دور التشريعات في إرساء الحماية المدنية للبيانات الشخصية عبر شبكة الإنترنت

الباحث/ حامد محمد حسين محمد على دشتي

(ISSN: 2537 - 0758)

دور التشريعات في إرساء الحماية المدنية للبيانات الشخصية عبر شبكة الإنترنت

الباحث/ حامد محمد حسين محمد على دشتي

ملخص:

إنَّ خصوصية البيانات أو قوانين حماية البيانات الشخصية تمنع إفشاء البيانات الشخصية المتعلقة بالأفراد أو إساءة استخدامها، إنَّ هناك الكثير من الدول على مستوى العالم قامت بتشريع قوانين كاملة للخصوصية، فمثلاً في أغلبية الدول الأوروبية وكذلك دول أمريكا اللاتينية، بالإضافة إلى بعض الدول العربية.

وبناءً على ذلك نقسم هذا البحث إلى قسمين على النحو الآتي:

القسم الأول: إطار حماية البيانات الشخصية في الوطن العربي.

القسم الثاني: إطار حماية البيانات الشخصية في التشريعات الأجنبية.

القسم الأول

إطار حماية البيانات الشخصية وتشريعات تقنية المعلومات في الوطن العربي

أولاً: في سلطنة عمان:

في البداية بموجب المرسوم السلطاني رقم ٢٠٠١/٧٢ المنشور في الجريدة الرسمية العمانية رقم ٦٩٨ تاريخ ٢٠٠١/٧/١م، تم تعديل بعض أحكام قانون الجزاء العماني رقم ٧ لعام ١٩٧٤، ومن ضمن هذه التعديلات: إضافة الفصل الثاني مكرر على الباب السابع، تحت عنوان جرائم الحاسب الآلي (المواد ٢٧٦ مكرر ١، و٢٧٦ مكرر ٢، و٢٧٦ مكرر ٣، و٢٧٦ مكرر، ٢٧٤ مكرر ٢، و٢٧٦ مكرر ٣، و٢٧٦ مكرر ٤.

وقد نصت المادة (٢٧٦ مكررًا): على أنه يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر، ولا تزيد عن سنتين، وبغرامة من مائة ريال إلى خمسمائة ريال، أو بإحدى هاتين العقوبتين، كل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الأفعال الآتية:

١. الالتقاط غير المشروع للمعلومات أو البيانات.
٢. الدخول غير المشروع على أنظمة الحاسب الآلي.
٣. التجسس والتصنت على البيانات والمعلومات.
٤. انتهاك خصوصيات الغير، أو التعدي على حقهم في الاحتفاظ بأسرارهم.
٥. تزوير بيانات، أو وثائق مبرمجة أيًا كان شكلها.
٦. إتلاف وتغيير ومحو البيانات والمعلومات.
٧. جمع المعلومات والبيانات وإعادة استخدامها.
٨. تسريب المعلومات والبيانات.

٩. التعدي على برامج الحاسب الآلي سواء بالتعديل، أو الاصطناع.
١٠. نشر واستخدام برامج الحاسب الآلي، بشكل انتهاكًا لقوانين حقوق الملكية والأسرار التجارية[١].

كما نصت المادة (٢٧٦ مكررًا ١): على أنه: "يُعاقب بالسجن مدة لا تقل عن ستة أشهر، ولا تزيد عن سنتين، وبغرامة لا تقل عن مائة ريال، ولا تزيد عن خمسمائة ريال، أو بإحدى هاتين العقوبتين كل من استولى أو حصل على نحو غير مشروع على بيانات تخص الغير، تكون منقولة، أو مختزنة، أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات.[٢]"

ونصت المادة (٢٧٦) مكررًا (٢): على أنه: "تضاعف العقوبة إذا ارتكبت الأفعال المُشار إليها في المادة (٢٧٦) مكررًا، و(٢٧٦) مكررة (١) من مستخدمي الكمبيوتر.

