هيئة تنظيم الاتصالات

سلطنة عمان

مشروع البيانات الضخمة (Big Data)

ورقة عمل

حول تنظيم البيانات الشخصية / الالكترونية وفق قوانين الاتحاد الأوروبي واستراليا

المهندس/ ابراهيم المعولي

هيئة تنظيم الاتصالات - سلطنة عمان

يناير ٢٠١٥

المحتـــــويات

سلطان

سلطان

المقدمة

البيانات الضخمة (Big Data) ليس فقط موضوعا ساخنا لتكنولوجيا المعلومات والصحفيين التجاريين في جميع أنحاء العالم، انها بداية لتحول الشركات كذلك. يمكن لتكنولوجيات البيانات الضخمة الجديدة تحليل بيانات المجسات/أجهزة الاستشعار ، وموقع الانترنت، وبيانات شبكات التواصل الاجتماعي السلوكية منها والاجتماعية، مما يوفر لصانع القرار أدوات مبتكرة لفهم أفضل للعملاء والأسواق، وإدارة المخاطر على نحو فعال. يجدر القول في مسار ثورة البيانات الضخمة ، بأن البيانات سوف تصبح عاملا رئيسيا للإنتاج ـ ربما أكثر أهمية من الأرض والعمل ورأس المال ـفي المقابل، فإن هذه المعلومات سوف تدفع تحول العمليات والنماذج التجارية ،نحو تحقيق مستويات أعلى من الجودة والكفاءة والفعالية.

ولكن في المقابل،تنطوي على العديد من المخاطر خاصة بالنسبة للمستخدم البسيط وخصوصا فيما يتعلق بحريته الشخصية، حيث أن البيانات الضخمة ربما تعزز سطوة المؤسسات الكبرى على تفاصيل الحياة الشخصية مما يؤدي الى تقويض الحريات الفردية وبالتالي الأنظمة الاجتماعية. لذلك، يجب تعزيز الوعي لدى المستخدمين بمخاطر هذه التكنولوجيات بحيث يتم استخدامها بحذر، كما يجب العمل على تعزيز البيئة القانونية والتنظيمية التي من شأنها حماية المصالح الشخصية.

تنظيم البيانات الشخصية / الالكترونية وفق قوانين الاتحاد الأوروبي واستراليا

أولا: الاتحاد الأوروبي

في عام ١٩٩٥، سنّ الاتحاد الأوروبي تشريعًا للخصوصية وهو توجيه الاتحاد الأوروبي عرّف «البيانات الشخصية» على أنها أي معلومات من شأنها أن تحدد هوية الشخص، سواء بطريقة مباشرة أو غير مباشرة. ومن الواضح أن المشرّعين كانوا يفكرون في أشياء مثل وثائق تحتوي على رقم هوية، وأرادوا أن تتمتع هذه الوثائق بالحماية وكأنها تحمل اسمك.

واليوم، يشمل هذا التعريف معلومات أكثر بكثير من تلك التي يمكن أن يكون المشرعون الأوروبيون قد تخيلوها، أكثر من جميع البتات والبايتات التي كانت موجودة في العالم بأسره عندما صاغوا قانونهم منذ عشرون عامًا.

فالمعلومات التي نظرنا إليها على أنها بيانات شخصية في الماضي — مثل اسمنا، أو عناويننا، أو تسجيلات استخدام كروت الائتمان الخاصة بنا — يشتريها بالفعل ويبيعها متعهدو البيانات مثل شركة أكسيوم، تلك الشركة التي تملك في المتوسط ١٥٠٠ معلومة عما يزيد عن ٥٠٠ مليون عميل، وهي البيانات التي يضعها الأفراد في المجال العام في شكل استبيان أو عندما يسجلون الدخول على بعض الخدمات.

ومن هنا سنستعرض بعض أحكام هذا التوجيه، حيث يهدف هذا التوجيه الى حماية الحقوق والحريات الأساسية للأشخاص، وعلى وجه الخصوص الحق في الخصوصية، فيما يتعلق بمعالجة البيانات الشخصية.

علما بأن هناك بعض المصطلحات التي يجب تعريفها وتوضيحها لكي يتسنى للقارىء فهم تلك الأحكام بصورة سلسة. ومن هذه المصطلحات المعرفة في هذا التوجيه:

١) "معالجة البيانات الشخصية" يعني أي عملية أو مجموعة من العمليات التي تتم على البيانات الشخصية،سواء كان ذلك تلقائيا أو غير تلقائي، مثل جمع وتسجيل وتنظيم وتخزين وتعديل، استرجاع أو الاستشارة، واستخدام، والكشف عن طريق

النقل أو النشر أو غير ذلك مما يجعلها متاحة، أو مجموعة، أو محظورة، أو ممسوحة أو مدمرة

٢) "نظام الايداع البيانات الشخصية" ("نظام الايداع") يعني أي مجموعة منظمة من البيانات الشخصية التي يمكن الوصول إليها وفقا لمعايير محددة، سواء كانت مركزية واللامركزية أو مبعثرة على أساس جغرافية البيانات أو الدور التي تقوم بها.

٣) "المتحكم" تعني الشخص الطبيعي أو الاعتباري أو الهيئة العامة أو الوكالة أو أي هيئة أخرى التي تحدد الأغراض ووسائل معالجة البيانات الشخصية سواءا ذلك بمفردها أو مجتمعة، حيث يتم تحديد الأغراض ووسائل المعالجة من قبل القوانين الوطنية أو اللوائح التنظيمية، حيث يتم تسمية المتحكم أو تحديد معايير معينة للتسمية وفق القانون الوطني أو اللوائح التنظيمية.

٤) "المعالج" تعني الشخص الطبيعي أو الاعتباري أو الهيئة العامة أو الوكالة أو أي هيئة أخرى التي تعالج البيانات الشخصية نيابة عن المتحكم.

