حماية البيانات الشخصية الرقمية

وفقاً لأحكام القانون المصرى رقم ١٥١ لسنة ٢٠٢٠

(حماية البيانات الشخصية المعالجة إلكترونياً)

بين الواقع والمأمول

دكتور

سيد أحمد محمود

أستاذ قانون المرافعات

كلية الحقوق - جامعة عين شمس

مقدمة

فى ظل ازدياد التعاملات الإلكترونية بشكل يومي ومشاركة الأشخاص معلوماتهم الشخصية مع جهات عامة أو خاصة، وفى ظل توجه الدولة إلى التحول الرقمي بدلاً من المعاملات الورقية، تتجلى قيمة الأمن الرقمي وأهمية الحفاظ علية بشكل أكبر (م ٣١ من الدستور المصرى، وكذلك المواد ٢١، ٢٢، ٢٥، ٥٧، ٦٨منه)، وتظهر بالتالي أوجه الخلل التى قد تصيب هذا الأمان، وتخلق مستفيدين بشكل غير قانونى من البيانات الشخصية سواء بطريق مباشر أو بتبعيتها لشركات تجارية وغيرها من الكيانات. وهنا يأتي دور التشريع بالضرورة ليحقق الحماية القانونية لهذه البيانات، لذا صدر فى عام ٢٠١٨ فى مصر قانونى جرائم تقنية المعلومات وتنظيم وسائل الإعلام والتى أدت إلى تطبيق مراقبة الحياة الإلكترونية وبالتالي تقييد الحريات الرقمية.

وفى يونيو عام ٢٠٢٠ صدر فى مصر قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠[١] ومن خلاله تسعى الدولة المصرية إلى فرض سيطرتها على المجال الرقمي وتداول

(١) نشر فى الجريدة الرسمية – العدد ٢٨ مكرر (هـ) فى ١٥ يولية ٢٠٢٠ حددت المادة الاولى من قانون الإصدار نطاق سريانه من حيث الأشخاص المستفيدين من الحماية (الأشخاص الطبيعية) والملزمين بها (الحائز أو المحتكم أو المعالج) وموضوع الحماية للبيانات الشخصية المعالجة جزئياً أو كلياً ، وحددت كذلك المادة الثانية منه سريانه من حيث المكان على كل من يرتكب احدى الجرائم المنصوص عليه فيه متى كان الجاني من المصريين داخل أو خارج مصر أو كان من غير المصرين المقيمين فى داخل الجمهورية أو من غير المصرين خارج الجمهورية إذا كان الفعل معاقباً عليه فى الدولة التى وقع فيها تحت أي وصف قانونى وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية.

كما أوضحت المادة الثالثة منه حالات عدم سريانها على البيانات التى يحتفظ بها الأشخاص الطبيعيون للغير ويتم معالجتها للاستخدام الشخصي أو تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو القانونية أو حصراً للأغراض الإعلامية أو متعلقة بعناصر الضبط القضائي والتحقيقات والدعاوى القضائية أو لدى جهات الأمن القومي صراحه(الرئاسة ، الدفاع ، الداخلية ، المخابرات العامة ، هيئة الرقابة الإدارية) أو لدى البنك المركزي المصرى والجهات الخاضعة لرقابته وإشرافه عدا شركات تحويل الأموال والصرافة ، والوزير المختص هو وزير الاتصالات وتكنولوجيا المعلومات (م ٤) ، وتختص المحكمة الاقتصادية بنظر الجرائم الناشئة عنه (م ٥) ، ومدة توفيق الأوضاع سنة (م ٦)، ويعمل به بعد ٣ شهور بعد نشره فى الجريدة الرسمية (م ٧) .

البيانات ، ويعمل هذا القانون على تحقيق المعايير الدولية [٢] فى هذا المجال وكذلك الضمانات الدستورية المقررة له ، وكذلك القوانين الأخرى بما يعمل على الحفاظ على حق الشخص فى التعبير وكذلك ضماناً للحقوق والحريات الشخصية وحتى لا يتم استخدام البيانات بشكل غير قانونى من قبل سلطات الدولة أو غيرها .

ويهدف قانون حماية البيانات الشخصية المصرى رقم ١٥١ لسنه ٢٠٢٠ (م ٧ إصدار ، م ٤٤)[٣]الى وضع إطار قانونى يشكل للمستخدم حماية بياناته التى خضعت للمعالجة الإلكترونية وذلك من خلال الحفاظ على عدة حقوق فرعية مثل الحق فى معرفه طبيعة البيانات التى يمتلكها الحائز على البيانات والمعالج لها ، كما يسمح للمعنى بالبيانات بتقديم شكوى ضد مستخدمي البيانات ومقاضاتهم إذا استدعى الأمر ذلك . ويخاطب القانون أيضا الشركات والمؤسسات التجارية التى تتعامل مع قواعد البيانات الخاصة بالمستخدمين ويحدد على أساس ذلك المعايير التى تحكم العلاقة بين المستخدمين والشركات الرقمية ، ومن هذا المنطق نص القانون على إنشاء مركز حماية البيانات الرقمية لتكون مهامه الرقابة على تنفيذ القانون وإصدار التراخيص والتصاريح والاعتمادات للشركات التى تقوم بمعالجة واستخدام البيانات الشخصية للمستخدمين وكذلك توجيه الإرشادات اللازمة لتطبيق القانون ، وهذا التوجه محمود لأنه يواكب التطورات الإلكترونية فى الحياة العامة والخاصة ، ولكن يثار التساؤل هل يحافظ هذا القانون بشكل كامل على الحريات الرقمية ؟ وكذلك نسعى إلى قياس مدى فاعلية القانون المصرى فى حماية بيانات

---

(٢) بصدد المعايير الدولية فعرفة طريق لتشريع قوانين حماية البيانات الشخصية ، انظر آلاء كليب ، قانون حماية البيانات الشخصية فى ضوء المعايير الدولية ، ١٤ يوليو ٢٠٢١ ،مؤسسة الفكر والتعبير (afte) .

(٣) كما اصدر المشرع القطري القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية ، انظر طارق جمعة السيد راشد ، الحماية القانونية لخصوصية البيانات الشخصية فى القانون القطري والمقارن ، المجلة القانونية والقضائية ، وزارة العدل القطرية ، مركز الدراسات القانونية والقضائية ، ياسر عبد السلام ، القانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية ، نفس المجلة ، ص ٤٩٧ – ٥٢٣ ، إكرام سليمان فجم ، الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي فى القانون القطري والقانون المقارن ، مركز المجموعات الرقمية بجامعة قطر – أبحاث القانون DOI/handle ,١٢٢itemz

http : hdl. Handle .net /١٠٥٧٦/٢١٣٧٢, ٦/٢٠٢١

المستخدمين مع حماية الحق فى الخصوصية باعتباره حقاً مرتبطاً بشكل أساسي بالبيانات الشخصية الرقمية، وهذا ما نسعى للإجابة عليه من خلال هذا البحث.

ولقد ذكر فى الصحف الإلكترونية أن القانون المصرى جاء محاكياً للقوانين العالمية وعلى رأسها اللائحة الأوربية " General Data Protection Regulation"

مع أضافة تعديلات ومعايير تساهم فى تعزيز حماية البيانات الشخصية وبالاطلاع على مجموعة من المعايير الدولية لإنشاء قانون حماية البيانات الرقمية، وكذلك البيانات التى أشارت إليها مؤسسة أكسس ناو والتى اعتبرتها مقياساً للدول السابقة من القوانين المعنية بحماية البيانات الشخصية، ويمكن من خلال ذلك قياس مدى فاعلية القانون المصرى فى حماية بيانات المستخدمين مع حماية الحق فى الخصوصية باعتباره حقاً مرتبطاً بشكل أساسي بالبيانات الشخصية.

وتحدد تشريعات حماية البيانات الشخصية الأسس القانونية لحماية حقوق الأفراد فيما يتعلق بمعالجة جميع الجهات في داخل الدولة وخارجها للبيانات الشخصية، وكذلك الجهات خارج الدولة التي تتعامل مع البيانات الشخصية للأفراد المقيمين داخل الدولة بأي شكل من الأشكال بما فى ذلك معالجة البيانات الشخصية عبر شبكة الإنترنت، وتحدد التشريعات أيضاً حقوق أصحاب البيانات وأهداف مراقب البيانات والمبادئ الأساسية لحماية البيانات، وكذلك الأدوار والمسؤوليات.

أولا :المبادئ الأساسية لحماية البيانات(٤) :

المبدأ الأول: المسؤولية: أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بجهة التحكم واعتمادها من قبل المسؤول الأول بالجهة (أو من يفوضه)، ونشرها إلى جميع الأطراف المعنية بتطبيقها.

(٤) آلاء كليب ، قانون حماية البيانات الشخصية فى ضوء المعايير الدولية ، ١٤ يوليو ٢٠٢١ ، مؤسسة حرية الفكر والتعبير (afte)

المبدأ الثاني: الشفافية: أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بجهة التحكم يحدد فيه الأغراض التي من أجلها تم معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة.

المبدأ الثالث: الاختيار والموافقة: أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته (الضمنية والصريحة) فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.

المبدأ الرابع: الحد من جمع البيانات: بأن يجمع الحد الأدنى منها الذي يفي بالغرض المحدد.

المبدأ الخامس: الحد من استخدام البيانات والاحتفاظ بها والتخلص منها: أن يتم تقييد معالجة البيانات الشخصية بالأغراض المحددة فى إشعار الخصوصية والتى من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة والاحتفاظ بها طالما كان ذلك ضرورة لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها فى الدولة، وإتلافها، بطريقة أمنة تمنع التسريب أو الفقدان أو الاختلاس أو إساءة الاستخدام أو الوصول غير المصرح به قانوناً.

المبدأ السادس: الوصول إلى البيانات بوسيلة تمكن من مراجعتها وتحديثها وتصحيحها.

المبدأ السابع: الحد من الإفصاح عن البيانات للأطراف الخارجية بالأغراض المحددة فى إشعار الخصوصية والتى من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة.

المبدأ الثامن: أمن البيانات: أن يتم حماية البيانات الشخصية من التسرب أو التلف أو الفقدان أو الاختلاس أو إساءة الاستخدام أو التعديل أو الوصول غير المصرح به وفقاً لما يصدر من الهيئة الوطنية للأمن السيبرانى والجهات ذات الاختصاص.

المبدأ التاسع: جوده البيانات: أن يتم الاحتفاظ بالبيانات الشخصية بصورة دقيقة وكاملة وذات علاقة مباشرة بالأغراض المحددة فى إشعار الخصوصية.

المبدأ العاشر: الحفاظ على سرية البيانات وأمن المعلومات الإلكترونية.

خطة البحث: –

مبحث أول: أساس الحماية ودوافعها وطبيعتها ونطاقها.

مطلب أول: – الاساس القانوني للحماية.

مطلب ثاني: – الدوافع والطبيعة والنطاق.

مبحث ثاني: – ماهية البيانات الشخصية وحقوق والتزامات المعنين بها.

مطلب أول: – ماهية البيانات الشخصية وعلاجها.

مطلب ثان: – حقوق والتزامات المعنيين بها.

مبحث ثالث: – صور الحماية القانونية.

مطلب أول: – الحماية الإدارية والجنائية.

مطلب ثاني: – الحماية المدنية.