ونصت المادة (٢٧٦) مكررة (٣): على أنه "يُعاقب بالسجن مدة لا تزيد عن خمس سنوات، وبغرامة لا تتجاوز ألف ريال كلاً من:
١. قام بتقليد، أو تزوير بطاقة من بطاقات الوفاء، أو السحب.
٢. استعمل، أو حاول استعمال البطاقة المقلدة، أو المزورة مع العلم بذلك.
٣. قبل الدفع ببطاقة الوفاء المقلدة، أو المزورة مع العلم بذلك.

ونص في المادة (٢٧٦) مكررًا (٤): على أنه: "يُعاقب بالسجن مدة لا تزيد عن ٣ سنوات، وبغرامة لا تتجاوز خمسمائة ريال كلاً من:
١. استخدم البطاقة كوسيلة للوفاء، مع علمه بعدم وجود رصيد له.
٢. استعمل البطاقة بعد انتهاء صلاحيتها، أو إلغائها وهو عالم بذلك.
٣. استعمل بطاقة الغير بدون علمه.

وبإمعان النظر في هذه النصوص، نجد أن المشرّع العماني اختار طريق إضافة النصوص الخاصة إلى القسم الخاص في قانون العقوبات (التشريع الجزائي العام)، ولم يختر طريقة سن تشريع خاص، كما لم يختر نموذج النص على مساواة الأموال المنقولة المادية بغير المادية لأغراض انطباق النصوص المتعلقة بالجرائم الواقعة على الأموال، وحسنًا فعل في هذا الشق إذ تتمايز كما عرفنا صور جرائم الكمبيوتر، من حيث مبناها وطبيعتها وسلوكياتها عن الجرائم التقليدية، ليس فقط من ناحية محل الجريمة[٣].

كما أنه بالصورة التي تضمنها نص على بعض صور جرائم الخصوصية، أو انتهاك حرية الشخص في بياناته الخاصة المعالجة آليا، فلم ينص على بقية صور الاعتداء على الخصوصية، كنقل البيانات دون إذن، أو استغلالها في نشاط غير المعدة له، ثم أغلق النص الطريق على وضع تشريع تكاملي في ميدان الخصوصية، يتناول

(ISSN: 2537 - 0758)

الجوانب المتعلقة بحماية الأفراد من مخاطر الجمع الحكومي للبيانات، ومسائل تعيين جهات الرقابة على عمليات جمع ومعالجة ونقل البيانات، وغيرها الكثير من المسائل الموضوعية والإجرائية ذات الصلة بموضوع الخصوصية، إضافة إلى بقية صور الحماية الجزائية، خاصة من الموظفين المناط بهم جمع وتداول واستخدام البيانات الشخصية.

المادة ٢٧٦ مكررًا ١ نصت على تجريم صورة إضافية، وهي الاستيلاء على البيانات، لكنها لم تنص على سرقة وقت الكمبيوتر، أو صور أخرى متصلة بتعطيل عمل الأنظمة الإلكترونية، كما لم تتضمن النصوص، ولم تتعرض احتيال الكمبيوتر، وإن كانت النصوص تضمنت بعض صوره من الناحية الفنية.

أما المادة ٢٧٦ مكررًا ٤ فقد عالجت ثلاث صور من صور إساءة استخدام بطاقات الوفاء الإلكترونية، ويؤخذ على النص تقيده باصطلاحات مقيدة، في حين كان يمكنه أنْ يكون أكثر اتساعًا حين يجرم صور الاعتداء المذكورة على كل أنواع البطاقات، منعًا للدفع بأنَّ البطاقة محل الاعتداء ليست بطاقة وفاء.

وعندما صدر قانون الجزاء العماني الجديد رقم ٧ لسنة ٢٠١٨، فقد خلت نصوصه من الجرائم المتعلقة بالحاسب الآلي، حيث تم إلغاء تلك الجرائم من قانون الجزاء لأنها غير ذات جدوى، أن يتم تنظيمها عن طريق قانون عام هو قانون الجزاء، خاصة بعد إصدار قانون مكافحة جرائم تقنية المعلومات رقم ١٢ لسنة ٢٠١١، والذي نظم كافة الجرائم التي ترتكب من خلال الوسائل الإلكترونية.