٥) "طرف ثالث" تعني أي شخص طبيعي أو اعتباري، سلطة عامة أو وكالة أو أي هيئة أخرى بحيث لا تكون المتحكم، أوالمعالج أوالأشخاص الذين كانوا تحت السلطة المباشرة للمتحكم أو المعالج، والذي يحق له معالجة البيانات.

١) الخصوصية

يهدف هذا التوجيه في المقام الأول الى حماية الخصوصية في معالجة البيانات، ويظهر ذلك واضحا في المادة الاولى من التوجيه ، والتي تشير لى الهدف الاساسي من التوجيه .

١- وفقا لهذا التوجيه، يجب على الدول الأعضاء حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين، وعلى وجه الخصوص الحق في الخصوصية، فيما يتعلق بمعالجة البيانات الشخصية.

كما تنص المادة السابعة الى أن الموافقة السابقة لجمع ومعالجة البيانات الزامية حيث أنه :

٢- يجب على الدول الأعضاء أن تقدم تلك البيانات الشخصية فقط إذا:

- قد قدم موضوع البيانات بموجب موافقة صريحة لا لبس فيها.

كما أشارت حيثيات التوجيه الى:

٣- يجب أن يتم تصميم أنظمة معالجة البيانات لخدمة الإنسان، مهما كانت الجنسية أومحل إقامة الأشخاص، كما يجب احترام الحقوق والحريات الأساسية، ولا سيما الحق في الخصوصية،والذي يؤدي الى التقدم الاقتصادي والاجتماعي، وتوسيع التجارة ورفاه الأفراد.

كما أكدت حيثيات التوجيه رقم ٣٣ على:

٤- يجب أن لا تتم معالجة أية بيانات من الممكن أن تتعدى على الحريات أو الخصوصية إلا اذا أعطى صاحب البيانات الموافقة الصريحة لذلك. ومن الممكن الاستثناء بشرط أن يتم النصعلى ذلك بصراحة كمعالجة البيانات المتعلقة بالصحةمن قبل الأشخاص الخاضعين لالتزام قانون السريةالمهنية أو الأنشطة المشروعة من قبل بعض الجمعيات والمؤسسات الداعية لممارسة الحريات.

أما بالنسبة للبيانات الحساسة فقد نصت حيثيات التوجيه رقم ٣٤ على:

٥- يجب أن لدى الدول الأعضاء الترخيص الملائم لمعالجة البيانات الحساسة، على أن يتكون أسباب تلك المعالجة للمصلحة العامة كمجال الصحة العامة والحماية الاجتماعية، على أن يتعين عليها توفير ضمانات محددة ومناسبة لحماية الحقوق الأساسية والخصوصية.

٢)أمن المعلومات

تفيد مواد التوجيه أنه يجب أن تبقى البيانات الشخصية التي تم جمعها آمنة ومأمونة من الإساءة المحتملة، أوالسرقة، أو الفقدان. ومن هنا سنستعرض على بعض تلك المواد:

١- المادة السادسة من التوجيه تنص على:

يجب على الدول الأعضاء الالتزام بأن البيانات الشخصية يجب أن تكون:

- تحظى بمعالجة عادلة وقانونية
- أن تتم المعالجة حسب الغرض من جمع تلك البيانات، إن تكون تلك الأغراض واضحة. ولكن لا يعتبر مزيد من المعالجة للبيانات لأغراض تاريخية أو إحصائية أو علمية تتعارض مع ذلك شريطة تقديم الضمانات اللازمة والمناسبة من قبل الدول الأعضاء
- أن تكون تلك البيانات كافية وذات صلة وليست مفرطة أو منحرفة من الغرض من جمعها.
- أن تكون دقيقة، وعند الضرورة يجب تجديدهاحتى تبقى صالحة. كما يجب اتخاذ كل الخطوات المعقولة لضمان أن البيانات الغير دقيقة أو ناقصة يتم شطبها أو تصحيحها، مع إيلاء الاعتبار للأغراض التي تم جمعها أو التي يتم معالجتها.
- الاحتفاظ بها في الشكل الذي يسمح بتحديد مواضيع بيانات لمدة لا تزيد عن المدة التي جمعت للأغراض التي تم جمعها أو التي يتم معالجتها. يتعين على الدول الأعضاء وضع الضمانات المناسبة للبيانات الشخصية المخزنة لفترات أطول بغرض الاستخدام التاريخي،او الإحصائي أو العلمي.
- يجب على المتحكم الامتثال لما ورد أعلاه.

٢- الجزء الثاني من المادة ١٣ من التوجيه نصت على:

مع مراعاة الضمانات القانونية الكافية، ولا سيما أن البيانات لا تستخدم لاتخاذ تدابير أو قرارات فيما يتعلق بشخص معين، يجوز للدول الأعضاء - وفي حالةعدم وجود خطر من اختراق خصوصية موضوع البيانات- تقييد عن طريق تدبير تشريعي الحقوق المنصوص عليها في المادة ١٢ (الحق في النفاذ للبيانات)عند معالجة البيانات فقط لأغراض البحث العلمي أو الاحتفاظ بها لفترة التي لا تتجاوز الفترة اللازمة لغرض الإحصاءات.

٣- المادة ١٧ تنص على:

- على الدول الأعضاء أن تشترط على المتحكم تنفيذ التدابير الفنية والتنظيمية المناسبة لحماية البيانات الشخصية من التدمير المتعمد أو غير القانوني أو فقدانها وتعديلها أوالكشف غير المصرح به أو النفاذ اليها، وبخاصة ما ينطوي على معالجة ونقل البيانات عبر الشبكة، وضد الأشكال الاخرى غير المشروعة في المعالجة.