المبحث الأول

الاساس القانوني للحماية (الدولية والدستورية والقانونية) وطبيعتها

المطلب الاول

الاساس القانوني للحماية

أولاً الحماية الدولية: –

حماية البيانات الشخصية الرقمية وفقاً للقانون المصرى: كيفية تحقيق الحماية للبيانات الشخصية الرقمية وفقاً للقانون المصرى:

يتضمن قانون حماية البيانات الشخصية المصرى معظم المعايير الدولية الأساسية فى مجال حماية البيانات ومنها على سبيل المثال : حقوق أصحاب البيانات والأساس القانوني لمعالجة البيانات (الخاضعة وغير الخاضعة للموافقة) ، ومتطلبات سياسات الخصوصية ، وواجب الإبلاغ فى حال انتهاك خصوصية البيانات ، وضرورة تقيم الأثر قبل معالجتها والقواعد المحددة بشأن البيانات الصحيحة وبيانات الائتمان ، والتزامات جهات التحكم وإجراءات العناية الواجبة ، وإنشاء جهة مشرفة والعقوبات فى حالات الانتهاكات وتتوافق العديد من خصائص القانون مع المعايير والمبادئ الواردة فى تشريعات حماية البيانات الدولية الأخرى ، مثل " اللائحة العامة الأوربية لحماية البيانات (٦٧٩ / ٢٠١٦ GDPR) [٥] أي اللائحة التى ينص عليها قانون الاتحاد الأوروبي حول حماية البيانات والخصوصية فى الاتحاد الأوروبي والمنظمة الاقتصادية الأوربية حيث إنها تعتبر معياراً دولياً فى توفير اكبر وأوسع حماية للبيانات الشخصية ولها تأثير مهم على القوانين واللوائح خارج الاتحاد الأوروبي ، إذ أن التشريعات الناشئة يستند الى اللائحة الأوربية كـ " نقطة انطلاق " للقوانين التى تنص عليها " .

وإن كان القصد من القانون أن يكون متماشياً مع روح اللائحة الأوربية الا انه اختلف عنها خصوصاً ما تضمنته المادة ٢٠ منه والخاصة بتشكيلها مركز حماية البيانات المصرى حيث جاء التشكيل غير محقق لشرط الحياد والاستقلال الذى أكدته قواعد الاتحاد الأوروبي ، لأنها نصت على أن " يترأس الجهاز رئيس الوزراء ويتكون من أعضاء ممثلين عن وزارات الحكومة بعكس الأجهزة المماثلة فى الدول الأوروبية والتى جاء تشكيلها من خبراء مستقلين ، وأعضاء

---

(٥) نورا فخرى ضوابط حماية البيانات الشخصية للتسوق الإلكتروني ، نوفى عليها ، مقالة باليوم السابع

Shbrtur١.at/hp٣b٦.

برلمانيين وقضاة مثل مركز حماية المعلومات والحريات الفرنسي وذلك توافقاً مع قواعد حماية البيانات الأوروبية .

كما ينبغي أن يتماشى القانون مع المعايير الدولية التى تتمثل فى الاتي: –

١– ضمان إجراء مفاوضات شفافة وشاملة لجميع الأطراف المعنية (غير موجود).

٢– تعريف قائمة مبادئ لحماية البيانات تكون ملزمة وتضمينها فى الإطار القانوني.

٣– تحديد الاساس القانوني الذي يسمح بمعالجة البيانات.

٤– إدراج قائمة بحقوق المستخدمين الملزمة فى القانون.

٥– تحديد نطاق واضح للتطبيق.

٦– إنشاء آليات ملزمة شفافة لنقل البيانات بشكل آمن الى بلدان ثالثة.

٧– حماية آمن ونزاهة البيانات.

٨– تطوير آليات منع انتهاك البيانات والإبلاغ عنها.

٩– إنشاء سلطة مستقلة وآليات قوية لإنفاذ القانون (غير موجود).

١٠– مواصلة حماية البيانات والخصوصية (الاستمرارية).

يلتصق الحق فى حماية البيانات الشخصية بالحق فى الخصوصية الرقمية وهو " التسليم بحق الأفراد فى التمتع بفسحة للتنمية الذاتية تقوم على مبدأي التفاعل والحرية أو حقهم فى مجال خاص يتسع لهم فيه التفاعل أو عدم التفاعل مع الآخرين ، دون الخضوع لتدخل الدولة أو تدخل زائد بممارسة أفراد آخرين بلا دعوة " وذلك وفقاً للتقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان عن الحق فى الخصوصية فى العصر الرقمي [٦] ، ويشمل التقرير أيضاً الحياة الإلكترونية للأفراد ، مساحة البيانات الشخصية التى تقع تحت بند الخصوصية ، واكد على ذلك

(٦)التقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان عن الحق فى الخصوصية فى العصر الرقمي https://undocs.org/ar/A/HRC/٣٩/٢٩.

الإعلان العالمي لحقوق الإنسان فى المادة (١٢)[٧]، وكذلك العهد الدولي الخاص بالحقوق المدنية والسياسية فى المادة(٧)[٨] .

الحماية الدستورية القانونية والتنفيذية:

الأساس القانوني لحماية البيانات الشخصية الرقمية للشخص سواء أكان طبيعياً أو اعتبارياً عاماً أو خاصاً – فى رأينا – هى صورة أو تطبيق من حرمة الحياة الخاصة (م ٥٧ من الدستور المصرى) من ناحية والحق فى الخصوصية (م ٥٤، ٩٢ من الدستور المصرى) من ناحية أخرى ، كما أنها تطبيق من تطبيقات الحق فى سرية المعلومات المتعلقة بالشخص (م ٦٨ من الدستور المصرى) من ناحية ثالثة ، وهذه الحقوق هى حقوق عامة و دستورية (المواد ٣١ ، ٥١ ، ٥٣ ، ٥٤ ، ٥٧ ، ٥٩ ، ٦٠ ، ٦٧ ، ٩٢ ، ٩٨ : ١٠٠ (من الدستور المصرى الحالي) ، وهى كذلك من حقوق الإنسان التى نصت عليها الإعلانات والمواثيق الدولية والتى تلتزم بها مصر بمجرد التصديق عليها وتصبح لها قوة القانون بعد نشرها وفقاً للأوضاع المقررة (م ٩٣ من الدستور المصرى)[٩].

---

(٧)

https://www.un.org/ar/udhrhoos/H٢٩

(٨)

https://www.nhrc-ga.org/WP-content/uploads/٢٠١٤/١

(٩) البيانات الشخصية محمية بموجب الحق فى الخصوصية فى الصكوك الدولية لحقوق الإنسان ، وعلى سبيل المثال

المادة (٨ / ١) من الاتفاقية الأوروبية لحقوق الإنسان لعام ١٩٥٠ " لكل فرد الحق فى احترام حياته الخاصة والعائلية ومسكنه ومراسلاته، لا يجوز التدخل الا بقانون وكإجراء ضروري لحماية المصالح الاجتماعية العليا فى الدولة ".

والمادة (١١) من الاتفاقية الأمريكية لحقوق الإنسان لعام ١٩٦٩، والمادة (٨) من الاتفاقية الأفريقية تغطى اتفاقية الاتحاد بشأن الأمن الإلكتروني وحماية البيانات الشخصية لعام ٢٠١٤ " الحق فى احترام البيانات الشخصية"، والمادة (٨ / ١) من ميثاق الحقوق الأساسية للاتحاد الأوروبي لعام ٢٠٠٠، والمادة ١٦ / ١ من معاهدة عمل الاتحاد الأوروبي لعام ١٩٥٧ (المعروفة أيضا بمعاهدة روما) تنظر فى حماية البيانات للأشخاص كحق من حقوق الإنسان.

وتنص المادة ٣١ من الدستور المصرى الحالي لعام ٢٠١٤ على أن " أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون."

كما تشير المادة ٥١ من ذات الدستور على أن "الكرامة حق لكل إنسان، ولا يجوز المساس بها، وتلتزم الدولة باحترامها وحمايتها. " .

وتضيف المادة ٥٣ من نفس الدستور أن " المواطنون لدى القانون سواء، وهم متساوون في الحقوق والحريات والواجبات العامة، لا تمييز بينهم بسبب الدين، أو العقيدة، أو الجنس، أو الأصل، أو العرق، أو اللون، أو اللغة، أو الإعاقة، أو المستوى الاجتماعي، أو الانتماء السياسي أو الجغرافي، أو لأي سبب آخر."

وتؤكد المادة ٥٤ من ذات الدستور على أن "الحرية الشخصية حق طبيعي، وهي مصونة لا تُمس، وفيما عدا حالة التلبس، لا يجوز القبض على أحد، أو تفتيشه، أو حبسه، أو تقييد حريته بأي قيد إلا بأمر قضائي مسبب يستلزمه التحقيق....."

وتؤكد المادة ٥٧ من نفس الدستور على أن " الحياة الخاصة حرمة، وهي مصونة لا تمس. والمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين

وتنص المادة الثالثة من الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨ على أن " لكل فرد الحق فى الحياة وسلامة شخصه " وتضيف المادة الثامنة منه على أن " لكل شخص الحق فى أن يلجأ إلى المحاكم الوطنية وإنصافه عن أعمال فيها اعتداء على الحقوق الأساسية التى منحها له القانون "، وتضيف المادة الثانية عشر منه على انه " لا يعرض أحد لتدخل تعسفي فى حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته ، ولكل شخص الحق فى حماية القانون من مثل هذا التدخل او تلك الحملات " ، ودائماً وفقاً للمادة السادسة منه أن " لكل أنسان أينما وجد الحق فى أن يعترف بشخصيته القانونية " وتنص المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية عام ١٩٦٦ ، ١٩٧٦ على انه " ١- لا يجوز تعريض أي شخص ، على نحو تعسفي أو غير قانونى لتدخل فى خصوصياته أو شئون أسرته أو بيته أو مراسلاته ، ولا لأى جهات غير قانونية تمس شرفه او سمعته . ٢- من حق كل شخص أن يحميه القانون من مثل هذا التدخل او المساس ".

في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك."

وتضمن المادة ٥٩ من الدستور بأن " الحياة الآمنة حق لكل إنسان، وتلتزم الدولة بتوفير الأمن والطمأنينة لمواطنيها، ولكل مقيم على أراضيها."

وتؤكد المادة ٦٠ من ذات الدستور على أن " لجسد الإنسان حرمة، والاعتداء عليه، أو تشويهه، أو التمثيل به، جريمة يعاقب عليها القانون. ويحظر الاتجار بأعضائه.....". وتشير المادة ٦٧ من ذات الدستور إلى أن " المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها، وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمداً.

وتلتزم مؤسسات الدولة بإيداع الوثائق الرسمية بعد الانتهاء من فترة العمل بها بدار الوثائق القومية، وحمايتها وتأمينها من الضياع أو التلف، وترميمها ورقمنتها، بجميع الوسائل والأدوات الحديثة، وفقاً للقانون."

كما أن الحقوق والحريات اللصيقة بشخص المواطن لا تقبل تعطيلاً ولا انتقاصاً. ولا يجوز لأي قانون ينظم ممارسة الحقوق والحريات أن يقيدها بما يمس أصلها وجوهرها (م ٩٢ من الدستور)

كما أشارت كل من المادتين ٩٧، ٩٨ من الدستور على ان " التقاضي حق مصون ومكفول للكافة....." وأن حق الدفاع أصالة أو بالوكالة مكفول. ..." .

وأضافت المادة ٩٩ منه على أن " كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط

الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر. "(١٠).

علاوة على أن المادة ١٠٠من ذات الدستور تشير إلى أن " تصدر الأحكام وتنفذ باسم الشعب، وتكفل الدولة وسائل تنفيذها على النحو الذي ينظمه القانون. ويكون الامتناع عن تنفيذها أو تعطيل تنفيذها من جانب الموظفين العموميين المختصين، جريمة يعاقب عليها القانون، وللمحكوم له في هذه الحالة حق رفع الدعوى الجنائية مباشرة إلى المحكمة المختصة. وعلى النيابة العامة بناءً على طلب المحكوم له، تحريك الدعوى الجنائية ضد الموظف الممتنع عن تنفيذ الحكم أو المتسبب في تعطيله."

المطلب الثانى

دوافع صدور القانون رقم ١٥١ لسنة ٢٠٢٠ وطبيعته

أولا: دوافع وأسباب صدور هذا القانون:

ترجع الدوافع والأسباب التى أدت إلى صدور قانون حماية البيانات الشخصية الى

١- المعالجة الكترونياً(١١): استنادا للحماية الدستورية للبيانات الشخصية باعتبارها تمس الكرامة الإنسانية وحرمة الحياة الخاصة والحق فى الخصوصية (م ٣١ ، ٥١ ، ٥٤ ، ٥٧ ، ٥٩ ، ٦٧ ، ٩٩ ، ١٠٠) .