هذه الحقائق التي بدت واضحة أمام جهات التشريع والقضاء في النظم المقارنة، بعد جدل طويل وتقييم واسع، استدعت أنْ تتدخل العديد من الدول الأجنبية– التي تقارب قوانينها قوانيننا العقابية العربية، بل تعد أكثر اتساعًا منها في هذا الجانب– أقول استدعى تدخل المشرعين في هذه الدول لتعديل القوانين الجنائية، أو سن قوانين جديدة لمواجهة هذه الظاهرة المستجدة، فبعض الدول عدلت قوانينها بالنص صراحةً على إنزال معطيات الكمبيوتر، منزلة المال المادي المنقول، وذلك لتحقق إمكانية تجريم المعتدين على هذا المال بنصوص جرائم السرقة، والاحتيال، والإتلاف، وغيرها، وبعضها اتجه نحو سن تشريعات مستقلة لتجريم جرائم الكمبيوتر، أو استحداث نصوص مستقلة وإضافتها إلى تشريعاتها القائمة، وهذا المسلك امتد ليشمل الدول نفسها التي تحدت المسلك الأول، فعادت لسن تشريعات جديدة، لعدم كفاية التعديلات التي أحدثتها(٤).

ثانيًا: في مصر:

نجد أنَّ مكافحة جرائم الكمبيوتر في مصر تمت معالجتها بقوانين عامة، كالقانونين المدني والجنائي، فنجد في المادة التاسعة من القانون ٢٦٠ لسنة ١٩٨٠ في شأنْ

الأحوال المدنية المعدل بالقانونين رقم ١١ لسنة ١٩٦٥ و١٥٨ لسنة ١٩٨٠، على أنَّ البيانات التي تحويها سجلات الأحوال المدنية تعتبر سرية، وقد جاء بالمذكرة الإيضاحية للقانون: "أنه لما كانت هذه السجلات تحوي أدق البيانات عن حالة الشخص، فقد أسبغت عليها السرية حتى يطمئن كل شخص على ما يقدمه من بيانات". إنَّ نطاق السرية يمتد إلى كل من لا يفرض عليه واجبه– طبقًا لقانون الأحوال ولائحته التنفيذية والقرارات المنفذة له– الاطلاع على هذه البيانات، وذلك ما لم تصدر سلطة قضائية أو سلطة تحقيق قرارًا بالاطلاع عليها أو فحصها، لأنَّ الصالح العام يفضل مصالح الشخص في المحافظة على سرية بياناته، وباعتبار هذه البيانات سرًا فإن إفشاءها من قبل الموظف الملزم بكتمانها يوقعه تحت العقاب المنصوص عليه في المادة ٣١٠ من قانون العقوبات"[٥].

ثالثًا: في المملكة العربية السعودية

فقد وافق مجلس الوزراء في المملكة العربية السعودية سنة ٢٠٠٧ على نظامي مكافحة جرائم المعلوماتية والتعاملات الإلكترونية، وكان ذلك للحد من وقوع الجرائم المعلوماتية، وتحديد الجرائم المستهدفة بالنظام، والعقوبات المقدرة لكل جريمة أو مخالفة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات[٦].

ويرمي هذا القانون إلى تأمين استخدام أجهزة الكمبيوتر وشبكة المعلومات الدولية (الإنترنت) من عبث العابثين، الذي يتمثل في ارتكاب جرائم الأموال، وجرائم الآداب، وجرائم الإرهاب، وجرائم السب والقذف، وجرائم غسل الأموال.

رابعاً: في الإمارات العربية المتحدة

في الإمارات العربية المتحدة صدر القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات، حيث تنص المادة ٢ من القانون على أنَّ: "كل فعل عمدي يتوصل فيه بغير وجه حق، إلى موقع أو نظام معلوماتي، سواء بدخول الموقع أو النظام، أو بتجاوز مدخل مصرح به، يُعاقب عليه بالحبس وبالغرامة، أو بإحدى هاتين العقوبتين، فإذا ترتب على الفعل إلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو إعادة نشر بيانات أو معلومات، فيعاقب بالحبس مدة لا تقل عن ٦ أشهر، وبالغرامة أو بإحدى هاتين العقوبتين".