وبالنظر إلى تكلفة تنفيذ تلك التدابير، فإن هذه التدابي تعتبر ضمان مناسب لمستوى الأمن من المخاطر التي تمثلها معالجة تلك البيانات وطبيعتها التي يتحتم حمايتها.

- يجب على الدول الأعضاء أن تشترط على المتحكم اختيار المعالج الذي يوفر ضمانات كافية فيما يتعلق بالتدابير الأمنية التقنية والتدابير التنظيمية التي تحكم معالجة تلك البيانات وضمان الامتثال لتلك التدابير.
- إجراء المعالجة عن طريق معالج معين يجب أن يحكمها عقد قانوني ملزم للمعالج من قبل المتحكم وتنص على وجه الخصوص ما يلي:
  - يقوم المعالج بالامتثال الى تعليمات المتحكم.
  - الالتزامات المنصوص عليها أعلاه، وعلى النحو الذي حدده قانون الدولة العضو يجب أن يكون أيضا ملزم على عاتق المعالج.
- بهدف حفظ الإثبات، يتعين أن يكون العقد أو المتطلبات المتعلقة بالتدابير المشار إليها أعلاه أن تكون مكتوبة.

٤ـ المادة ١٦ من التوجيه أشارت الى:

أي شخص يعمل تحت سلطة المتحكم أو المعالج، الذي لديه حق النفاذ إلى البيانات الشخصية يجب عدم معالجة تلك البيانات إلا بناء على تعليمات من المتحكم، ما لم يطلب منه القيام بذلك بموجب القانون.

٥ـ حيثيات التوجيه رقم ٢٥ ذكرت:

يجب أن تنعكس مبادىء الحماية، في الالتزامات المفروضة على الأشخاص أو السلطات العامة والمؤسسات والوكالات والهيئات الأخرى المسؤولة عن المعالجة، ولا سيما فيما يتعلق

بجودة البيانات، والأمن التقني، وإخطار السلطة الإشرافية، و ظروف معالجة البيانات، ومن ناحية أخرى، في الحقوق الممنوحة للأفراد، ومعرفة موضوع المعالجة، ليكون على علم بأن المعالجة تجري، للتشاور في البيانات،أو لطلب التصحيحات وربما للاعتراض على معالجة تلك البيانات في ظروف معينة.

٣)ملكية البيانات

لم يتم ذكر ملكية البيانات بشكل صريح، ولكن يمكن استنتاج ذلك من بعض المواد. حيث ذكر أن جمع ومعالجة البيانات لا يتم إلا بموافقة صريحة من صاحبها حسب ما تم توضيح ذلك أعلاه في جزئية الخصوصية.

٤)تصنيف البيانات

لم يشر التوجيه الى تصنيف البيانات ولكن تم توضيح بأن البيانات المعنية بالسلامة العامة أو أمن الدولة أو الدفاع أو اقتصاد الدولة لا يشمله التوجيه، حيث نصت المادة ١٣ من التوجيه أن من ضمن الاعفاءات والاستثناءات من هذا التوجيه:

- الأمن الوطني
- الدفاع
- الأمن العام
- التحقيق والكشف والملاحقة القضائية للجرائم الجنائية، أو المخالفات الأخلاقية للمهن المنظمة.
- مصلحة اقتصادية أو مالية هامة لدولة عضو في الاتحاد الأوروبي، بما في ذلك المسائل النقدية والميزانية والضرائب.
- حماية موضوع البيانات أو حقوق الآخرين وحرياتهم.

كما أشارت المادة الثامنة من التوجيه بأنا يحظر على الدول الأعضاء عند معالجة البيانات الشخصية ، الكشف عن الأصل العرقي أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو

الانتماء النقابي أو معالجة البيانات المتعلقة بالحياة الصحية أو الجنسية. ولكن تم الاستثناء من هذا الحظر في الحالات التالية:

- هناك موافقة صريحة على معالجة تلك البيانات، إلا إذا كانت قوانين الدولة العضو تحظر ذلك حتى في حالة وجود الموافقة الصريحة لذلك.
- المعالجة ضرورية لأغراض تنفيذ الالتزامات في مجال قانون العمل بقدر ما يسمح ذلك القانون الوطني على أن تتوفر الضمانات الكافية.
- المعالجة ضرورية لحماية المصالح للموضوع أوبيانات شخص ما غير قادر على أعطاء الموافقة الصريحة قانونيا.
- معالجة في سياق الأنشطة المشروعة مع الضمانات المناسبة من قبل مؤسسة أو جمعية أو هيئة غير ربحية، وذلك بهدف سياسي أو فلسفي أو ديني أو نقابي بشرط أن المعالجة تتعلق ببيانات شخص ما في تلك المؤسسة أو لاشخاص لديهم اتصال منتظم معها وبحيث لا يتم الإفصاح عن تلك البيانات لطرف ثالث دون الموافقة الصريحة.
- كما لا يسري الحظر على معالجة البيانات لأغراض الطب الوقائي والتشخيص الطبي، وتوفير الرعاية أو العلاج أو إدارة خدمات الرعاية الصحية، حيث تتم معالجة تلك البيانات عن طريق موضوع الصحة المهنية بموجب القانون أو القواعد التي وضعتها الهيئات الوطنية المختصة بالالتزام بالسرية المهنية أو عن طريق شخص آخر يخضع إلى التزام مماثل من السرية.

كما يمكن القيام بمعالجة البيانات المتعلقة بالجرائم، وإدانات جنائية أو إجراءات أمنية ، فقط تحت سيطرة السلطة الرسمية، أو إذا قدمت ضمانات محددة مناسبة بموجب القانون الوطني. ولكن، وجب الاحتفاظ بسجل كامل للإدانات جنائية فقط تحت سيطرة السلطة الرسمية.