٢- ثورة المعلوماتية وتكنولوجيا الاتصالات وازدياد الاعتماد عليها على المستوى الفردي والجماعي أو مستوى الدولة والحكومة مما أدى الى زيادة مخاطر استخدامها بأنماطها المختلفة على الحياة الخاصة للشخص الطبيعي (أو حتى فى رأينا الاعتباري الخاص

(١٠) وتنص الفقرة الثانية من ذات المادة على أنه " وتكفل الدولة تعويضاً عادلاً لمن وقع عليه الاعتداء، وللمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضماً إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون."

(١١) المعالجة إلكترونياً : هى كل عملية أو مجموعة عمليات أياً كانت الطريقة المستعملة ، وعلى وجه الخصوص الجمع ، التسجيل ، التنظيم ، الحفظ ، الاقتباس أو تعديل الأصل ، الكشف أو الاستعمال الاتصال من خلال نقل ، نشر أو أي شكل آخر من الوضع للتداول ، التعريف ، الربط ، وكذا الحجب ، المحو أو الإتلاف .

أو العام) لما يمثل اعتداءً على الحق فى الخصوصية حيث تمثلت فى معظم الأحوال فى انتهاك الحق فى سرية البيانات الخاصة ، على الرغم من اثر التكنولوجي يكون لتقرير حماية حقوق الإنسان وليس العكس(١٢).

٣- كثرة استخدام المصريين بنسبة تكاد تكون أكثر من نصف الشعب المصرى لوسائل التقدم التكنولوجي منها الإنترنت وغيره فى حياته العامة بل والخاصة أيضاً.

٤- قفز حجم التجارة الإلكترونية فى مصر بدءاً من عام ٢٠٢٠ وحتى الأن إلى نحو مليارات من الدولارات مما يؤكد نمو هذا السوق بشكل مطرد ويتطلب ضرورة حماية رواد هذه السوق حفاظاً على الثقة فى التعامل الإلكتروني وضمان استمرارية ازدهاره.

٥- اجتياح فيروس كورونا لدول العالم منها مصر أدى إلى زيادة استخدام الوسائل التكنولوجية بشكل اكبر ، ولما كانت حماية البيانات الشخصية يعد مكوناً رئيسياً فى ازدهار التجارة الإلكترونية خصوصاً فى ظل الأزمات والأوبئة العالمية مثل الكورونا ، فإن الحاجة أصبحت ماسة فى مصر لتدخل تشريعي يحمى البيانات الشخصية للشخص الطبيعي بالدرجة الأكبر ويفرضها مما يؤدى إلى تعزيز ثقة الأفراد فى التعامل عبر وسائل التقدم التكنولوجي مثل الإنترنت أو غيره ، مما يشكل عاملاً رئيسياً لازدهار التجارة الإلكترونية(١٣).

ثانياً: – النطاق الشخصي والموضوعي للقانون فى مواد الإصدار:

(١٢) التقرير السنوي بمفوضية الأمم المتحدة السامية ، اثر التكنولوجيا الجديدة فى تقرير حقوق الإنسان وحمايتها

https://undocs.arg/ar/A/HRC/٤٤/٢٤.

(١٣) لقد حددت المادة الاولى من قانون حماية البيانات الشخصية تعريفاً لاصطلاح التسويق الإلكتروني بانه" إرسال أي رسالة أو بيان أو محتوي إعلاني أو تسويقي بأي وسيلة تقنية أيًا كانت طبيعتها أو صورتها تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو التماسات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة إلى أشخاص بعينهم. "

١- الموضوع: هو حماية البيانات الشخصية المعالجة إلكترونيًا عن طريق وسائل الأنظمة الإلكترونية، جزئيًا أو كليًا – داخل الدولة أو خارجها – (م ١).

٢- الأشخاص: الحائز أو المتحكم أو المعالج أو المسئول هو الملتزم والمستفيد هو الشخص الطبيعي وليس الاعتباري.

٣- المخالف أو المجرم قد يكون مصرياً أو مقيماً داخلياً أو خارجياً، والمجني عليه هو المصرى أو الأجنبي المقيم فى مصر (م ٢)

٤- حالات عدم سريانه محدده فى المادة (٣ من مواد الإصدار):

لا تسري أحكام القانون المرافق على ما يأتي:

١ – البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير، ويتم معالجتها للاستخدام الشخصي.

٢ – البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقًا لنص قانوني.

٣ – البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تستخدم في أي أغراض أخري، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام.

٤ – البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوي القضائية.

٥ – البيانات الشخصية لدي جهات الأمن القومي، وما تقدره لاعتبارات أخري. ويجب على المركز، بناءً على طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، خلال مدة زمنية محددة، وفقًا لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به.

٦ – البيانات الشخصية لدي البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل الأموال وشركات الصرافة، على أن يراعي في شأنهما القواعد المقررة من البنك المركزي المصري بشأن التعامل مع البيانات الشخصية.

ويتكون القانون رقم ١٥١ لسنة ٢٠٢٠ من ٤٩ مادة – يسبقه قانون إصدار من سبع مواد – تتوزع على أربعة عشر فصلًا، يختص الفصل الأول بالتعريفات التي يؤسس عليها القانون (م ١) ، والفصل الثانى عن حقوق الشخص المعني بالبيانات وشروط جمع ومعالجة البيانات (م ٢: ٣) ، والثالث يتعلق بالتزامات المتحكم والمعالج(م ٤ : ٧) ، والرابع يحدد مسئول حماية البيانات الشخصية (م ٨ : ٩) ، والخامس عن إجراءات إتاحة البيانات الشخصية (م ١٠ : ١١)،والسادس عن البيانات الشخصية الحساسة (م ١٢ : ١٣) ، والسابع يتعلق بالبيانات الشخصية عبر الحدود (م ١٤ : ١٦) ، والثامن فى التسويق الإلكتروني المباشر(م ١٧ : ١٨) .والتاسع فى ماذا ؟ عن مركز حماية البيانات الشخصية (م ١٩: ٢٥)، والعاشر فى التراخيص والتصاريح والاعتمادات (م ٢٦ :٣٠)، الفصل الحادي عشر فى موازنه المركز وموارده المالية (م ٣١)، والفصل الثانى عشر فى الطلبات والشكاوى (م ٣٢: ٣٣)، والفصل الثالث عشر الضبطية القضائية (م ٣٤)، والفصل الرابع عشر فى الجرائم والعقوبات (م ٣٥: ٤٩) والصلح والتصالح فيها.

وعلى ذلك يؤسس القانون المصرى الاطار الذى يحدد العلاقة بين المعنى بالبيانات من جهة ومستخدمي البيانات من جهة أخرى كالحائز والمتحكم والمعالج والمسئول وذلك من خلال تفنيد حقوق المعنى بالبيانات وشروط جمع البيانات ومعالجة البيانات ، والتزامات المتحكم والمعالج وإجراءات إتاحة البيانات الشخصية وطبيعة استخدام البيانات الشخصية الحساسة ،وكذلك البيانات الشخصية عبر الحدود ،واستخدام البيانات الشخصية فى التسويق الإلكتروني المباشر، ويؤسس القانون كذلك بداية من الفصل التاسع وصولاً للأخير لإنشاء مركز حماية البيانات الشخصية الذي تتحدد مهامه في الرقابة على إنفاذ القانون وإصدار التراخيص والتصاريح والاعتمادات لمزاولة الشركات، وجمع ومعالجة بيانات المستخدمين، كما يمنح القانون حق الضبطية القضائية لأفراد معينة من المركز، ويحدد كذلك الجرائم والعقوبات والصلح والتصالح فيها وذلك فى الفصل الأخير.

لقد وضع القانون إطار متكاملاً لضمان حماية خصوصية الشخص الطبيعي وسرية المعلومات عبر توفير الحوكمة السليمة لإدارة البيانات وحمايتها فهو يحدد الأطر العامة للتعامل مع البيانات الشخصية للأفراد وكيفية جمعها ومعالجتها وتخزينها ووسائل ضمان حمايتها، وحقوق وواجبات كافة الأطراف المعنية. لذا فهو يسرى على معالجة البيانات الشخصية الكترونياً للشخص الطبيعي – دون الشخص الاعتباري – سواء كلها أو جز منها عن طريق وسائل الأنظمة الإلكترونية سواء داخل او خارج الجمهورية، كما حظر القانون معالجة البيانات الشخصية دون موافقة أصحابها وذلك باستثناء بعض الحالات التى يكون من ضمنها المعالجة ضرورية لحماية

المصلحة العامة (للأجهزة الأمنية والرقابية) أو لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القضائية.

كما حدد القانون ضوابط معالجة البيانات الشخصية والالتزامات العامة للشركات التى تتوافر لديها البيانات الشخصية وعن الأفراد وتلك العاملة فى مجال معالجة البيانات الشخصية.

رابعاً: – مكونات القانون رقم ١٥١ لسنة ٢٠٢٠

والخلاصة: يتكون هذا القانون من تسع وأربعين مادة موزعة على أربعة عشر فصلًا، علاوة على التصدير الذي يتكون من سبع مواد كالتالي:

الفصل الأول بعنوان التعريفات التي يتأسس عليها القانون، مثل البيانات الشخصية، ومن خلال بقية الفصول يؤسس القانون الإطار الذي يحدد العلاقة بين المعنى بالبيانات من جهة ومستخدمي البيانات من جهة أخرى، كالحائز والمتحكم والمعالج والمسئول، وذلك من خلال تفنيد حقوق المعني بالبيانات وشروط جمع ومعالجة البيانات، والتزامات المتحكم والمعالج، وإجراءات إتاحة البيانات الشخصية، وطبيعة استخدامها، وتلك الماسة والعابرة للحدود، وكذلك استخدامها في التسويق الإلكتروني المباشر.

كما يؤسس القانون بدايةً من الفصل التاسع ووصولًا الى الأخير لإنشاء مركز حماية البيانات الشخصية الذي تتحدد مهامه في الرقابة على إنفاذ القانون، وإصدار التراخيص والتصاريح والاعتمادات لمزاولة الأشخاص الطبيعية والشركات، وجمع ومعالجة بيانات المستخدمين، كما يخصص القانون حق الضبطية القضائية لأفراد معينة من المركز، ويحدد كذلك الجرائم والعقوبات في الفصل الأخير منه.

- نظرة عامة على القانون ثم الإطار المفاهيمي للقانون باستخدامه جملة مصطلحات أساسية، ثم حقوق الشخص المعنى البيانات وشروط المعالجة، والتزامات أطراف معالجة وجمع البيانات (المتحكم والمعالج) وأخيراً وسائل إنفاذ القانون:
- أ– حددت المادة الاولى من القانون مفاهيم المصطلحات الأتية:

١– الشخص المعنى بالبيانات: هو أي شخص طبيعي تنسب إليه بيانات شخصية معالجة إلكترونيا تدل عليه قانونا أو فعلا، وتمكن من تمييزه عن غيره.

٢- الحائز: أي شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيا أو فعليا ببيانات شخصية فى أي صورة من الصور، أو على أي وسيلة تخزين سواء أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة.

٣- المتحكم: أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق فى الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقا للغرض المحدد أو نشاطه.

٤- المعالج: أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته.

فهو الذي يحدد طرق وأسلوب ومعايير المعالجة.

٥- المسئول عن حماية البيانات الشخصية: لدى الكيانات التى يعمل لديها فهو المسئول عن حسن تنفيذ هذه الكيانات أحكام القانون داخلها وحدد القانون طرق تعينه وواجباته بالتفصيل.

المبحث الثانى

ماهية البيانات الشخصية وحقوق والتزامات المعنين بها

المطلب الاول

ماهية البيانات الشخصية وعلاجها.

على الرغم من أن المشرع لم يعرف كلمة الحماية لأنها مهمة الفقه والقضاء ولم يبين كذلك صورها إلا إنه وفقاً للفصل الاول من القانون رقم ١٥١ لسنة ٢٠٢٠ فإن البيانات الشخصية هى بيانات متعلقة بشخص طبيعي – وليس اعتباري – محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري 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 (م ١).