فيما تنص المادة ٣ من القانون السالف الذكر على أنَّ كل: "من ارتكب أيًا من الجرائم المنصوص عليها في البند ٢ من المادة ٢ من هذا القانون، أثناء أو بسبب تأدية

(ISSN: 2537 - 0758)

عمله، أو سهل ذلك للغير، يُعاقب بالحبس مدة لا تقل عن سنة، ويُغرم ما لا يقل عن ٢٠ ألف درهم، أو بإحدى هاتين العقوبتين"[٧].

ونخلص مما سبق، أنَّ نصوص التجريم المقررة في قوانين العقوبات "ماعدا مصر التي أصدرت قانون قانون حماية البيانات الشخصية المصري رقم ٢٠٢٠/١٥١" عاجزة عن مواجهة خطر جرائم الكمبيوتر، ونقصد هنا خطر الجرائم الواقعة على البيانات الشخصية، فإذا ما أضيف إلى هذا الواقع عدم وجود نصوص تجرم أفعال الاعتداء على البيانات الشخصية المخزنة في نظم المعلومات وبنوكها، أو نصوصًا تحمي البيانات من خطر المعالجة الآلية، وتكفل حماية الخصوصية- بوجه عام طبعًا وفي جميع الدول العربية- فإننا نكون أمام واقع قاتم، لن تزيل قتامته غير جهود وتدابير تشريعية حثيثة لسد النقص الحاصل، وإيجاد قواعد تحيط بهذا النمط الخطر والمستجد من أنماط الإجرام[٨]، **وبالتالي نستنتج الحقائق الآتية:**

الحقيقة الأولى: أنَّ جرائم الكمبيوتر تستهدف المعطيات ذات الطبيعة المعنوية، فعندما يكون الكمبيوتر هدفًا للجريمة، فإنَّ السلوك يستهدف المعلومات المخزنة فيه، أو المنقولة منه، أو إليه، وعندما يكون وسيلة لارتكاب الفعل، فإنَّ السلوك يستهدف بيانات تمثل قيمًا مالية، أو اعتبارًا ماليًا، ويجرى الفعل أو السلوك بتوسل طرق تقنية في بيئة معنوية، وليست في بيئة سلوكيات مادية، وعندما يكون بيئة للجريمة، فإنَّ محتوى الفعل غير المشروع هو المعلومات غير المشروعة، كما هو الحال في جرائم المحتوى المعلوماتي الضار.

الحقيقة الثانية: إنَّ مبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة إلاَّ بنص، ومتى ما انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص القائمة، امتنعت المسؤولية، وتحقق القصور في مكافحة هكذا جرائم.

الحقيقة الثالثة: إنَّ القياس في النصوص الجنائية الموضوعية محظور وغير جائز، ويكاد ينحصر في الحقل الجنائي بنصوص الإجراءات الجنائية كلما كانت أصلح للمتهم ومؤدى ذلك امتناع قياس أنماط جرائم الكمبيوتر على الجرائم التقليدية، التي تستهدف الأموال والاعتبار المالي من جهة أخرى، لا يصلح القياس على نصوص خاصة بنوع من الجرائم كقياس سرقة المعلومات أو سرقة وقت الكمبيوتر على الاستيلاء على القوى المحرزة كالكهرباء، لتخلف علة القياس، ولأنَّ هذه نصوص شرعت خصيصًا لتطال الأنماط التي تنظمها، وهي نصوص خاصة لا يتوسع في القياس عليها، بل لا نبالغ إذا قلنا إنَّ جزءًا من النصوص الخاصة بعد استثناء على أصل، والاستثناء لا يتوسع فيه.