كما يمكن معالجة البيانات المتعلقة بالجزاءات الإدارية أو الأحكام في القضايا المدنية على أن تكون المعالجة تحت سيطرة السلطة الرسمية.

٥)المسؤولية والمساءلة

جاءت عدة مواد في التوجيه تتعلق بالمسؤولية والمساءلة ومن ضمنها:

- المادة ١٨ بخصوص الالتزام بإخطار السلطة الاشرافية:

يجب على الدول الأعضاء إلزام المتحكم أو من ينوب عنه، بإخطارالسلطة الإشرافية قبل القيام بأي عملية من عمليات المعالجة سواءا معالجة كلية أو جزئيةسواء كانت تلك المعالجة تهدف لخدمة هدف واحد أو عدة أهداف ذات صلة. ويجوز للدول الأعضاءوفقا للقانون الوطني الأعفاء من اخطار السلطة الأشرافية في حالات معينة بشرط ضمان حقوق وحريات معالجة تلك البيانات.

- المادة ١٩ نصت على أن إخطار السلطة الاشرافية يجب أن يشمل:
  - اسم وعنوان المتحكم أو من يمثله
  - الغرض أو الأغراض من المعالجة؛
  - وصفا للفئة أو فئات موضوع البيانات
  - المستلمين أو الفئات المستفيدة التي قد يتم الكشف عنها في البيانات؛
  - اقترح نقل البيانات إلى بلدان ثالثة.
  - وصفا عاما يسمح بتقييم أولي للتدابير المتخذة لضمان أمن معالجة البيانات

المادة ٢٠ من التوجيه نصت على المراجعة لمسبقة من قبل السلطة الأشرافية وقد جاء نص المادة كالتالي:

- تحدد الدول الأعضاء عمليات المعالجة التي يمكن أن تشكل مخاطر على حقوق وحريات معالجة البيانات على أن تتم المراجعة المسبقة لتلك العمليات.
- تقوم السلطة الأشرافية بتلك المراجعة المسبقة للعمليات فور استلامها لاشعار المتحكم .

المادة٢٢ من التوجيه تشير الى:

- مع عدم الإخلال بالعلاج الأداري، يجوز الحكم على عدة أمورمن قبل السلطوة الأشرافية قبل إحالته الى السلطة القضائية، كما يجب على الدول الأعضاء أن تتقدم للحصول على حق كل شخص في الانتصاف القضائي عن أي خرق من الحقوق المكفولة له بموجب القانون الوطني.

المادة ٢٣ من التوجيه حدد المسؤولية في حالة الفشل في الالتزام بحقوق وحريات معالجة البيانات، حيث أشارت المادة على:

- يحق لأي شخص تعرض لأضرار نتيجة عملية المعالجة الغير قانونية أو تتعارض مع أحكام القوانين الوطنية المعتمدة وفقا لهذا التوجيه، أن يحصل على تعويض من المتحكم حسب الأضرار التي لحقت بهم. كما يجوز أعفاء المتحكم جزئيا أو كليا في حالة تم إثبات أن المتحكم ليست مسؤولية عن هذا الحدث الذي أدى الى ذلك الضرر.

المادة ٢٤ حددت وجوب العقوبات في حالة الاخلال باحكام هذا التوجيه حيث نصت المادة على:

- يجب على الدول الأعضاء اتخاذ التدابير المناسبة لضمان التنفيذ الكامل لأحكام هذا التوجيه ، وعليها وضع العقوبات التي ستفرض في حالة التعدي وفقا لهذا التوجيه.

٦)تنظيم النفاذ إلى البيانات

المادة العاشرة من التوجيه أظهرت الحق في النفاذ للبيانات وتصحيحها حيث نصت المادة:الحق في الوصول والحق في تصحيح البيانات المتعلقة به مادامت تحتاج مزيد من المعلومات الضرورية، مع مراعاة الظروف الخاصة التي يتم فيها جمع البيانات، لضمان معالجة عادلة فيما يتعلق بموضوع البيانات.

كما شرحت المادة ١٢ من التوجيه حق النفاذ للبيانات كالتالي:

يجب على الدول الأعضاء ضمان إخضاع كل البيانات للحق في الحصول من المتحكم:

- دون أية قيود ودون تأخير أو أعباء مالية زائدة:
  - تأكيد ما إذا كانت البيانات المتعلقة به يجري معالجتها وبحسب الغرض من معالجتها، وفئة البيانات، والمستفيدين أو فئات المتلقين الذين يتم الإفصاح عن البيانات
  - التواصل بخصوص عملية معالجة تلك البيانات وإبلاغه بأية معلومات متاحة لمصدرها.
  - معرفة المنطق من خضوع البيانات لمعالجة تلقائية وإخطاره بذلك.
- حسب الاقتضاء، يمكن تصحيح، أو محو أو حجب البيانات التي لا تتوافق مع أحكام هذا التوجيه، ولا سيما بسبب عدم إكتمالية أو دقة البيانات.
- إخطار لأطراف ثالثة الذين تم الكشف عن البيانات لهم عم أي تصحيح، محوللبيانات وبحسب الجزئية أعلاه.

كما أوضحت المادة ١٦ من التوجيه الى أن:

أي شخص يعمل تحت سلطة المتحكم أو المعالج، الذي لديه حق النفاذ إلى البيانات الشخصية يجب عدم معالجة تلك البيانات إلا بناء على تعليمات من المتحكم، ما لم يطلب منه القيام بذلك بموجب القانون.