أي من خلال الإشارة إلى واحد أو أكثر من الخصائص المادية أو الفسيولوجية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي.

أما البيانات الشخصية الحساسة: فهي البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية، وكذلك تعد بيانات الأطفال من البيانات الشخصية الحساسة (م ١).

اما المعالجة : فهي " أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليلها باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيا أو كليًا "(م ١) أو هى كل عملية يتم إجراؤها على البيانات الشخصية جزئياً أو كلياً بشكل أوتوماتيكي أو بشكل يدوى وإدخالها على أنظمه التسجيل والأرشفة وتسجيلها وتخزينها وحفظها وأرشفتها وتغيرها او تعديلها أو تجديد تنظيمها وتوضيحها أو نقلها أو استلامها أو جعلها قابلة للاطلاع عليها أو تصنيفها أو منع استعمالها فكل تلك العمليات والإجراءات تدخل فى مفهوم معالجة البيانات الشخصية .

وصور جرائم انتهاك البيانات الشخصية للأفراد هى: ١- استخدام بيانات شخصية غير صحيحة.

٢- جمع وتخزين بيانات شخصية صحيحة ولكن على نحو غير مشروع جنائياً. ٣- الإفشاء غير المشروع لبيانات الشخصية وإساءة استخدامها. ٤- مخالفة القواعد الشكلية المنظمة لجمع

ومعالجة ونشر البيانات ذات الطبيعة الشخصية التى تدخل فى نطاق الحماية التشريعية لخصوصية المعلومات.

ويهدف القانون أذن إلى وضع إطار تشريعي يكفل للمستخدم حماية بياناته التى خضعت للمعالجة الإلكترونية، فله الحق فى معرفة طبيعة البيانات التى لدى الحائز أو المعالج، وله الحق فى مقاضاتهما أذا استدعى الأمر ذلك.

- طبيعة الحماية أنها تتعلق بالحق فى الخصوصية [١٤] (م ٥٤ من الدستور المصرى) أو الحق فى حرمة الحياة الخاصة (م ٥٧ من الدستور المصرى) وهى من اكثر الحقوق ارتباطا بالشخصية القانونية للإنسان وأكثرها تعلقاً بالكرامة (م ٥١ من الدستور المصرى) وهو مؤشر على تحضر الأمم ورقيها ، وذلك لجمعه بين الجوانب المادية والمعنوية لشخصية الإنسان ، وعلاقته الوثيقة وتداخله الشديد بالحقوق والحريات الأخرى ، وتحرص المجتمعات على احترامه ، واعتبرته حقاً قائماً بذاته ، وكذلك لأنه من الحقوق الدستورية المكفولة ، كما أنه يعتبر من وجهة نظرنا حقاً من الحقوق اللصيقة بالشخص من ناحية ، ويتعلق بحق الملكية الفكرية من ناحية أخرى ، ومن ناحية ثالثة يتعلق أمن

---

(١٤) الخصوصية هى قدرة الشخص على منع المعلومات المتعلقة به من أن تصبح معروفة للآخرين ، إن لم يختر طوعاً أن يقدم تلك المعلومات . وهذا المصطلح يشير الى الحياة الخاصة وكذلك أمن وسرية المعلومات.

حماية الخصوصية جزء من المنظومة التشريعية فى دولة الإمارات ودستورها مثل القانون الاتحادي رقم ٤٥ لسنه ٢٠٢١ بشأن حماية البيانات الشخصية، والقانون الاتحادي رقم ٤٤ لسنة ٢٠٢١ بشأن إنشا مكتب الإمارات للبيانات، وكذلك القانون الاتحادي رقم ١٥ لسنة ٢٠٢٠ بشأن حماية المستهلك بما فى ذلك خصوصية وأمن بيانات المستهلك، ويمنع استخدامها لأغراض الترويج والتسويق.

ولقد نص القانون الاتحادي رقم ١٢ لسنة ٢٠١٦ بتعديل المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ فى شأن مكافحة جرائم تقنية المعلومات ، والمعدل على القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات وحظر فى المادة ٢١ من القانون "كل من استخدام شبكة معلوماتية أو نظاماً معلوماتيا الكترونياً ، او احدى وسائل تقنية المعلومات ، فى الاعتداء على خصوصية شخص فى غير الأحوال المصرح بها قانوناً ، بإحدى الطرق التالية (كالتقاط صوراً الغير ، أو إعداد صوراً الكترونية او نقلها أو كشفها أو نسخها أو الاحتفاظ بها ". مثال الشركات التى تتعامل مع البيانات الشخصية والتى تتجسد فى " جوجل ومايكروسوفت وأمازون فودافون، ودوو، واتصالات، فيسبوك وتويتر وماسنجر، وماستر كارد، وأي بي ام، وأوبر، كريم لطلب خدمات النقل الذكي، وأوليكس وساب وغيرها "

البيانات[١٥] والمعلومات أي الأمن السيبرانى ، ومن ناحية رابعة فهو حق إجرائي يتمثل فى الحماية لهذه البيانات الذى ينصب على منقول معنوي واجب حمايته .

(١٥) أمن البيانات هو إجراءات وعمليات تقنية وتنظميه من شأنها الحفاظ على خصوصية البيانات الشخصية وسريتها وسلامتها ووحدتها وتكاملها فيما بينهما بدون اختراق أو انتهاك ، أي بدون دخول غير مرخص به اليها أو وصول غير مشروع لها بهدف الكشف أو الإفصاح عنها أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها .

ويعرف الأمن السيبرانى بانه حماية الأنظمة والشبكات والبرامج والموقع الجغرافي من الهجمات الرقمية، ومن أي مشكلة أو عائق أو هجمات الكترونية تحول دون أداء عملها، وتهدف الهجمات الإلكترونية عادة الى الوصول الى المعلومات الحساسة بهدف تغييرها أو إتلافها أو ابتزاز الأموال من المستخدمين، ويعتبر مفهوم الأمن السيبرانى أوسع من آمن المعلومات حيث يتضمن تأمين البيانات والمعلومات التى تتداول عبر الشبكات الداخلية أو الخارجية والتى يتم تخزينها فى خوادم داخل أو خارج المنظمات من الاختراقات.

ويعتمد العالم على التكنولوجيا اليوم اكثر من أي وقت مضى نتيجة لذلك ينتهج الآمن السيبرانى نهجاً معيناً يتكون عادة من طبقات متعددة الحماية تنتشر فى أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التى ينوى المرء الحفاظ على سلامتها ، وفى أي دولة يجب على المستخدمين والعمليات والتكنولوجيا أن يكملوا بعضهم بعضاً ويتكاتفوا لإنشاء دفاع فعال من الهجمات السبيرانية، الذى يستفيد فيه الأفراد من سرقة هوياتهم او محاولات الابتزاز أو فقدان البيانات المهمة ، وكذلك الدول فى حماية محطات الطاقة والمستشفيات وشركات الخدمات المالية وغيرها .

لذا اتخذت دولة الإمارات العربية المتحدة العديد من الإجراءات والتدابير لتعزيز أمنها السيبرانى يتولى فريق الشبكة الإلكترونية الاتحادية مهمه رصد ومراقبة وقائع ومجريات البنية التحتية للشبكة الإلكترونية الاتحادية على مدار الساعة، بما يضمن اتخاذ الإجراءات اللازمة فى حال حدوث أخطاء او انتهاكات، انظر: فاطمة عبد الله الدربي، مقالة، ما هو الأمن السيبرانى؟ بتاريخ ١٣ / ٢٠٢١/١ على الإنترنت: (https://www.albayan.ae/opinions/by-the-way/٢٠٢١-٠١-١٣-١.٤٠٦٤٥٩٠).

وتتركز أنواع تهديدات الأمن السيبرانى فى تصيد المعلومات وبرامج الفدية الضارة والبرامج الضارة، والتحايل باستخدام الهندسة الاجتماعية، مقالة فى النت Ciscoما هو الأمن السيبرانى فى ١١ / ٣ / ٢٠٢٢.

وحيث الأمن السيبرانى هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية وتهدف عادة الى الوصول الى المعلومات الماسة أو تغييرها أو تدميرها، بغرض الاستيلاء على المال من المستخدمين أو مقاطعه عمليات الأعمال العادية.

المطلب الثانى
حقوق والتزامات المعنيين بها
الفرع الاول
حقوق المعنيين بها

كيفية تحقيق حماية البيانات الشخصية: –

فى تأمين البيانات والحفاظ على سريتها وخصوصيتها، والإجراءات والتدابير المتوفرة لديها لضمان عدم اختراقها أو إتلافها أو تغييرها أو العبث بها، كما وضح القانون إجراءات الإبلاغ عن انتهاك هذه البيانات. ومنح القانون لصاحب البيانات الشخصية عدة حقوق تشمل :

١ – الحصول بمقابل يحدده المركز بما لا يجاوز ٢٠ الف جنية على المعلومات والقرارات التى تتخذ بناء على معالجة البيانات الشخصية باستثناء علمه ومعرفته بأي خرق أو انتهاك(م ٢من القانون).

٢ – الحق فى طلب تصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية الخاطئة أو القديمة (م ٢ / ٢ / ٣من القانون).

٣– حق النسيان الذي يوفر للفرد الحق بأن يطلب من أي شركة يطبق عليها القانون بأن تحذف أو إتلاف بياناته بشكل كلى وحقه فى تخصيص المعالجة فى نطاق محدد (م ٢ / ٢ / ٤ من القانون).

٤– حقة فى العلم بالمعالجة ومبررها القانوني والاطلاع والوصول (الحصول على نسخة مجانية) أو الحصول على البيانات الشخصية (م ٢ / ٢/ ١، ٥ من القانون)، وكذلك حقه فى العلم والمعرفة بأي خرق أو انتهاك لها (م ٢ / ٢ / ٣ من القانون)، حق الإعلام الذي يوفر له أو للمستهلك الحق بأن يتم إعلامه فى حال تم اختراق نظام شركة مطبق عليها القانون، حيث يتم إعلامه بأن بياناته قد انتهكت.

٥–العدول عن الموافقة أو سحبها المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

٦–وحقه فى أي وقت الاعتراض على معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات (م ٢ / ٢ / ٦من القانون).

٧–وفى كل الأحوال لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل الا بموافقة صريحة من الشخص المعنى بالبيانات، أو فى الأحوال المصرح بها قانوناً (م ٢ / ١، ٦، ١٢ من القانون).

وفى كل الأحوال تجب مراعاة الحصول على موافقة الشخص المعنى، وحقه فى رفضه بعد ذلك والعدول عنها بعد ذلك (م ٢/٢/٢ من القانون).

٨- الحق فى تقديم الشكاوى والمقاضاة ضد من يمس أو يعتدى عليها إلى الجهات المسئولة عن ذلك فى الدولة (م ٢ / ٢ / ٥، ٣٢، ٣٣ من القانون).

ولقد حددت المادة الثالثة من القانون شروط جمع البيانات الشخصية ومعالجتها[١٦](شروط المعالجة) والاحتفاظ بها الكترونياً – علاوة على الموافقة من الشخص المعنى او تدوين موافقته فى الأحوال المصرح بها قانوناً بذلك وهى :-

١- جمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني.

٢ – أن تكون صحيحة وسليمة ومؤمنة.

٣ – أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها.

٤ – ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.

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

علماً بأن هذه اللائحة التنفيذية لم تصدر بعد – حسب علمنا – حتى لحظة كتابة هذا البحث.

الفرع الثانى
التزامات المعنيين بها

نص القانون كذلك على التزامات كل من المتحكم والمعالج (م ٤: ٧ من القانون) والمسئول عن حماية البيانات الشخصية (م ٨، ٩ من القانون) كالتالي: -

أولاً: – التزامات المتحكم:

(١٦) المعالجة هى " أي عملية إلكترونية أو تقنية للكتابة ، أو التجميع، أو التسجيل، أو ما إلى ذلك أو استرداد أو تحليل البيانات الشخصية باستخدام أي وسيلة إلكترونية من الوسائط أو تقنية جزئيا أو كليًا."