وهناك عدد نتائج تستنبط من الواقع العربي في حماية المعلومات وتشريعات تقنية المعلومات بوجه عام (عدا تشريعات حماية المصنفات الرقمية في نطاق الملكية الفكرية):

أولاً: برغم وجود أطر قانونية تنظم بنوك المعلومات وقواعد البيانات المركزية في عدد من الدول العربية، إلاَّ أنه لا يوجد تشريع متكامل في حقل الخصوصية في أي من الدول العربية، وثمة أفكار أو مشاريع في هذا الحقل في الأردن والإمارات، وبالتالي تظل البيانات المتعلقة بالأشخاص والحياة الخاصة دونها تنظيم كان ودونها حماية كافية، رُغمَّ الحاجة المُلحة إلى ضبط استخدام ومعالجة ونقل البيانات الشخصية في البيئة الرقمية، وما تتيحه أنشطة الاعتداء على هذه البيانات من مساس جوهري بحقوق الإنسان، بل وثقة المستهلك بوسائل التقنية واستخداماتها(٩).

ثانيًا: باستثناء التعديل الذي حصل على قانون البيانات الأردني، ومشروع تعديل قانون أصول المحاكمات اللبناني، لم تشهد قوانين الإثبات العربية تعديلات في حقل حجية مستخرجات الكمبيوتر والمواد الإلكترونية في النزاعات الحقوقية والتجارية(١٠).

ثالثًا: في ميدان التجارة الإلكترونية والأعمال الإلكترونية، أقرت الأردن ودبي وتونس تشريعات عالجت موضوع التجارة الإلكترونية، وتكاد تتفق جميعا في بنائها الذي يعتمد على القانون النموذجي للتجارة الإلكترونية، الذي وضعته لجنة اليونسترال (لجنة قانون التجارة في الأمم المتحدة) عام ١٩٩٦م(١١).

ومع ذلك، وحتى في هذه الدول التي وضعت هذه التشريعات، فإنَّ النقص التشريعي لا يزال قائمًا في الحقول التي تتيح تفعيل هذه التشريعات، ووضعها موضع التطبيق، فليس ثمة لتنظيم السلطات توثيق المعاملات الإلكترونية، وليس ثمة تشريعات للمعايير الأمنية، أو المعايير القياسية لخدمات التقنية، وليس ثمة حسم لكثير من المشكلات الرئيسة في ميدان التجارة الإلكترونية، كمسائل الضرائب على الإنترنت، ومسائل الخصوصية وغيرها، ولا أبالغ إنْ قلت إنَّ سياسات الاستنساخ التشريعية، والنقل والترجمة عن القوالب الجاهزة دون مراعاة للنظام القانوني، أو تعمّق في المسالة محل التنظيم، أدى إلى ولاية تشريعات تشوبها النواقص، وتطال أحكامها المطاعن، والأهم من ذلك أنها لم تتح تحقيق الغرض الذي وضعت من أجله.

رابعًا: لم يجر إقرار أي تشريع عربي في حقول المعايير الأمنية، أو القياسية في تقنية المعلومات، أو في حقول الإجراءات الجنائية الملائمة للأفعال، التي تستهدف المعلومات وقواعدها وشبكاتها(١٢).

(ISSN: 2537 - 0758)

خامسًا: انحصر التلاقي بين النظام القانوني العربي وبين موجات تشريعات تقنية المعلومات في ميدان حماية المصنفات الرقمية، وتحديدا حماية البرامج، وقواعد البيانات، والدوائر المتكاملة عبر تشريعات حق المؤلف، أو تشريعات خاصة، كما في قوانين حماية طبوغرافيا الدوائر المتكاملة، وليس ثمة أي تشريع في الوقت الحاضر ينظم حماية عناصر الإنترنت ومواقع المعلوماتية(١٣).

القسم الثاني

إطار حماية البيانات الشخصية في التشريعات الأجنبية

أولاً- خصوصية البيانات في الولايات المتحدة الأمريكية

من الملاحظ أنَّ الولايات المتحدة الأمريكية لم تعتمد قوانين شاملة لحماية خصوصية البيانات، بل اعتمدت على القوانين القطاعية المتعلقة بكل قطاع على حدة، وذلك في بعض المناطق.