:ما أعطى التوجيه الحق للسلطة الأشرافية الحق في النفاذ للبيانات حسب المادة ٢٨ من التوجيه: "تتعاون السلطة الاشرافية علي وجه الخصوص مع:

- سلطات التحقيق، في موضوع صلاحيات النفاذ إلى البيانات وصلاحيات معرفة تفاصيل المعالجة وذلك من أجل أداء واجباتها الرقابية.
- القوى الفعالة للتدخل، وعلى سبيل المثال، تقديم الآراء قبل إجراء عمليات المعالجة، وضمان نشر المناسب لهذه الآراء، من حظر، أو محو أو تدمير البيانات، أوفرض حظر مؤقت أو نهائي بشأن المعالجة، أوإنذارالمتحكم، أو أن إحالة المسألة إلى البرلمانات الوطنية أو المؤسسات السياسية الأخرى.

٧)وجودها خارج السلطنة

على الدول الأعضاء عدم تقييد أو منع انسيابية البيانات عبر الحدود على شرط الالتزام بحماية الحقوق والحريات وبخاصة حق الخصوصية فيما يتعلق بمعالجة البيانات.

ومن هنا يمكن تلخيص المباديء السبعة التي تأسس بها هذا التوجيه الأوروبي::

١) لاحظ: المواد التي يتم جمع البيانات عنها ينبغي الاشعارعن ذلك الجمع

٢) الغرض: البيانات يجب ان تستخدم فقط للغرض المعلن عنه وليس لأغراض أخرى

٣) الموافقة: لا ينبغي الإفصاح عن البيانات الشخصية أو مشاركة أطراف أخرى بدون موافقة مسبقة.

٤) أمن المعلومات: يجب أن تبقى البيانات الشخصية التي تم جمعها آمنة ومأمونة من الإساءة المحتملة، أوالسرقة، أو الفقدان.

٥) الكشف: يجب أن تكون البيانات الشخصية التي يتم جمعها معروفة للجهات الجامعة لتلك البيانات

٦) النفاذ للبيانات: يجب السماح بالوصول الى البيانات الشخصية والسماح لاصحابها بتصحيح أية أخطاء.

٧) المساءلة: يجب على جامعي البيانات الشخصية التمسك بكل المباديء السابقة ، والاخلال بذلك يعرضهم للمسائلة.

بالاضافة الى العولمة،فأن التقدم التكنولوجي يؤثر بشكل كبير على طريقة جمع ومعالجة النفاذ الى البيانات. علاوة على ذلك، يتم تنظيم الإطار القانوني الأوروبي لحماية البيانات الحالية من قبل هذا التوجيه، مما يؤدي إلى تفسيرات متباينة من قبل القوانين المحلية للدولة العضو في الاتحاد الأوروبي وكذلك تنفيذ تلك الأحكام المنصوص عليها.

وقد أدت التطورات التقنية والتباين في التطبيقبين أعضاء الاتحاد الأوروبي الى إعادة النظر في إطار حماية البيانات الحالية في أوروبا. وقد اتخذت خطوة أولى نحو وضع إطار قانوني جديد عندما قدمت المفوضية الأوروبية مشروع اقتراحها لائحة حماية البيانات الجديدة في ٢٥ يناير ٢٠١٢

ومن أهم التغييرات المقترحةعلى التوجيه ما يلي:

١) يجب أن تكون هناك قواعد موحدة تسري بشكل مباشرعلى جميع أعضاء الاتحاد
٢) زيادة المسؤولية والمساءلة عن معالجة تلك البيانات الشخصية ، وعلى سبيل المثال، يجب أن تخطر الشركات والمؤسسات السلطة الرقابية الوطنية من اختراق البيانات الخطيرة في أقرب وقت ممكن (إذا كان ذلك ممكنا في غضون ٢٤ ساعة).

٣) يجب أ تتعامل المنظمات مع السلطة الوطنية الموحدة لحماية البيانات في دول الاتحاد الأوروبي. وبالمثل، فأنه يمكن للناس الرجوع إلى تلك السلطة في بلادهم، حتى عندما تتم معالجة البيانات من قبل شركة مقرها خارج الاتحاد الأوروبي.

٤) يجب أن تعطى الموافقة بشكل صريح لمعالجة البيانات، وليس على شكل فرضيات.

٥) من حق المستخدمين الوصول الى بياناتهم الخاصة ونقل تلك البيانات من مزود خدمة الى اخرى بشكل سلس، وهذا من شأنه تحسين وزيادة المنافسة بين الخدمات.

٦) من حق الناس إدارة المخاطر لحماية بياناتهم الشخصية على الانترنت حيث يمكن لهم إدخال طرف ثالث لحذف البيانات الخاصة بهم إذا لم تكن هناك أسباب مشروعة للابقاء عليها.

٧) يجب أن تطبق قواعد الاتحاد الاوروبي في حالة تم التعامل في البيانات الشخصية خارج حدود الاتحاد من قبل الشركات النشطة في الاتحاد والتي تقدم خدماتها لمواطني الاتحاد الاوروبي.

٨) سيتم تعزيز سلطات حماية البيانات الوطنية المستقلة بحيث تكون قادرة على فرض قواعد الاتحاد الأوروبي في نطاق اختصاصاتها. كما ستكون مخولة لفرض الغرامات للشركات التي تنتهك قواعد حماية البيانات في الاتحاد الأوروبي.

٩) عدم الامتثال لقواعد الاتحاد الاوروبي يمكن أن يؤدي إلى عقوبات أشد (مقارنة مع الإطار الحالي)، مثل غرامات تصل إلى ٢٪ من قيمة التداول السنوي للمؤسسة في جميع أنحاء العالم ، وهذا يتوقف على الالتزام الذي أخل به.

ثانيا: استراليا

أصبح موضوع البيانات الضخمة هو الشغل الشاغل للشركات من حيث كيفية جمعها وربطها ببعضها ودمجها والاستفادة منها ،وأصبحت الحكومات تتسابق مع الشركات لوضع ضوابط لهذه العمليات من حيث الخصوصية والاجراءات المسموح فيها وغيرها. استراليا هي واحدة من الدول التي تبحث عن طريقة للاستفادة من البيانات الضخمة الناتجة عن نشاطات الحكومة الالكترونية والشركات ووضع الضوابط اللازمة لها.