فقد نصت المادة (٤ من القانون على انه)" مع مراعاة أحكام المادة (١٢) من هذا القانون، يلتزم المتحكم بما يأتي:

١ – الحصول على البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا.

٢ – التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها.

٣ – وضع طريقة وأسلوب ومعايير المعالجة طبقا للغرض المحدد، ما لم يقرر تفويض المعالج في ذلك بموجب تعاقد مكتوب.

٤ – التأكد من انطباق الغرض المحدد من جمع البيانات الشخصية لأغراض معالجتها.

٥ – القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية إلا في الأحوال المصرح بها قانونًا.

٦ – اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظًا على سريتها، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قِبَل أي إجراء غير مشروع.

٧ – محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض، فيجب ألا تبقي في صورة تسمح بتحديد الشخص المعني بالبيانات.

٨ – تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به.

٩ – إمساك سجل خاص للبيانات، على أن يتضمن وصف فئات البيانات الشخصية لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها وأي بيانات أخري متعلقة بنقل تلك البيانات الشخصية عبر الحدود ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات.

١٠ – الحصول على ترخيص أو تصريح من المركز للتعامل مع البيانات الشخصية.

١١ – يلتزم المتحكم خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية.

١٢ – توفير الإمكانيات اللازمة لإثبات التزامه بتطبيق أحكام هذا القانون وتمكين المركز من التفتيش والرقابة للتأكد من ذلك.

وفي حال وجود أكثر من متحكم يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وللشخص المعني ممارسة حقوقه تجاه كل متحكم على حدة مسئولية فردية.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير الفنية لتلك الالتزامات.

ثانياً: – التزامات المعالج:

أ- المفهوم:

ونصت المادة (٥) على: التزامات المعالج انه " مع مراعاة أحكام المادة (١٢) من هذا القانون، **يلتزم معالج البيانات الشخصية بما يأتي:**

١ – إجراء المعالجة وتنفيذها طبقًا للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقًا للحالات المشروعة والقانونية وبناءً على التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أي ذي صفة بحسب الأحوال، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها ونوع البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد له.

٢ – أن تكون أغراض المعالجة وممارستها مشروعة، ولا تخالف النظام العام أو الآداب العامة.

٣ – عدم تجاوز الغرض المحدد للمعالجة ومدتها، ويجب إخطار المتحكم أو الشخص المعني بالبيانات أو كل ذي صفة، بحسب الأحوال، بالمدة اللازمة للمعالجة.

٤ – محو البيانات الشخصية بانقضاء مدة المعالجة أو تسليمها للمتحكم.

٥ – القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانونًا.

٦ – عدم إجراء أي معالجة للبيانات الشخصية تتعارض مع غرض المتحكم فيها أو نشاطه إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة.

٧ – حماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك وما عليها من بيانات شخصية.

٨ – عدم إلحاق أي ضرر بالشخص المعني بالبيانات بشكل مباشر أو غير مباشر.

٩ – إعداد سجل خاص بعمليات المعالجة لديه، على أن يتضمن فئات المعالجة التي يجريها نيابة عن أي متحكم وبيانات الاتصال به ومسئول حماية البيانات لديه، والمدد الزمنية للمعالجة

وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها، ووصفًا للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة.

١٠ – توفير الإمكانيات لإثبات التزامه بتطبيق أحكام هذا القانون عند طلب المتحكم وتمكين المركز من التفتيش والرقابة للتأكد من التزامه بذلك.

١١ – الحصول على ترخيص أو تصريح من المركز للتعامل على البيانات الشخصية.

١٢ – يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية.

وفي حال وجود أكثر من معالج، يلتزم كل منهم بجميع الالتزامات المنصوص عليها مسئولية فردية في هذا القانون وذلك في حال عدم وجود عقد يحدد التزامات ومسئوليات كل منهم بوضوح.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والشروط والتعليمات والمعايير القياسية لتلك الالتزامات.

- ب– شروط المعالجة:

لم يحدد المشرع تعريفاً للمعالجة، لكن حدد من هو المعالج، والمعالجة هى إجراء عملية أو أكثر على البيانات الشخصية كالجمع والاستلام والتسجيل والتخزين والتهيئة والتعديل والاسترجاع والاستخدام والإنشاء والنشر والنقل والحجب والتخلص والمحو والإلغاء "

فنصت المادة (٦) على أن:" تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات الآتية:

١ – موافقة الشخص المعني بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر[١٧].

(١٧) تضمنت اللائحة الأوروبية عدم استحواذ الشركات على بيانات المستخدمين بدون موافقة مسبقة من الشخص المعنى بالبيانات مع حقه فى مراجعتها وتعديلها أو إلغاء التعاقد معها ، التقرير السنوي بمفوضية الأمم المتحدة السامية ، ٢٠ ، اثر التكنولوجيا الجديدة فى تقرير حقوق الإنسان وحمايتها ،

https://gdpr-inbo.eu/art-٤-gdpr.Debinitions

٢ – أن تكون المعالجة لازمة وضرورية تنفيذًا لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها.

٣ – تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً على حكم قضائي.

٤ – تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.

ج– التزام مشترك: الالتزام بالإخطار والإبلاغ عن الحقوق والانتهاك:

نصت المادة (٧) على أن:" يلتزم كل من المتحكم والمعالج بحسب الأحوال حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ المركز خلال اثنتين وسبعين ساعة، وفي حال كان هذا الخرق أو الانتهاك متعلقًا باعتبارات حماية الأمن القومي فيكون الإبلاغ فوريا، وعلى المركز وفي جميع الأحوال إخطار جهات الأمن القومي بالواقعة فورًا، كما يلتزم بموافاة المركز خلال اثنتين وسبعين ساعة من تاريخ علمه بما يأتي:

١ – وصف طبيعة الخرق أو الانتهاك، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها.

٢ – بيانات مسئول حماية البيانات الشخصية لديه.

٣ – الآثار المحتملة لحادث الخرق أو الانتهاك.

٤ – وصف الإجراءات المتخذة والمقترح تنفيذها لمواجهة هذا الخرق أو الانتهاك والتقليل من آثاره السلبية.

٥ – توثيق أي خرق أو انتهاك للبيانات الشخصية، والإجراءات التصحيحية المتخذة لمواجهته.

٦ – أي وثائق أو معلومات أو بيانات يطلبها المركز.

وفي جميع الأحوال يجب على المتحكم والمعالج، بحسب الأحوال، إخطار الشخص المعني بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ وما تم اتخاذه من إجراءات.

وتحدد اللائحة التنفيذية لهذا القانون الإجراءات الخاصة بالإبلاغ والإخطار.

ثالثاً: – مسئول حماية البيانات الشخصية

أ: تعيين مسئول حماية البيانات الشخصية:

فنصت المادة (٨ من القانون على أن):" ينشأ بالمركز سجل لقيد مسئولي حماية البيانات الشخصية، وتحدد اللائحة التنفيذية لهذا القانون شروط القيد وإجراءاته وآليات التسجيل.
ويلتزم الممثل القانوني للشخص الاعتباري لأي متحكم أو معالج بأن يعين داخل كيانه القانوني وهيكله الوظيفي موظفًا مختصًا مسئولاً عن حماية البيانات الشخصية، وذلك بقيده في سجل مسئولي حماية البيانات الشخصية بالمركز، ويعلن عن ذلك.

ويكون الشخص الطبيعي المتحكم أو المعالج هو المسئول عن تطبيق أحكام هذا القانون.

ب: التزامات مسئول حماية البيانات الشخصية: هى ما نصت المادة (٩):
يكون مسئول حماية البيانات الشخصية مسئولاً عن تنفيذ أحكام القانون ولائحته التنفيذية وقرارات المركز، ومراقبة الإجراءات المعمول بها داخل كيانه الإشراف عليها، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقا لأحكام هذا القانون. ويلتزم على الأخص بالآتي:
١ – إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها.

٢ – العمل كنقطة اتصال مباشرة مع المركز وتنفيذ قراراته، فيما يخص تطبيق أحكام هذا القانون.

٣ – تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في هذا القانون.

٤ – إخطار المركز في حال وجود أي خرق أو انتهاك للبيانات الشخصية لديه.

٥ – الرد على الطلبات المقدمة من الشخص المعني بالبيانات أو كل ذي صفة، والرد على المركز في التظلمات المقدمة إليه من أي منهما وفقا لأحكام هذا القانون.

٦ – متابعة القيد والتحديث لسجل البيانات الشخصية لدي المتحكم أو سجل عمليات المعالجة لدي المعالج، بما يكفل ضمان دقة البيانات والمعلومات المقيدة به.

٧ – إزالة أي مخالفات متعلقة بالبيانات الشخصية داخل كيانه، واتخاذ الإجراءات التصحيحية حيالها.

٨ – تنظيم البرامج التدريبية اللازمة لموظفي كيانه، لتأهيلهم بما يتناسب مع متطلبات هذا القانون.

وتحدد اللائحة التنفيذية لهذا القانون الالتزامات والإجراءات والمهام الأخرى التي يجب على مسئول حماية البيانات الشخصية القيام بها.

المبحث الثالث
صور الحماية القانونية
(التشريعية)
المطلب الاول
الحماية الإدارية والجنائية.
الفرع الاول
الحماية الإدارية للبيانات الشخصية الرقمية

١- بمقتضى القانون رقم ١٥١ لسنة ٢٠٢٠انشأ مركز[١٨] يتولى الإشراف والمتابعة لتحقيق هذه الحماية الإدارية والذى من صلاحياته أن يوقع جزاءات على المخالف – إداريا أو تأديبا كالإنذار أو وقف العمل لمدة معينة أو غيرها من الجزاءات (م ٣٠ من القانون).

(١٨)**وفقاً للمادة (١٩) من القانون** تنشأ هيئة عامة اقتصادية تسمي «مركز حماية البيانات الشخصية»، تتبع الوزير المختص، وتكون لها الشخصية الاعتبارية، ويكون مقرها الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، وتهدف إلي حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، ولها في سبيل تحقيق أهدافها أن تباشر جميع الاختصاصات المنصوص عليها بهذا القانون

المركز هو هيئة منوط بها مراقبة حسن تطبيق القانون، ووضع القواعد العامة والنظم والاستراتيجيات حماية للبيانات الشخصية، ووضع إجراءات وشروط إصدار التراخيص المختلفة فى إطار تنفيذ أحكام القانون وحدد القانون تشكيلها واختصاصاتها، كما حدد موازنه المركز وموارده المالية.

ونظمت المواد من ١٩ الى ٢٥ أحكامه أي المركز فى الفصل التاسع من حيث نشأته ومقره وهدفه واختصاصاته (م ١٩) وتكوينه (م ٢٠)، وتحديد قراراته (م ٢١) واجتماعاته (م ٢٢)، ومسئولية الرئيس التنفيذي (م ٢٣) والتزامه بعدم إفشاء سر البيانات (م ٢٤) وتعاونه مع نظرائه فى البلاد الأجنبية (م ٢٥).

٢- ويتلقى الشكاوى والبلاغات[١٩] المتعلقة بأحكام هذا القانون وإصدار القرارات الرسمية فى شانها (م ١٩) ،٣٢ : ٣٣) ، لذا يجوز للشخص المعني بالبيانات ولكل ذي صفة أن يتقدم إلى أي حائز أو متحكم أو معالج بطلب يتعلق بممارسة حقوقه القانونية مع التزام المقدم إليه الطلب بالرد عليه خلال ستة أيام عمل من تاريخ تقديمه إليه (م ٣٢ من القانون) ،بحيث تقدم الشكوى الى المركز وله فى ذلك اتخاذ ما يلزم من إجراءات التحقيق ، وعليه أن يصدر قرارة خلال ثلاثين يوماً عمل من تاريخ تقديمها اليه على أن يخطر الشاكي والمشكو فى حقه . ويلتزم الأخير بتنفيذ قرار المركز خلال سبعة أيام عمل من تاريخ إخطاره به، وإفادة المركز بما تم نحو تنفيذه (م ٣٣).