هذه الحزمة من القوانين شرعت على أساس الاستخدام العادل للبيانات الشخصية، وفي عام ١٩٧٠م قامت إدارة الصحة والتعليم بالولايات المتحدة بطرح أول هذه القوانين، معتمدة على بعض المبادئ الأساسية في حماية البيانات الشخصية، **ومنها:**

- أن يكون جمع البيانات لغرض محدد.
- البيانات الشخصية التي يتم الحصول عليها لا يجوز التصريح بها لأي فرد أو مؤسسة، إلاَّ برضا صاحب البيانات، أو بسند قانوني.
- جميع البيانات المجمعة من الأفراد يجب أنْ تكون دقيقة ومحدثة.
- لا بد من وجود آلية تمكن الأفراد من مراجعة بياناتهم الشخصية لضمان الدقة، بالإضافة إلى التمكن من الحصول على تقارير دورية.
- يجب مسح البيانات الشخصية في حالة انتهاء الغرض من تجميعها.
- يحظر نقل البيانات إلى المواقع غير الآمنة على مثلها من البيانات الشخصية.
- بعض البيانات قد تكون حساسة، حيث إنَّ الإفصاح عنها لا يكون إلاَّ في الحالات القصوى، وذلك مثل (الدين، والتوجه الجنسي)(١٤).

ثانيًا- خصوصية البيانات في أوروبا

قد نظمت أوروبا قوانين خصوصية البيانات، سواء على مستوى الاتحاد الأوروبي (أولاً)، أو كل دولة على حدة، مثل فرنسا (ثانيًا)، والمملكة المتحدة.

١ – الاتحاد الأوروبي

أما في أوروبا، فيتم تنظيم وتنفيذ حق خصوصية البيانات بشكل كبير وفعال، وتنص المادة رقم ٨ من المعاهدة الأوروبية لحقوق الإنسان على حق احترام الحياة الشخصية والعائلية للفرد ومنزله ومراسلاته، وفقًا لقيود محددة.

لقد أعطت المحكمة الأوروبية لحقوق الإنسان هذه المادة تفسيرًا متسعًا في قانونها، فوفقًا لقانون محكمة الأحوال، فإنَّ قيام المسؤولين الحكوميين بجمع المعلومات حول فرد دون الحصول على موافقته، عادةً ما تقع ضمن مجال المادة رقم ٨.

وبذلك، فإنَّ جمع المعلومات لأجل التعداد السكاني، أو تسجيل بصمات اليد والصور في سجل الشرطة، أو جمع بيانات طبية، أو تفصيلات حول المصروفات الشخصية، وتنفيذ نظام تحديد الشخصية قد أثارت الكثير من القضايا المتعلقة بخصوصية البيانات.

ولا تقبل المحكمة أي تدخل للدولة في خصوصية الأفراد، إلاَّ بتوافر ثلاثة شروط، هي:

١. إذا كان التدخل وفقًا للقانون.
٢. إذا كان التدخل يتلمس هدفًا مشروعًا.
٣. إذا كان التدخل ضروريًا في مجتمع ديمقراطي.

ولا تُعد الحكومة بالكيان الوحيد الذي قد يفرض تهديدًا على خصوصية البيانات، فالمواطنون الآخرون والشركات الخاصة تحديدًا يشتركون في أنشطة تشكل تهديدًا أكبر خاصةً مع انتشار المعالجة الإلكترونية للبيانات، ولقد تم إبرام معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية داخل المجلس الأوروبي في عام ١٩٨١، وتلزم هذه المعاهدة الموقعين عليها بسن التشريعات المتعلقة بالمعالجة الآلية للبيانات الشخصية، وهو ما قامت كثير من الدول بعمله بالفعل"[١٥].

وحيث إنَّ جميع الدول الأعضاء في الاتحاد الأوروبي من الموقعين على المعاهدة الأوروبية لحقوق الإنسان، ومعاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية، كانت المفوضية الأوروبية مهتمة بأنَّ تشريعات حماية البيانات المتباينة سوف تبرز، وتعيق التدفق الحر للبيانات داخل إقليم الاتحاد الأوروبي؛ لذلك قررت المفوضية الأوروبية التقدم باقتراح توفيق قانون حماية البيانات داخل الاتحاد الأوروبي. لقد قام البرلمان الأوروبي ووزارات الحكومات القومية بتطبيق توجيه حماية البيانات في عام ١٩٩٥، وكان لزامًا أنْ يتم نقله إلى القانون الوطني مع نهاية عام ١٩٩٨.