ولكن بخلاف قانون الخصوصية وقانون الرسائل الاقتحامية عبر الشبكة العنكبوتية (Spam)، لا ينظم القانون الأسترالي البيانات الضخمة، حيث ينظم قانون الخصوصية جمع واستخدام والإفصاح عن المعلومات أوالأراء حول شخص محدد أو فرد ممكن تحديده على نحو معقول (المعلومات الشخصية) من خلال فرض الإخطار الإجباري والتقيد ببعض الالتزامات الواجب اتباعها. وبالإضافة إلى ذلك، فإن قانون SPAM يحظر ارسال الاتصالات التسويقية الإلكترونية بدون "التقيد بـــ" موافقة المستلم السابقة.

وقد تم أصدار قانون الخصوصية في ١٩٨٨ وتم تعديله مؤخرا في ٢٠١٢ وبدأ العمل به في مارس ٢٠١٤، ويهدف الى تعزيز حماية الخصوصية، وهو القانون الأسترالي الذي ينظم التعامل مع المعلومات الشخصية عن الأفراد. هذا ويشمل القانون ١٣ مبدأ من مبادئ الاسترالية المتعلقة بجمع واستخدام وتخزين والكشف عن المعلومات الشخصية، والنفاذ وتصحيح البيانات.

وقبل البدأ في تحليل تلك القوانين ، ربما وجب التويه على بعض المصطلحات التي ذكرت في تلك القوانين وهي:

- المنظمة:مؤسسات القطاع الخاص وتشمل الأفراد، الشركات، الشراكة، الجمعيات.
- الوكالة: مؤسسات القطاع العام
- البيانات الشخصية الحساسة: المعلومات والآراء عن الأصول العرقية، الآراء السياسية، عضويات الجمعيات السياسية، المعتقدات الدينية أو انتماءاتهم، المعتقدات الفلسفية، عضوية الجمعيات المهنية والتجارية، العضوية النقابية، الممارسات الجنسية،السجل الاجرامي، المعلومات الصحية عن الفرد، المعلومات الوراثية عن الفرد،المعلومات البيومترية التي يتم استخدامها للتعرف على بيانات الهوية الآلي.

ومن هنا يمكن تحليل هذه القوانين حسب الآتي:

١)الخصوصية

مبدأ الخصوصية الثاني من قانون الخصوصية أعطى خيارا للافراد بالكشف عن هوياتهم أو استخدام اسماء مستعارة حيث نص المبدأ على:

- يجب أن يكون للأفراد خيار عدم الكشف عن هوياتهم، أواستخدام اسم مستعار، عند التعامل مع المؤسسة فيما يتعلق بمسألة معينة.

لا ينطبق ما ورد أعلاه في حالة:

- اذا كلفت المؤسسة بموجب القانون الأسترالي، أو أمر من المحكمة، بالتعامل مع الأفراد الذين كشفوا عن هوياتهم أو
- غير عملي للمؤسسة بأن تتعامل مع الأفراد الذين لم يكشفوا هويتهم أو الذين استخدموا اسم مستعار.

بينما المبدأ الثالث من القانون أوضح وسائل جمع البيانات حيث نص على:

- يجب جمع البيانات الشخصية عن طيق الوسائل المشروعة والعادلة.
- يجب جمع البيانات الشخصية من الأفراد أنفسهم إلا اذا:
  - اذا كان جامع البيانات وكالة فيمكن الحصول على الموافقة من شخص آخر أو بأذن حسب القانون الاسترالي أو إذن من المحكمة.
  - تعذر القيام بذلك.

لم تقتصر أحكام قانون الخصوصية على البيانات المطلوبة فقط، بل تعدى إلى توضيح الخطوات الواجب اتباعها بالنسبة للمعلومات الغير مرغوب بها من خلال مبدأ الخصوصية الرابع والذي نص على:

- اذا تلقت المؤسسة معلومات شخصية لم تكن ترغب بها، فعليها – في غضون فترة معقولة- تحديد اذا قامت المؤسسة بجمع المعلومات حسب مبدأ الخصوصية الثالث في حالة رغبت المؤسسة في تلك المعلومات.
- ويمكن للمؤسسة استخدام أو الكشف عن المعلومات الشخصية بغرض اتخاد القرار في حالة أن المؤسسة لم تقم بجمع المعلومات ولم يتم تضمين تلك المعلومات في سجلات المؤسسين، وعليها في أقرب وقت إتلاف تلك المعلومات بطريقة معقولة ومشروعة.
- أما في حالة قامت المؤسسة بجمع تلك المعلومات، فعليها تطبيق مباديء الخصوصية بالقانون.

المبدأ السادس من القانون استعرض أحكام استخدام والكشف عن المعلومات الشخصية من خلال النصوص التالية:

- اذا قامت المؤسسة بالاحتفاظ بالمعلومات الشخصية بغرض معين (الهدف الأساسي) ، يجب عدم استخدام أو الكشف عن تلك المعلومات بغرض آخر (الهدف الثانوي) إلا اذا:
  - الموافقة المسبقة من الفرد للاستخدام أو الكشف والافصاح عن المعلومات
  - أن يتوقع الفرد من المؤسسة الكشف عن المعلومات لغرض ثانوي بحيث يكون الغرض الثانوي:
    - إذا كانت المعلومة حساسة أن ترتبط أرتباطا مباشرا بالغرض الاساسي
    - إذا كانت المعلومة غير حساسة أن تتعلق بالغرض الأساسي
  - يتطلب إذن حسب القانون الاسترالي أو أمر من المحكمة
  - وجود حالة عامة مسموح لها الكشف عن المعلومات
  - المؤسسة عبارة عن منظمة مسموح لها الكشف عن المعلومة
- يمكن لمؤسسة معينة استخدام المعلومات المجموعة من مؤسسة اخرى ذات صلة بالمؤسسة الاولى اذا توافقا في الغرض الاساسي من جمع البيانات.

