندرية، مصر، ٢٠١٢.

ثانياً: الأبحاث المنشورة في المجلات العلمية:

- أحمد جاد منصور، **ضمانات الحق في حرمة الحياة الخاصة في المواثيق الدولية لحقوق الإنسان والقوانين الوطنية**، المجلة العربية للإدارة - المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، إصدار خاص، ٢٠١٣ .
- حسام الدين كامل الأهواني، **الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني**، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، العدد الأول، ١٩٩٠.

- حسام محمد نبيل الشنراقي، **حماية البيانات الشخصية عبر الإنترنت**، المجلة العربية للإدارة – المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، ملحق العدد ٢، مجلد ٣٨، ٢٠١٨.

- خالد المسلمي، **المستحدث من الأحكام الصادرة من محكمة النقض**، مجلة القضاء والقانون، مركز البحوث والدراسات القضائية بدائرة القضاء – أبو ظبي، عدد خاص بفيروس كورونا (كوفيد ١٩)، السنة السادسة، يوليو ٢٠٢٠.

- سامح عبدالواحد التهامي:

- **الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي**، مجلة الحقوق، جامعة الكويت، مجلد ٣٥، عدد ٣، ٢٠١١.

- **نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها**، دراسة في القانون الإماراتي، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، كلية الحقوق، مصر، عدد ٦٧، ٢٠١٨.

- طارق جمعة السيد، **الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن**، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، عدد ٢، ٢٠١٧.

- مصطفى بن قارة، **الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية**، مجلة الندوة للدراسات القانونية، الجزائر، عدد ١٣، ٢٠١٧.

ثالثاً: الأبحاث المقدمة في المؤتمرات والندوات :

- جبالي أبو هشيمة كامل، **حماية البيانات الشخصية في البيئة الرقمية**، بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق، جامعة آسيوط، مصر، ١٢-١٣ أبريل ٢٠١٦.

- زايد الشامسي، **الضوابط القانونية لاستخدام وسائل التواصل الاجتماعي**، منتدى نحو مجتمع رقمي آمن، جمعية أم المؤمنين، عجمان، بتاريخ ٢٣ سبتمبر ٢٠٢٠، عبر تطبيق زوم zoom .

- عبيد صالح المختن، **طرق الوقاية من أساليب الاختراق الإلكتروني**، منتدى نحو مجتمع رقمي آمن، جمعية أم المؤمنين، عجمان، بتاريخ ٢٣ سبتمبر ٢٠٢٠، عبر تطبيق زوم zoom .

- محمد خليفة الغفلي، **ندوة الجرائم الإلكترونية في فترة التعقيم الوطني**، غرفة تجارة وصناعة عجمان، بتاريخ ٢٣ سبتمبر ٢٠٢٠، ندوة إلكترونية عبر برنامج زوم: zoom .

رابعاً: الأبحاث المنشورة في المواقع الإلكترونية :

- جيهان العرفاوي، **العقوبات البديلة في القانون الجزائي الإماراتي - المراقبة الإلكترونية نموذجاً**، مقال منشور على موقع مكتب السويدي ومشاركوه للمحاماة والاستشارات القانوني، بتاريخ ١٣ فبراير ٢٠٢٠، www.alsuwaidi.ae، آخر زيارة للموقع: ١-٨-٢٠٢٠.
- محمد أحمد المعداوي، **حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي**، بحث منشور على الموقع الإلكتروني لجامعة بنها، جمهورية مصر العربية، الموقع الرسمي للجامعة: www.bu.edu.eg، آخر زيارة للموقع: ١٢-١٠-٢٠٢٠.

خامساً- المواقع الإلكترونية :

- الموقع الإلكتروني للبوابة الرسمية لحكومة الإمارات https://u.ae/ar-AE
- الموقع الرسمي لمركز محمد بن راشد للابتكار الحكومي https://ibtekr.org
- الموقع الرسمي لمنظمة حقوق الإنسان www.hrw.org
- الموقع الرسمي لوزارة الصحة ووقاية المجتمع www.mohap.gov.ae

Legal effects of the Coronavirus / COVID-19 pandemic On the protection of personal data

Eman Khamiss Alyahyaee
Phd Studente\ researcher in private law
University of Sharjah-UAE

Prof. Adnan Ibrahim Sarhan
Professor of civil law & Assistant Chancellor
for branch affaires, University of Sharjah-UAE

The spread of the new Corona pandemic, Covid 19, and the measures taken to confront it, have led to a move away from the physical and tangible rapprochement in the provision of various services and work in various fields. So that imposed social distancing measures applied in various countries of the world, specifically United Arab Emirates, the transition to the digital or virtual world. UAE has introduced many technologies and mechanisms developed to confront the emerging corona virus, Covid 19, in order to detect cases infected with the virus and cases that have been in contact with it, and to impose the necessary measures represented in quarantining the infected, in order to ensure that they do not come into contact with community members so that the virus is restricted and its spread is limited. In addition to using the new technologies and mechanisms to continue providing remote health care services. However, the shift to digital and the use of modern technologies and mechanisms to confront the virus increased the risks to the personal data of the users of these technologies and the new mechanisms and the beneficiaries of them, especially Corona patients who had to use these modern technologies under penalty and legal accountability. In addition to the risks involved in tracking and monitoring individuals through the use of smart applications and mechanisms used to track Corona patients and monitor their whereabouts in order to ensure that they remain in the place of isolation scheduled for them and not to come into contact with community members, which exposes them to infection with the virus. Especially since the electronic monitoring techniques are not limited to Corona patients only, but the concerned authorities in the state have called on all members of society to use these modern technologies. In light of the increasing risks to the protection of personal data, we decided to shed light on the legal rules established for the protection of personal data under the UAE law. Although there is no law for the protection of personal data in the country, there are some protective rules contained in the general rules of the law, as stipulated in health

legislation The country has protective rules regarding the personal data of patients and recipients of health care services. This necessitates stating these protective rules and their adequacy and effectiveness in providing legal protection for the personal data of Corona pandemic patients.