٣- وتتجسد حالات الشكوى فى انتهاك حقه فى حماية بياناته الشخصية والإخلال به، وكذلك فى حالة الامتناع عن تمكينه من استيفاء حقوقه والقرارات الصادرة عن المسئول عن هذه الحماية لدي المعالج أو المتحكم بشأن الطلبات المقدمة إليه (م ٣٣ / ١).

٤- وينشأ بالمركز سجل لقيد مسئولي حماية البيانات الشخصية لدى المتحكم أو المعالج وفقاً للمادة ٨ من القانون.

٥- يملك المركز تعديل او إلغاء التراخيص والتصاريح والاعتمادات فى حالات محدده قانوناً بالنسبة للمحتكم أو المعالج.

---

(١٩) نظم الفصل الثانى عشر من القانون الطلبات والشكاوى التى تقدم من المعنى بالبيانات فى مواجهة المتحكم والمعالج والاطار الزمنى الممنوح كلاً منهما للرد على ذلك الطلب او تلك الشكوى ونص القانون على تقديم الشكوى الى المركز لاتخاذ ما يراه من إجراءات التحقيق ، واتخاذ القرار خلال ٣٠ يوم عمل من تاريخ تقديمها إليه مع إخطار كل من الشاكي والمشكو فى حقه بالقرار ، ويلتزم المشكو فى حقه بتنفيذه خلال سبعه أيام عمل من تاريخ إخطار به ، وإفادة المركز بما تم نحو تنفيذه .

تعديل شروط التراخيص والتصاريح بعد إصدارها استجابة للتشريعات الدولية والوطنية أو بناء على طلب المرخص له أو اندماج المتحكم أو المعالج مع آخرين داخل الدولة أو خارجها أذا كان التعديل ضرورياً لتحقيق أهداف القانون فنصت المادة (٢٨) على انه " يجوز للمركز، وفقًا لاعتبارات المصلحة العامة، تعديل شروط الترخيص أو التصريح بعد إصداره في أي من الحالات الآتية:

١- الاستجابة إلى الاتفاقيات الدولية أو الإقليمية أو القوانين الوطنية ذات الصلة.

٢ - بناءً على طلب المرخص له.

٣ - اندماج المتحكم أو المعالج مع آخرين داخل جمهورية مصر العربية أو خارجها.

٤- إذا كان التعديل ضروريًا لتحقيق أهداف هذا القانون."

- إلغاء التراخيص والتصاريح والاعتمادات بعد إصدارها، فيجوز للمركز إلغاء الترخيص أو التصريح أو الاعتماد بعد إصداره في أي من الحالات الآتية عند مخالفة شروطها أو التنازل عنها للغير بعد موافقة المركز، وعدم سداد رسوم تجديدها أو تكرار عدم الامتثال لقرارات المركز أو صدور حكم بإفلاس المتحكم أو المعالج.

ونصت المادة (٢٩) على انه " يجوز للمركز إلغاء الترخيص أو التصريح أو الاعتماد بعد إصداره في أي من الحالات الآتية:

١ - مخالفة شروط الترخيص أو التصريح أو الاعتماد.

٢ - عدم سداد رسوم تجديد الترخيص أو التصريح أو الاعتماد.

٣ - تكرار عدم الامتثال لقرارات المركز.

٤ - التنازل عن الترخيص أو التصريح أو الاعتماد للغير دون موافقة المركز.

٥- صدور حكم بإفلاس المتحكم أو المعالج."

٥- ويملك الرئيس التنفيذي للمركز سلطة توقيع الجزاءات الإدارية الواردة فى المادة ٣٠ من القانون وهي: " مع عدم الإخلال بأحكام المسئولية المدنية والجنائية، يقوم الرئيس التنفيذي للمركز، في حال ارتكاب أي مخالفة لأحكام هذا القانون بإنذار المخالف بالتوقف عن المخالفة وإزالة أسبابها أو آثارها خلال فترة زمنية يحددها، فإذا انقضت المدة المشار إليها دون تنفيذ مضمون ذلك الإنذار، كان لمجلس إدارة المركز أن يصدر قرارًا مسببًا بما يأتي:

١ - الإنذار بإيقاف الترخيص أو التصريح أو الاعتماد جزئيًا أو كليًا لمدة محددة.

٢ – إيقاف الترخيص أو التصريح أو الاعتماد جزئيًا أو كليًا.

٣ – سحب الترخيص أو التصريح أو الاعتماد أو إلغاؤه جزئيًا أو كليًا.

٤ – نشر بيان بالمخالفات التي ثبت وقوعها في وسيلة إعلام أو أكثر واسعة الانتشار على نفقة المخالف.

٥ – إخضاع المتحكم أو المعالج للإشراف الفني للمركز لتأمين حماية البيانات الشخصية على نفقتهما بحسب الأحوال."

٦–ويكون لبعض العاملين بالمركز الذين يحددهم قرار من وزير العدل بناءً على اقتراح الوزير المختص صفة الضبطية القضائية في إثبات الجرائم المخالفة لهذا القانون (م ٣٤ من القانون).

الفرع الثانى
الحماية الجنائية للبيانات الشخصية الرقمية

١– بمقتضى المادة ٩٩ / ١ من الدستور المصرى الحالي فإن الدعوى الجنائية الناشئة عن وقوع جريمة تتعلق بالاعتداء على الحرية الشخصية أو حرمة الحياة الخاصة، لا تسقط بالتقادم، وللمضرور إقامتها بالطريق المباشر.

٢– كما يوجد قانون مكافحة جرائم تقنية المعلومات وعقوبتها الجنائية ، وقوانين أخرى تتعلق بالإعلام لعام ٢٠١٨ وغيرها مثل قانون تنظيم وسائل الإعلام ، وتودى الى تقنين مراقبة الحياة الإلكترونية(٢٠) .

٣– تنص المادة الثانية من مواد إصدار قانون رقم ١٥١ لسنة ٢٠٢٠ على أن "تسري أحكام هذا القانون والقانون المرافق له على كل من ارتكب إحدى الجرائم المنصوص عليها في القانون المرافق متي كان الجاني من المصريين داخل الجمهورية أو خارجها، أو كان من غير المصريين المقيمين داخل الجمهورية، أو كان من غير المصريين خارج الجمهورية

(٢٠) مؤسسة حرية الفكر والتعبير ، بيان قانون " مكافحة الجريمة الإلكترونية وتنظيم الصحافة والإعلام " فى مصر

Httpp:// abteegyrt . org/res–releares/٢٠١٨ /٠٩/٠٦/١٥٧٦٢–abteegypt.htm .

إذا كان الفعل معاقبًا عليه في الدولة التي وقع فيها تحت أي وصف قانوني وكانت البيانات محل الجريمة لمصريين أو أجانب مقيمين داخل الجمهورية."

٤- كما نص القانون رقم ١٥١ لسنة ٢٠٢٠ على صلاحية بعض العاملين بالمركز فى التمتع بسلطة الضبط القضائي فى إثبات الجرائم لذلك نصت المادة ٣٤ من القانون على أن يصدر بتحديدهم قرار من وزير العدل.

٥- ونص القانون رقم ١٥١ لسنة ٢٠٢٠ على جرائم الاعتداء على حرمة الحياة الخاصة التى منها حماية البيانات الشخصية ويتجسد عقوباتها فى (غرامات أو حبس أو كليهما) ، وذلك فى المواد من ٣٥ : ٤٨ ، وتنص المادة٣٦ منه مثلاً على انه " يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز[٢١] أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات.

وتكون العقوبة الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكب ذلك مقابل الحصول على منفعة مادية أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر".

ويعاقب بالعقوبة ذاتها المتحكم او المعالج الذي يمنع الشخص المعنى بالبيانات من ممارسة حقوقه المخولة له بالقانون. وارتفعت العقوبة بحدها الأدنى والأقصى لتصبح الغرامة من ٥٠٠ ألف الى ٥ ملايين جنية فى حالة مخالفة أحكام التصاريح والتراخيص، وتبنى القانون فكرة عقابية جديدة نسبياً تعاقب المسئول عن الإرادة الفعلية للشخص الاعتباري بالعقوبة ذاتها المقررة عن الأفعال المخالفة لأحكام هذا القانون إذا ثبت علمه بها، وفى حالة أن أسهم إخلاله بواجباته فى وقوعها.

وتنص المادة (٣٧): على أن " يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، كل حائز أو متحكم أو معالج امتنع دون مقتض من القانون عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في المادة (٢) من هذا القانون ويعاقب بغرامة

(٢١) القانون لم ينظم عمل " الحائز " للبيانات ، فلا يتصور أصلاً حالة حيازة الحائز لتلك البيانات بسبب قانونى .

لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في المادة (٣) من هذا القانون."

وتنص المادة (٣٨): "يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، كل متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في المواد (٤، ٥، ٧) من هذا القانون."

والمادة (٣٩): تنص " يعاقب بالغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، كل ممثل قانوني للشخص الاعتباري لم يلتزم بأحد واجباته المنصوص عليها في المادة (٨) من هذا القانون."

والمادة (٤٠) تنص " يعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، كل مسئول حماية بيانات شخصية لم يلتزم بمقتضيات وظيفته المنصوص عليها في المادة (٩) من هذا القانون. ويعاقب بغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز خمسمائة ألف جنيه إذا وقعت الجريمة نتيجة لإهمال مسئول حماية البيانات الشخصية."

والمادة (٤١) تنص على انه "يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل حائز أو متحكم أو معالج جمع أو أتاح أو تداول أو عالج أو أفشي أو خزن أو نقل أو حفظ بيانات شخصية حساسة بدون موافقة الشخص المعني بالبيانات أو في غير الأحوال المصرح بها قانونًا."

والمادة (٤٢) تنص " يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل من خالف أحكام حركة البيانات الشخصية عبر الحدود المنصوص عليها في المواد (١٤، ١٥، ١٦) من هذا القانون."

المادة (٤٣) تنص" يعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، كل من خالف أحكام التسويق الإلكتروني المنصوص عليها في المادتين (١٧، ١٨) من هذا القانون."

والمادة (٤٤) تنص على " يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، كل عضو مجلس إدارة أو أي من العاملين بالمركز خالف الالتزامات المنصوص عليها في المادة (٢٤) من هذا القانون."

ونصت المادة (٤٥) على أنه " يعاقب بغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، كل من خالف أحكام التراخيص أو التصاريح أو الاعتمادات المنصوص عليها في هذا القانون."

وتنص المادة (٤٦)" يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، كل من منع أحد العاملين بالمركز ممن يتمتعون بصفة الضبطية القضائية من أداء عمله."

وتنص المادة (٤٧) على انه " يعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا ثبت علمه بها، وكان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة.
ويكون الشخص الاعتباري مسئولاً بالتضامن عن الوفاء بما يحكم به من تعويضات إذا كانت المخالفة قد ارتكبت من أحد العاملين لديه وباسم الشخص الاعتباري ولصالحه."

وكذا تنص المادة (٤٨): انه" في جميع الأحوال، وفضلاً عن العقوبات المنصوص عليها في هذا القانون، تقضي المحكمة بنشر حكم الإدانة في جريدتين واسعتي الانتشار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه. وفي حالة العود، تضاعف العقوبات الواردة في هذا الفصل بحديها الأقصى والأدنى.
ويعاقب على الشروع في ارتكاب الجرائم المنصوص عليها في هذا القانون بنصف العقوبة المقررة لها.

٦- وتنص المادة الخامسة من قانون إصدار هذا القانون على أن " تختص المحاكم الاقتصادية[٢٢]بنظر الجرائم التي ترتكب بالمخالفة لأحكام القانون المرافق." ولكنه لم تخولها الاختصاص بالمنازعات المدنية رغم أن نظامها يحتوي على ذلك. ويمكن أن تتخذ الإجراءات الكترونياً أمامها وفقاً للمادة الثانية للقانون رقم ١٤٦ لسنة ٢٠١٩ المعدلة للقانون رقم ١٢٠ لسنة ٢٠٠٨.