وهنا نبذة عن التوجيه الأوروبي بشأن حماية البيانات والذي سوف يتم: تناوله بالبحث المفصل لاحقًا.

(ISSN: 2537 - 0758)

يحتوي التوجيه على عدد من المبادئ الأساسية، والتي يتوجب على الدول الأعضاء الالتزام بها، وعلى أي شخص يقوم بمعالجة البيانات الشخصية أن يلتزم بمبادئ الممارسة الجيدة الثمانية الواجبة التنفيذ، **وتحدد هذه المبادئ إلى أنَّ البيانات يجب أنْ:**

١. يتم معالجتها بشكل عادل وقانوني.
٢. يتم معالجتها لأغراض محدودة.
٣. تكون المعالجة مناسبة، ومعنية، وغير مفرط فيها.
٤. تكون المعالجة دقيقة.
٥. لا يتم الاحتفاظ بها فترة أطول مما هو ضروري.
٦. يتم معالجتها وفقًا لحقوق صاحب البيانات.
٧. تكون مؤمنة.
٨. يتم نقلها فقط إلى الدول التي تتوافر لديها الحماية المناسبة[١٦].

وتغطي البيانات الشخصية كلاً من الحقائق والآراء الخاصة بالفرد، كما أنها تشمل أيضًا معلومات متعلقة بنوايا مراقب البيانات تجاه الفرد، برغم أنّه سوف يتم تطبيق بعض الاستثناءات الظرفية المحدودة، أما فيما يتعلق بمفهوم المعالجة، فإنَّ تعريف المعالجة أصبح أكثر اتساعًا عن ذي قبل، فعلى سبيل المثال، تتضمن المعالجة مفاهيم "الحصول" و"الاحتفاظ" و"الإفصاح".

لقد قامت جميع الدول الأعضاء في الاتحاد الأوروبي بتطبيق تشريع متسق مع هذا التوجيه، أو بتكييف قوانينها القائمة، كما أنَّ لدى كل دولة سلطتها الإشرافية الخاصة بها لمراقبة مستوى الحيطة .نتيجة لذلك، فإنَّ نقل المعلومات الشخصية– من الناحية النظرية– من الاتحاد الأوروبي إلى الولايات المتحدة يُعد محظورًا، عندما لا تتوافر سبل حماية الخصوصية المناظرة في الولايات المتحدة.

وعلى الشركات الأمريكية التي تسعى للتعامل مع بيانات الاتحاد الأوروبي أن تلتزم بإطار الملاذ الآمن، والمبادئ الرئيسة للبيانات التي يتم حمايتها، وهي محدودية عملية جمع البيانات، وموافقة الفرد، والدقة، والتكامل، والأمن وحق الفرد في مراجعة البيانات، وحذف ما يراه منها. نتيجة لذلك، فإنَّ لعملاء الهيئات الدولية مثل أمازون Amazon، و"إى باى" eBay في الاتحاد الأوروبي القدرة على مراجعة وحل المعلومات، في حين لا يتيسر هذا الأمر للأمريكيين، ففي الولايات المتحدة، نجد أنَّ الفلسفة التوجيهية المناظرة، هي قانون الاستخدام العادل للمعلومات.

اختلاف اللغة هنا له أهميته: ففي الولايات المتحدة يدور الجدال حول الخصوصية، في حين أنَّ الجدال في الاتحاد الأوروبي يدور حول حماية البيانات. يرى بعض

الفلاسفة أنَّ تحريك الجدال من الخصوصية إلى حماية البيانات، يبدو كآلية للانتقال إلى الأمام في الواقع العملي، في وقت لا يحتاج إلى اتفاق حول الأسئلة الرئيسية المتعلقة بطبيعة الخصوصية.