أما قانون الرسائل الاقتحامية عبر الشبكة العنكبوتية (Spam) فقد أوضح التالي فيما يخص التسويق الالكتروني:

يجب عدم إرسال أية رسالة الكترونية تجارية بدون التقيد بموافقة مسبقة من قبل المستلم، ويجب أن تحتوي كل رسالة على خاصية إلغاء الاشتراك ليتمكن المستلم من رفض تلقي تلك الرسائل في المستقبل. والفشل في الامتثال للقانون يؤدي الى عواقب مكلفة مع مضاعفة العقوبة عند التكرار.

٢)أمن المعلومات

وردت أحكام تتعلق بأمن المعلومات الشخصية في قانون الخصوصية ، حيث نص مبدأ الخصوصية ١١ على التالي:

- على المؤسسة التي تحتفظ بمعلومات شخصية، أن تتخذ بعض الخطوات المعقولة لحماية المعلومات من:
  - سوء الاستخدام والتدخل
  - النفاذ الغير المصرح به أو التعديل أو الكشف
- أن تتخذ المؤسسة بعض الخطوات المعقولة في سبيل إتلاف المعلومات أو أن لا يتم التعرف على تلك المعلومات أن لا يتم التعرف على تلك المعلومات إذا:

- احتفظت المؤسسة بمعلومات شخصية عن الفرد و
- المؤسسة لم تعد تحتاج لتلك المعلومات لأي غرض من الأغراض
- لم يتم تضمين المعلومات في السجلات
- لم يطلب من المؤسسة الاحتفاظ بالمعلومات بموجب القانون الاسترالي أو أمر من المحكمة

٣)ملكية البيانات

لم يتم ذكر ملكية البيانات بشكل صريح، ولكن يمكن استنتاج ذلك من بعض المواد. حيث ذكر أن جمع ومعالجة البيانات لا يتم إلا بموافقة صريحة من صاحبها حسب ما تم توضيح ذلك أعلاه في نصوص عدة.

٤)تصنيف البيانات

صنف قانون الخصوصية الاسترالي البيانات الى بيانات حساسة وبيانات غير حساسة، وحدد الأحكام لكل نوع بشكل واضح. المبدأ الثالث من القانون أشار على التالي:

- يجب على المؤسسة عدم جمع أية معلومات حساسة عن أي فرد إلا في حالة:

- الموافقة المسبقة من الفرد لجمع تلك المعلومات
- أن يتم جمع البيانات بموجب القانون الاسترالي أو أمر من المحكمة
- أن يكون جامع البيانات منظمة ومسموح لها بجمع البيانات الصحية
- أن يكون جامع البيانات هيئة تنفيذية وأن تكون البيانات التي تقوم بجمعها تتصل اتصالا بها أو أحد الانشطة المتعلقة بها أو
- أن يكون جامع البيانا منظمة غير ربحية على أن تكون تلك البيانات متعلقة بأنشطة المنظمة أو بأعضاء المنظمة أو للافراد الذين لديهم صلة مباشرة بأنشطة المنظمة

٥)المسؤولية والمساءلة

ألزم قانون الخصوصية الاسترالي الجهات المتعاملة مع البيانات وجود خطوات واجراءات واضحة يجب اتباعها ، كما الزمتها بوجود سياسة واضحة في إدارة البيانات وذلك حسب مبدأ الخصوصية الأول الذي نص على الآتي:

- يجب على المؤسسة وضع خطوات معقولة لتنفيذ الممارسات والاجراءات والنظم المتعلقة بمهام وأنشطة تلك المؤسسة بحيث:
  - يضمن التوافقة مع مبادئ الخصوصية الاسترالية ورموز التسجيل أن وجدت
  - سيمكن الجهة من التعامل مع الاستفسارات أو الشكاوى من الأفراد حول التزام الكيان مع مبادئ الخصوصية الأسترالية أو تلك الرموز.

- يجب على المؤسسة وضع سياسة واضحة للخصوصية حول إدارة المعلومات الشخصية من قبل تلك المؤسسة.
- يجب أن تحتوي سياسة الخصوصية على الآتي:
  - أنواع المعلومات الشخصية التي تجمعها أو تحتفظ بها المؤسسة
  - كيف تجمع وتحتفظ المؤسسة تلك المعلومات الشخصية.
  - الغرض من جمع وحفظ واستخدام والافصاح عن المعلومات الشخصية
  - كيف يمكن للفرد النفاذ إلى تلك المعلومات الشخصية التي بحوزة المؤسسة، وتصحيح تلك المعلومات اذا كانت بالحاجة الى تصحيح.
  - كيف يمكن للفرد تقديم شكوى بخصوص خرق لمبادئ الخصوصية الأسترالية، أو رمز التسجيل (إن وجد)، وكيفية التعامل مع مثل هذه الشكاوي.
  - هل ترغب المؤسسة في الكشف عن المعلومات الشخصية للمستفيدين في خارج الدولة.
  - إذا كانت المؤسسة ترغب في الكشف عن المعلومات الشخصية للمستفيدين بالخارج، أن تحدد تلك البلدان أن أمكن ذلك عمليا.

نص المبدأ السابع من قانون الخصوصية على عدم السماح للمؤسسة الاحتفاظ بالمعلومات لاستخدامها أو الكشف عن تلك المعلومات بغرض التسويق المباشر.