المطلب الثانى

الحماية المدنية للبيانات الشخصية

لقد تضمنت المادة ٩٩ من الدستور المصرى أن " كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر. وتكفل الدولة تعويضاً عادلاً لمن وقع عليه الاعتداء، وللمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضماً إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون."

(٢٢) أنشئت بالقانون رقم ١٢٠ لسنة ٢٠٠٨ جريدة رسمية العدد ٢١ ونشر فى ٢٢ / ٥/ ٢٠٠٨ ، وتعديلاته بالقانون رقم ١٤٦ لسنة ٢٠١٩ ، علاوة على اللائحة التنفيذية .

لم ينص القانون رقم ١٥١ لسنة ٢٠٢٠ على أية نصوص تنظم هذه الحماية المدنية مباشرة، ولكنه نص فى المادة ٣٣ / ١ على حق صاحب الحماية فى اللجوء الى القضاء، والمادة ٣٥ على حق المضرور فى الادعاء مدنياً.

وعلى ذلك وتطبيقاً للقواعد العامة فى المسئولية المدنية يستطيع المضرور رفع دعوى المسئولية بدون تقادم لهذه الدعوى. ويجوز أن ينضم اليه فيها المجلس القومي لحقوق الإنسان كمتدخل انضمامي، مطالباً بالتعويض على أساس هذه المسئولية الدستورية والقانونية أي المدنية مستخدماً المادة ١٦٣ من القانون المدني المصرى ومطبقاً لأحكام المسئولية المدنية به.

وتنص المادة ١٠ من الفصل الخامس من قانون الحماية عن "إجراءات إتاحة البيانات الشخصية " على أن "يلتزم كل من المتحكم والمعالج والحائز عند طلب إتاحة البيانات الشخصية بالإجراءات الآتية:

١ – أن يكون بناءً على طلب كتابي يقدم إليه من ذي صفة أو وفقًا لسند قانوني.

٢ – التحقق من توافر المستندات اللازمة لتنفيذ الإتاحة والاحتفاظ بها.

٣ – البت في الطلب ومستنداته خلال ستة أيام عمل من تاريخ تقديمه إليه، وعند صدور قرار بالرفض يجب أن يكون الرفض مسببًا، ويعتبر مضي المدة المشار إليها دون رد في حكم الرفض."

وتنص المادة ١١ من الفصل الخامس من قانون الحماية بعنوان " إجراءات إتاحة البيانات الشخصية " على أن " يكون للدليل الرقمي المستمد من البيانات الشخصية طبقًا لأحكام هذا القانون ذات الحجية في الإثبات المقررة للأدلة المستمدة من البيانات والمعلومات الخطية متي استوفت المعايير والشروط الفنية الواردة باللائحة التنفيذية لهذا القانون."

كما يجوز الصلح بين المتهم والمجني عليه أو وكيلة الخاص أو خلفة العام وبموافقة المركز أمام النيابة العامة او المحكمة المختصة بحسب الأحوال، وذلك فى الجنح المنصوص عليها فى المواد ٣٦، ٤١، ٤٣ من القانون، كما يكون التصالح مع المركز فى الجنح المنصوص عليها بالمواد ٤٢، ٤٤: ٤٥ من هذا القانون، فى أي حالة كانت عليها الدعوى (م ٤٩).

ونصت المادة ٤٩ من القانون بانه " يجوز للمتهم – فى أي حالة – الصلح أمام النيابة أو المحكمة في أي حالة كانت عليها الدعوي الجنائية، وقبل صيرورة الحكم باتًا، إثبات الصلح مع المجني عليه أو وكيله الخاص أو خلفه العام، وبموافقة المركز أمام النيابة العامة أو المحكمة

المختصة بحسب الأحوال، وذلك في الجنح المنصوص عليها في المواد (٣٦: ٤١، ٤٣) من هذا القانون.

-ويكون التصالح مع المركز في الجنح المنصوص عليها بالمواد (٤٢، ٤٤، ٤٥) من هذا القانون في أي حالة كانت عليها الدعوي.

وفي جميع الأحوال، يجب على المتهم الذي يرغب في التصالح أن يسدد قبل رفع الدعوي الجنائية مبلغًا يعادل نصف الحد الأدنى للغرامة المقررة للجريمة.

ويسدد المتهم راغب التصالح بعد رفع الدعوي وقبل صيرورة الحكم باتًا نصف الحد الأقصى للغرامة المقررة للجريمة، أو قيمة الغرامة المقضي بها أيهما أكبر.

ويكون السداد في خزانة المحكمة المختصة أو النيابة العامة أو المركز بحسب الأحوال.

ويترتب على التصالح انقضاء الدعوي الجنائية دون أن يكون له أثر على حقوق المضرور من الجريمة."

وبالنسبة للجهة المختصة – فى اعتقادنا – تأسيسا على ما جاء بالمادة ٥ من قانون الإصدار هى المحكمة الاقتصادية أو القضاء العادي وفقاً لأحكام قانون المرافعات، كما يستفيد الشخص المعنى بالبيانات من كافة صور الحماية القضائية.

الخاتمة

لا شك في أن إصدار مصر لقانون حماية البيانات الشخصية يعد خطوة على الطريق الصحيح نحو التنمية الاقتصادية لمصر بوجه عام ودفعة للأمام للاقتصاد الرقمي والتجارة الإلكترونية بوجه خاص.

وبرغم من أهمية القانون البالغة، فإنه لا يخفى على أحد أنه يلقي بأعباء عديدة وجديدة على كثير من المتعاملين الحاليين في البيانات وهو ما دعا المشرع المصري إلى النص في مواد إصداره على مدة أعطاها للمخاطبين بأحكامه لتوفيق أوضاعهم تماشيًا مع أحكام القانون.

فنصت المادة الرابعة من مواد الإصدار على أن يُصدر الوزير المعني بشؤن الاتصالات وتكنولوجيا المعلومات اللائحة التنفيذية للقانون المرافق خلال ستة أشهر من تاريخ العمل بهذا القانون، وهي لم تصدر إلى الآن.

كما نصت المادة السابعة من مواد الإصدار على أن يُنشر هذا القانون في الجريدة الرسمية، ويُعمل به بعد مضي ثلاثة أشهر من اليوم التالي لتاريخ نشره.

أما المادة السادسة من مواد الإصدار فنصت على أن يلتزم المخاطبون بأحكام هذا القانون بتوفيق أوضاعهم طبقًا لأحكام القانون المرافق ولائحته التنفيذية، وذلك خلال سنة من تاريخ صدور هذه اللائحة، ولما كان القانون قد صدر في يوليو ٢٠٢٠، بما يعني أن تاريخ العمل الفعلي للقانون لن يبدأ قبل أبريل ٢٠٢٢ حيث إن حتى ميعاد الأشهر الستة الممنوحة للوزير المعني بشؤون الاتصالات لإصدار اللائحة التنفيذية هو ميعاد تنظيمي لا يرتب أثرًا على عدم صدور اللائحة في ذلك الميعاد ، مما قد يؤدي إلى مد فترة البدء في النفاذ الفعلي لمعظم أحكام القانون.

سوف تسفر الفترة القادمة والتجارب العملية عند بدء العمل بأحكام القانون عن الممارسات الفضلى التي يجب أن تتوفر والتعديلات التي يمكن إدخالها على القانون من أجل خدمة الغرض منه وهو النهضة الاقتصادية والحماية المثلى لخصوصية أفراد الشعب المصري.

يعتبر قانون حماية البيانات الشخصية المصرى تنظيماً شاملاً لها، يهدف الى حماية خصوصية الأفراد من خلال عمليات جمعها ومعالجتها والإفصاح عنها، ويقدم إطاراً مفصلاً يشمل تحديد المفاهيم والمصطلحات المتعلقة بها، وتحديد معايير معالجة للبيانات، وحقوق والتزامات أطرافها المعنيين، والسيادة على البيانات وعقوباتها فى حالة الإخلال بأحكام القانون الذي ينظم حمايتها، وأن كنا فى انتظار صدور لائحته التنفيذية.

وهذا القانون من حلال تحليلنا له يبدو وللوهلة الاولى انه منسجم مع المعايير الدولية فى نواح معينة، وان كانت هناك بعض نصوصه تحتوي على غموض وثغرات قد تسمح بانتهاك الحق فى الخصوصية لان المشكلة تكمن ليس فى نصوص القانون فى حد ذاتها بل إمكانية تطبيقها وتنفيذها.

كما يشكل هذا القانون خطوة مهمة الى الأمام فى مجال حماية البيانات ونقطة انطلاق لمصر تجذب شركات الاستثمار الرقمية وغيرها من الشركات الدولية ولمواكبة دول العالم المتقدم فى مجال حماية البيانات الشخصية للإنسان رقمياً!

أن يعدل قانون أنشاء المحاكم الاقتصادية فى المادة ٤ بحيث تحوي على قاعدة حماية البيانات الشخصية، ولقد تم تعديلها بالقانون رقم ١٤٦ لسنة ٢٠١٩.

حيث إن إقرار قانون حماية البيانات الشخصية خطوة هامة لتوفير الحماية اللازمة لخصوصية المُستخدمين، وتتعاظم هذه الأهمية في ظل وجود بيئة تشريعية فقيرة تغيب عنها الضمانات المُتعلقة بخصوصية الأفراد بشكل عام، هذا بجانب غياب القواعد التنظيمية المُتعلقة بالقواعد والإجراءات اللازمة لحماية البيانات الشخصية، وعدم وضوح سُبل الإنصاف في حالة الاعتداء على الحياة الخاصة، وبناء على القراءة المتقدمة لنصوص القانون نستنتج الاتي:

أولا: النتائج:

١- أن الاعتداء على خصوصيات الأفراد وحتى الشركات أو الدول باستغلال مركب لقدرات وخصائص الذكاء الاصطناعي أمر واقع وحادث دون أن تدرك، وحماية الخصوصية تبدأ من السلوكيات الذاتية للأفراد وأخلاقه ودينه وآداب المجتمع الذي يعيش فيه وعاداته وتقاليده، ويلي ذلك دور المؤسسات فى الدولة، ومن ثم لابد من تضافر الجهود للعمل معاً لحماية خصوصياتنا سواء العادية والحساسة أو الأسرية بطريق تقليدية أو إلكترونية.

٢- أن انتهاك الخصوصية يعتبر مخالفة شرعية ودينية وكذلك هو انتهاك صارخ للاتفاقيات الدولية ،والدساتير، والقوانين ،وكل ما يتعلق بالضوابط والممارسات الخاصة بحماية الخصوصية ،مما يدفعنا الى اقتراح التوعية بمخاطر استخدام العامة لهذه التطبيقات المستقلة للبيانات الذكية والضخمة وتحليل البصمة الحيوية ، وإتاحة تطبيقات التعرف الى الأشخاص ،وتشديد تجريم استخدام هذه التطبيقات من قبل العامة وتطوير التقنيات وإتاحتها دون ضوابط أو تقنين ، وحجب مواقع الشركات المستخدمة مثل هذه الخدمات ، وإنذارها فى حال تأثر أي فرد بهذه التقنيات سلباً ودون مسوغ قانونى ، ومساءلتهم جنائياً ومدنياً .