٢- في فرنسا

قامت فرنسا بتطبيق قانونها القائم رقم ٧٨- ١٧ الصادر في ٦ يناير ١٩٧٨، والمتعلق بتكنولوجيا المعلومات والملفات والحريات المدنية.

٣- المملكة المتحدة

في المملكة المتحدة، قام قانون حماية البيانات ١٩٩٨ (مفوض المعلومات) بتطبيق التوجيه المعني بحماية البيانات الشخصية، وهو يحل محل قانون حماية البيانات الصادر في ١٩٨٤.

أما في مقاطعات كولومبيا البريطانية وألبرتا والكويبك، فتعد هي المقاطعات الوحيدة التي تطبق قوانين معترف بأنها تتماثل تماثلاً كبيرًا مع قانون حماية المعلومات الشخصية والمستندات الإلكترونية.

وتنظم هذه القوانين قيام الشركات وغيرها من الهيئات، بجمع واستخدام والإفصاح عن المعلومات الشخصية، وتمنح الأفراد حقًا عامًا بالدخول إلى معلوماتهم الشخصية وتصحيحها، وفي الوقت ذاته، قامت كل من مقاطعات أونتاريو ونيو برزويك ونيو فاوندلأزلى ولابرادور بتطبيق تشريع لحماية معلومات الصريحة الشخصية، والذي تم إقراره بأنه من القوانين المماثلة بشكل أساسي[١٧].

هوامش ومراجع البحث:

[١] أحمد شوكت فارس العزاوي، الحماية الجنائية لسرية البيانات الشخصية "دراسة مقارنة"، ص١١٢ .

[٢] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، ص٢٠٣.

[٣] شمس الدين إبراهيم، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات، دار النهضة العربية، القاهرة، ٢٠١٥، ص٢٢١.

[٤] أحمد شوكت فارس العزاوي، الحماية الجنائية لسرية البيانات الشخصية "دراسة مقارنة"، مرجع سابق، ص١٠٧.

[٥] أحمد شوكت فارس العزاوي، الحماية الجنائية لسرية البيانات الشخصية "دراسة مقارنة"، مرجع سابق، ص١٠١.

(ISSN: 2537 - 0758)

(٦) محروس نصار غايب، الجريمة المعلوماتية، ٢٠١٠م، ص١٨، بحث منشور على الرابط:
http://www.iasj.net//iasj?funcfulltext&aId

(٧) عبد الصبور عبد القوي علي، الجريمة الإلكترونية والجهود الدولية للحد منها، كلية الحقوق– جامعة بني سويف، ٢٠١٢، ص١٠.

(٨) مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، مرجع سابق، ص ٢١٢.

(٩) يونس عرب، الخصوصية وحماية البيانات في البيئة العربية، دائرة المكتبة الوطنية، ٢٠٠٢، ص٢.

(١٠) ويمكن القول إنَّ الاتجاه التشريعي منذ عام ١٩٩٧ في الأردن يتجه إلى الاعتراف بقيمة القيود الإلكترونية في مختلف قطاعات النشاط، كما هو الحال في الاعتراف بها لإثبات ملكية الأسهم في أسواق التداول المالي، والاعتراف بها لإثبات التصرفات والمراكز القانونية بالنسبة لتسجيل مصنفات الملكية الصناعية لدى دوائر وزارة الصناعة والتجارة وغيرها.

(١١) رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة، ١٩٩٩م، ص١٨.

(١٢) يونس عرب، التدابير التشريعية الحربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي النادي العربي للمعلومات، دمشق، ص ٤.

(١٣) علي عبد الله القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، جامعة الإمارات، ٢٠٠٨.

(١٤) **مشار إليه:** أحمد شوكت فارس العزاوي، الحماية الجنائية لسرية البيانات الشخصية " دراسة مقارنة"، ص١١٩.

(١٥) عبد المنعم أحمد سلطان، التقنيات المعلوماتية وأثرها على حماية الحياة الخاصة، جامعة بنها، ٢٠١١، ص١٨٢.

(١٦) **مشار إليه:** مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، مرجع سابق، ص ٢٣٦.

(١٧) مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، مرجع سابق، ص ٢٢١.