- واستثنى من ذلك الاشتراطات التالية في حالة المعلومات الغير حساسة:
  - قامت المؤسسة بجمع المعلومات من الفرد نفسه و
  - يتوقع الفرد من المؤسسة الكشف عن تلك المعلومات لهذا الغرض.
  - توفر المؤسسة وسيلة بحيث يسهل على الفرد طلب عدم تلقيه أي تسويق مباشر من المؤسسة
- واستثنى من ذلك الموافقة المسبقة للفرد على التسويق المباشر في حالة المعلومات الحساسة
- واستثنى من ذلك في حالة التعاقد مع مقدمي الخدمات بالشروط التالية:
  - قامت المؤسسة بالتعاقد و
  - جمعت المؤسسة تلك المعلومات بغرض الاجتماع المباشر أو غير المباشر وبموجب العقد و
  - استخدام والكشف عن المعلومات لتلبية ذلك الالتزام

٦)تنظيم النفاذ إلى البيانات

يجب على المؤسسة التي تحتفظ بمعلومات شخصية عن الفرد السماح للافراد النفاذ للمعلومات بناءا على طلبهم ، كما أوضح بعض الاستثناءات في حالة كانت المؤسسة:

١) وكالة:

- مطلوب من المؤسسة (الوكالة) رفض طلب الافراد النفاذ للمعلومات بموجب:
  - قانون حرية المعلومات
  - أي قانون آخر ينص على ذلك

٢) منظمة:

- إذا اعتقدت المؤسة أن إعطاء إذن النفاذ للمعلومات قد تشكل تهديدا خطيرا لحياة أو صحة أو سلامة الفرد أو الصحة العامة أو السلامة العامة.
- السماح بالنفاذ للمعلومات له تأثير على خصوصية الأفراد الأخرين
- طلب النفاذ تافه
- تتعلق المعلومات بالاجراءات القانونية سواءا القائمة أو المتوقعى بين المؤسسة والفرد مما قد يؤدي إلى الكشف عن تلك الاجراءات
- اذا كان النفاذ قد يؤدي إلى الكشف عن المفاوضات بين المؤسسة والفرد

- النفاذ لتلك المعلومات غير مشروع وغير قانوني
- منع النفاذ بموجب القانون الاسترالي أو أمر من المحكمة
- أن هناك شك في أنشطة المنشأة أن تكون فير مشروعة وقد يتيح النفاذ للبيانات المساس بالاجراءات المناسبة فيما يتعلق بالمسالة
- يتيح النفاذ إلى افشال أحد أنشطة هيئة تنفيذية
- يتيح النفاذ الكشف عن معلومات تقيمية للمؤسسة، والمتصلة بعملية صنع قرار خساس تجاريا للمؤسسة

أما بالنسبة للتعامل مع طلبات النفاذ للمعلومات فقد أوضح القانون لحكم التالي:

- الرد على طلب النفاذ للبيانات خلال ٣٠ يوما في حالة كانت المؤسسة وكالة، وفي غضون فترة معقولة في حالة كانت المؤسسة منظمة
- منح الحق للنفاذ حسب الطريقة المطلوبة من الفرد اذا كانت مقبولة عمليا

أما في حالة رفض طلب النفاذ، فيمكن للمؤسسة منح حق النفاذ بطريقة تلبي احتياجات المؤسسة والفرد أو من خلال استخدام وسيط متفق عليه الطرفان وبدون الإخلال بما ورد أعلاه من أحكام.

كما يجب على المؤسسة إشعار الفرد كتابيا ب:

- السبب وراء الرفض
- الآليات المتاحة للشكوى
- أية مسألة اخرى يحددها اللوائح التنظيمية

كما تم تحديد رسوم النفاذ حسب نوعية المؤسسة اذا كانت وكالة أو منظمة.

أما بالنسبة لتصحيح بيانات الافراد، فقد نص مبدأ الخصوصية ١٣ على الآتي:

المعلومات التي تحتفظ بها المؤسسة سواء:

- كانت المؤسسة مقتنعة بأن تلك المعلومات غير دقيقة أو ناقصة أو مضللة أو غير ذات صلة
- تقديم طلب من قبل الفرد لتصحيح المعلومات

فعلى المؤسسة بغض النظر من الهدف من الاحتفاظ بتلك المعلومات، اتخاذ الخطوات اللازمة لتصحيح تلك المعلومات لضمان دقة وحداثة واكتمال المعلومات وأن تكون ذات صلة و غير مضللة . أما في حالة رفض المؤسسة تصحيح المعلومات، فعليها إشعار كتابي للفرد ب:

- السبب وراء الرفض
- الآليات المتاحة للشكوى
- أية مسألة اخرى يحددها اللوائح التنظيمية

أما في حالة الرفض، وطلب الفرد بإضافة بيان لتلك المعلومات بأنها غير دقيقة أو غير مكتملة أو غير ذات صلة أو مضللة، فعلى المؤسسة اتخاذ الخطوات اللازمة لربط ذلك البيان بالمعلومات بحيث تكون واضحة لمستخدمي تلك المعلومات. وقد حدد المبدأ الفترة الزمنية اللازمة على الرد لطلبات تصحيح المعلومات حيث كانت نفس الفترات اللازمة للرد على طلبات النفاذ.

٧)الانتقال عبر الحدود

أوضح المبدأ الثامن من قانون الخصوصية بأنه يجب على المؤسسة وضع الخطوات اللازمة لضمان بان متلقي البيانات خارج حدود استراليا لا يتعارض مع مباديء الخصوصية الاسترالي

المراجـع

١- (URL: http://www.hindawi.org/safahat/41790724/)، تاريخ الدخول ١٥ ديسمبر ٢٠١٥

٢- https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

٣- DLA PIPER; Data Protection Laws of the World; August 2015