٣- وفى نهاية المطاف يجب احترام خصوصية البيانات الشخصية للإنسان من خلال حماية بياناته ومعلوماته ومعطياته بأفضل الطرق والوسائل التى تضمن عدم انتقالها للغير سواء تعلقت البيانات بمحتواه الدراسي أو التعليمي أو الجامعي أو بالعمل أو بالمركز الاجتماعي أو الصحي أو النفسي أو الوضع المادي أو المجتمعي لعضويته فى النقابات او الجمعيات أو المراكز أو النوادي أو اشتراكه فى الأحزاب أو غيرها ، وكذلك بياناته الشخصية المتعلقة بالأحكام الجنائية أو الجزائية والعقوبات الصادرة ضده أو البيانات الشخصية المتعلقة بوضع الشخص المدني وحياته الجنسية والمعلومات الإحصائية أو الصحية ، وذلك يمكن من تحديثها ولا يمكن معالجتها أو تصنيفها أو الإفصاح عنها أو نقلها للغير إلا فى اطار القانون والأنظمة المرعية. وتكون الجهات (الحائز ، المتحكم ، المعالج ، المسئول) مسئولة عن هذه الحماية – إدارياً وجنائياً ومدنياً – ويجب أن يتم التأمين والحصول عليها ونقلها وتبادلها بواسطة الهاتف أو الإنترنت أو غيرها من وسائل التقدم التكنولوجيا المدنية ، ويمكن تبادل وتشارك هذه البيانات مع جهات ومؤسسات أخرى ، ويمكن لصاحب البيانات مراجعة الجهة المسئولة عن هذه البيانات فى حالات المعالجة أو تسجيلها والحصول على المعلومات بصددها والاستعلام عن الغاية من تسجيلها والتأكد من استخدامها للغاية المحددة من عدمها ، وكذلك الاستعلام عن تمام نقلها الى طرف ثالث داخل الجهة أو خارجها ، وطلب استكمالها فى حال نقص بها أو عدم كفايتها أو طلب تصحيحها فى حال وجود خطأ فيها ، وكذلك طلب مسح هذه البيانات أو إلغاؤها ، وكذلك له الحق فى الاعتراض فى حال يتم عن المعالجة بواسطة الأنظمة الاتوماتيكية أي ضرر شخصي لصاحب البيانات الشخصية ، وله الحق فى تلافى الأضرار الناجمة عن استخدام البيانات الشخصية بطريقة مخالفة للقانون

تسبب فى الأضرار بصاحبها ، مع توافر طرق وآليات تقديم الطلبات والشكاوى المتعلقة بمعالجة البيانات الشخصية وإجراءاتها وكيفية البت فيها ومواعيدها .

٤- حدد المشرع حقوق الشخص المعنى بالبيانات والتزامات كل من الحائز والمتحكم والمعالج والمسئول عنها سواء قبل المعالجة أو أثناءها.

٥- حظر القانون معالجة البيانات الشخصية بدون موافقة مسبقة من صاحبها ما لم تكن المعالجة ضرورية للمصلحة العامة او لإقامة أي من إجراءات المطالبة بالحقوق وبالدعاوى القضائية. كما حدد القانون ضوابط المعالجة فى تأمين البيانات والمحافظة على سريتها وخصوصياتها والإجراءات والتدابير المتوفرة لديها لضمان عدم اختراقها أو إتلافها أو تغيرها أو العبث بها، وكذلك من ضوابط نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة.

ثانيا: ملاحظات على القانون:

١- أين التنظيم القانوني لحماية البيانات الشخصية غير المعالجة الكترونياً؟، وهي فى الواقع العملي كثيره.

٢- قصر الحماية على الأشخاص الطبعين دون الاعتباريين، فلماذا لم يدرج فى الحماية القانونية للبيانات الخاصة بالأفراد أو بالمتوطنين أو بالشخص الاعتباري الخاص كالشركات والجمعيات والمؤسسات مما يستلزم تعديل هذا القانون ليشملهم بحمايته؟

٣- لم يتم اللجوء الى الحوار المجتمعي لمناقشة القانون قبل صدوره، وان كان الآن يتم قيام وزارة الاتصالات وتكنولوجيا المعلومات بعقد حوارات مجتمعية مع مشغلي المحمول وشركات التكنولوجيا المحلية والعالمية والقطاعات المعنية وذلك لمناقشة مشروع اللائحة التنفيذية والتى لم تصدر حتى الآن – لقانون حماية البيانات الشخصية.

٤- لم تتناول الديباجة قوانين ذات صلة بهذا القانون.

٥- عرف البيانات تعريفاً ضيقاً وليس واسعاً.

٦- محل الحماية هى البيانات وليست المعلومات لان الاولى هى حقائق بعكس الثانية فهي نتائج.

٧- يلاحظ على هذا القانون عدم إدراج قوانين ذات صلة به فى الديباجة، وعدم إصداره اللائحة التنفيذية حتى هذه اللحظة. كما غاب اشتراك فئات المجتمع المدني المعنيين بذلك – ونتمنى تداركه قبل إصدار اللائحة التنفيذية له – وكذلك الشفافية فى إصداره، كذلك عدم استقلالية المركز بل هو تابع للسلطة التنفيذية وليست جهة مستقلة عنها. ويجب أن تكون السلطات المختصة لديها وعى بالتطورات التكنولوجية وتستجيب لها بشكل يحمى ويعزز حقوق الإنسان المادية والرقمية بدلاً من انتهاكها أو السماح بذلك. وفى حالة عدم معالجة هذه الأمور فى اللائحة التنفيذية المزمع إصدارها ، فيلزم تعديل نصوص القانون ذاته بالنص على الإعفاء المادي من مزاولة الحقوق الأساسية المرتبطة بحماية البيانات كالحق فى المعرفة ، والتخفيف من سلطوية أجهزة الدولة على التحكم فى آليات قواعد البيانات والسيطرة عليها ، وخلق سلطة متخصصة بالرقابة تتميز بالاستقلالية والشفافية ، وتتم المشاركة للمجتمع المدني فى صياغة اللائحة ، ثم بدأ تفسير اللائحة لاصطلاح " حرمة الحياة الخاصة" دون التطرق الى تفاصيل حتى لا نقع فى تفاسير مختلفة لمصطلحات مبهمة .

ثالثا: التوصيات:

١- يجب على السلطات المصرية إجراء مُراجعة تشريعية واسعة لكافة القوانين الأخرى التي تنظم المُعاملات اليومية التي تتطلب مُشاركة بيانات الأفراد مع الغير، وذلك لجعل أحكام قانون حماية البيانات فعالة، حيث يعتبر هذا القانون هو القاعدة العامة المعنية بتنظيم وحماية كل ما يتعلق بتداول البيانات الشخصية مع مشاركة المجتمع المدني قبل إقرار هذه القوانين.
ضرورة تبنى المفهوم الواسع لاصطلاح البيانات بحيث تكون المعالجة فيها "بأية وسيلة أخرى "يفرزها التقدم التكنولوجي بمفهوم المعالجة ومن ثم الخضوع لأحكام القانون.

٢- تجب على السلطات إعادة النظر في القواعد الإجرائية المنصوص عليها بقانون حماية البيانات الشخصية، على أن يتم تعديل القانون بإضافة كافة الضوابط المُتعلقة بحماية البيانات أو مُشاركتها مع أطراف أخرى، دون الإحالة إلى اللوائح والقرارات التنفيذية، حيث أحال قانون حماية البيانات الشخصية، تفصيلات إجرائية جوهرية إلى اللائحة التنفيذية، وهو ما يتعارض مع الطبيعة الخاصة لقانون حماية البيانات، فهو بطبيعته قانون ذو طابع إجرائي، ما يعني ضرورة أن تكون القواعد الإجرائية شاملة وكافية لتطبيقها بذاتها، وأن يتم

النص عليها في القانون لضمان استقرارها، دون الإحالة إلى لوائح وقرارات تنفيذية تصدرها الجهات التنفيذية، وتستطيع تغييرها دون الرجوع إلى السلطة التشريعية.

إنشاء لجنة وطنية – بدلا من المراكز – للحقوق والحريات تمشياً مع التشريعات المقارنة بحيث تكون لجنة إدارية ذات اختصاص قضائي والمتعلقة باحترام وتطبيق أحكام القانون المعنى محل جهة الإدارة فى إنفاذ أحكام القانون.

يجب تعديل القانون بإضافة نصوص إجرائية واضحة تُنظم الإجراءات المُتعلقة بمحو وتصحيح وتعديل البيانات الشخصية لدى الحائز أو المُتحكم أو المُعالج.

٣- أنشا لجنة وطنية مستقلة عن السلطة التنفيذية للمعلوماتية والحريات وتعتبر بمثابة لجنة إدارية ذات اختصاص قضائي بدلاً من جهة إدارية تتبع السلطة التنفيذية.

تجب على السلطات مُراعاة القواعد المُتعلقة بفرض رسوم لحصول الأفراد على بياناتهم الشخصية نظرًا إلى ارتفاع الحد الأقصى المنصوص عليه في القانون بشكل مبالغ فيه) عشرون ألف جنيه مصري)، لذلك يجب أن تُراعي قرارات مركز حماية البيانات التكلفة الفعلية لاستخراج البيانات أو تحديد مبلغ معقول يتفق مع الحماية القانونية لهذه البيانات.

٤- يجب أن يتبع إصدار قانون حماية البيانات الشخصية تشكيل هيئات مُستقلة قادرة على مُتابعة الالتزامات القانونية للمُخاطَبين بالقانون.

٥- ضرورة نشر الوعي والثقافة المطلوبة لدى مستخدمي شبكة الإنترنت أو غيرها تفادياً لوقوعهم فى أعمال نصب واحتيال الكتروني، وحتى لا يكونوا ضحايا تنتهك خصوصياتهم من قبل الأخرين. ورفع وعي المُستخدمين والجهات، وفي هذا الشأن يجب تعديل النصوص الخاصة بتشكيل مجلس إدارة مركز حماية البيانات، بما يضمن تمثيل الأطراف المُختلفة من أصحاب المصالح والمُستخدمين.

٦- ضرورة تعديل نصوص قانون العقوبات المصرى لمواجهة ظاهرة الإجرام المعلوماتي وتامين حماية فعالة للحياة الخاصة بحيث توفى الجريمة المعلوماتية على نحو واسع وتفرد العقوبة المناسبة لها وتجريم الأفعال التى جاءت فى القانون المقارن.

تجب إعادة صياغة النصوص المُتعلقة بدور ومسؤوليات مركز حماية البيانات في حالة مُشاركة البيانات مع أطراف خارج الحدود المصرية، ومن أهم هذه الالتزامات، توضيح المخاطر المترتبة على مُشاركة البيانات مع أطراف خارج الحدود المصرية والتي لا تلتزم

بالحد الأدنى من المعايير والإجراءات اللازمة لمُشاركة البيانات، كذلك توضيح دور مركز حماية البيانات في عملية تلقي ومُتابعة الشكاوى التي تتم في حالة تعرض البيانات الشخصية لأي انتهاك أثناء مُشاركتها مع أطراف خارج الحدود المصرية، مع ضرورة النص صراحة على السياسات والمعايير والضوابط اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود، حيث أن القانون قد أحال هذا الأمر إلى اللائحة التنفيذية، وهو أمر لا يستقيم مع أهمية هذه الإجراءات.

٧- يجب تعديل النصوص التي تتعلق بحقوق المُستخدم، لتشمل إلزام المُتحكم أو المُعالج بتقديم البيانات الشخصية التي يطلبها المُستخدم بطريقة مُلائمة يكون للمُستخدم الحق في تحديدها أو اختيارها من بين طرق وصيغ مُتعددة تتفق وحاجة المُستخدم، مع النص على آلية إبلاغ المُستخدم عن حدوث انتهاك للبيانات الشخصية الخاصة به والمدى الزمني الذي يجب أن يتم خلاله إخطار من وقع في حقه الانتهاك.

٨- يجب تعديل القانون بإضافة نصوص تُلزم الحائز أو المُتحكم، عند جمع البيانات بشكل مُباشر من المُستخدمين، أن يُسلم المُستخدمين قائمة تتضمن الحقوق الأساسية المُتعلقة بالبيانات التي تم جمعها أو مُعالجتها، على أن تتضمن هذه القائمة، أغراض المُعالجة، وسُبل الاتصال بالحائز أو المُتحكم أو المُعالج لمحو أو تعديل البيانات الشخصية.

٩- ضرورة تعديل القانون بما يتناسب مع المعايير الدولية وضبط مصطلحاته بدقة حتى لا تترك للائحة ولا للتفسيرات القضائية المختلفة وتحديد فكرة المصلحة المشروعة بدقة.

١٠- استخدام أحكام القضاء فى تطوير قواعد ونصوص حماية الحياة الخاصة لمواجهة ما يستجد من مخاطر وأفعال وجرائم الكترونية.