



هيئة تنظيم الاتصالات سلطنة عمان

مشروع البيانات الضخمة (Big Data) الاطار التنظيمي

شبكة الهيئات العربية لتنظيم الاتصالات وتقنية المعلومات

٢٠١٦ - ٢٠١٥

المحتوى

الفصل الاول: أساليب العمل وأهداف الدراسة

٣	المقدمة
٣	أهداف الدراسة
٤	أساليب العمل
٤	فريق التحرير
٤	فريق العمل

الفصل الثاني : الإطار التنظيمي

٥	1- الملخص التنفيذي
٥	2- المقدمة
٥	3- الاهداف
٦	4- التعريفات
٧	5- الاطراف في منظومة البيانات الضخمة
٧	1- موفر البيانات الضخمة (الموفر)
٧	2- مقدم خدمة البيانات الضخمة (مقدم الخدمة)
٨	٣- عميل خدمة البيانات الضخمة (العميل)
٨	6- التحديات
٨	أ. الخصوصية
١٠	ب. أمن البيانات
١١	ت. ملكية البيانات
١٢	ث. تصنيف البيانات الالكترونية
١٣	ج. المسؤولية والمساءلة (RESPONSIBILITY AND ACCOUNTABILITY)
١٣	ح. تنظيم النفاذ إلى البيانات الضخمة
١٤	7- الاطار التنظيمي المقترح
٢٠	8- الادوات التنظيمية
٢٠	9- المبادئ التوجيهية
٢٠	10- الخلاصة
٢١	١١- المراجع

الفصل الاول: أساليب العمل وأهداف الدراسة

المقدمة

حظيت ظاهرة البيانات الضخمة (Big Data) بترحيب محلي الصناعة واستراتيجي الأعمال ومهنيي التسويق باعتبارها تخمًا جديدًا للابتكار والتنافس والإنتاجية. وخلال الدورة الحادية عشرة للندوة العالمية لمؤشرات الاتصالات/تكنولوجيا المعلومات والاتصال (WTIS)، التي عقدت في مدينة المكسيك من ٤ إلى ٦ ديسمبر ٢٠١٣، نظر إلى البيانات الضخمة باعتبارها تمثل طاقة هائلة لتعزيز التنمية عن طريق تهيئة معلومات آنية، بتكلفة منخفضة بالقياس إلى البيانات المتأخرة من مصادر أخرى. تمتلك تقنية البيانات الضخمة إمكانية تحليل بيانات المجسات/أجهزة الاستشعار، وموقع الانترنت، وبيانات شبكات التواصل الاجتماعي السلوكية منها والاجتماعية، حيث أن تحليل هذه البيانات يسمح بوجود ارتباطات بين مجموعة من البيانات المستقلة لكشف جوانب؛ ومنها على سبيل المثال، التنبؤ للاتجاهات التجارية للشركات، وربط الاستشهادات القانونية، ومكافحة الجريمة، وتحديد ظروف حركة تدفق البيانات، وغيرها. توفر هذه التنبؤات لصانع القرار أدوات مبتكرة لفهم أفضل للعملاء والأسواق، وإدارة المخاطر على نحو فعال. يجدر القول في مسار ثورة البيانات الضخمة، بأن البيانات سوف تصبح عاملاً رئيسياً للإنتاج -ربما أكثر أهمية من الأرض والعمل ورأس المال في المقابل، فإن هذه المعلومات سوف تدفع تحول العمليات والنماذج التجارية، نحو تحقيق مستويات أعلى من الجودة والكفاءة والفعالية.

أهداف الدراسة

هذه الدراسة تهدف إلى تطوير إطار تنظيمي مشترك للبيانات الضخمة، بين الدول الأعضاء في الشبكة العربية لهيئات تنظيم الاتصالات وتقنية المعلومات (AREGNET)، والذي يعمل على تشجيع مشاركة البيانات الضخمة بين الدول أعضاء الشبكة و كما يشجع على تحليل البيانات والاستفادة منها لاتخاذ القرارات ووضع الحلول المناسبة وإيجاد حل لبعض التحديات التنظيمية.

المدة الزمنية:

ابريل ٢٠١٥ إلى ابريل ٢٠١٦

^١ البيانات الضخمة: تطورات عظيمة وتحديات هائلة (ITU News)

أساليب العمل

- ١- الأسلوب الاول : تتم بجمع الدراسات الحالية وقصص النجاح والدروس المستفادة من الدول التي لها تجارب في هذا المجال.
- ٢- الأسلوب الثاني: مساهمات فريق العمل حول تجارب كل دولة من الدول أعضاء الشبكة ، وخاصة الدول التي تمتلك تشريعات للبيانات الالكترونية أو تجارب حالية في هذا المجال.
- ٣- الأسلوب الثالث: جمع المعلومات عن:
 - أ. السياسات والأنظمة التي تعزز مشاركة البيانات الضخمة؛
 - ب. الشروط التنظيمية لمشاركة البيانات الضخمة.

فريق التحرير

- | | |
|--|------------------------------|
| Yahya.hajri@tra.gov.om | ١- المهندس / يحيى الحجري |
| ibrahim@tra.gov.om | ٢- المهندس / ابراهيم المعولي |
| mariyum.alhabsi@tra.gov.om | ٣- الفاضلة / مريم الحبسي |

فريق العمل

- ١- المهندس / يحيى الحجري (رئيس الفريق) – سلطنة عمان
- ٢- المهندس / مهند المغربل – جمهورية مصر العربية
- ٣- الفاضلة / كارول الحاج – الجمهورية اللبنانية
- ٤- السيد / سعيد المستفيد – المملكة المغربية
- ٥- المهندس / السيد عبد الفتاح حرمة - الجمهورية الإسلامية الموريتانية
- ٦- المهندس / سليمان بخش – الامارات العربية المتحدة
- ٧- السيد / نصر الدين البحرى – الجمهورية التونسية
- ٨- السيد / عادل درويش – مملكة البحرين
- ٩- المهندس / عبد الرحمن القاسم – المملكة العربية السعودية
- ١٠- المهندس / هاني السيالي - المملكة العربية السعودية
- ١١- الفاضلة / مريم الحبسي – سلطنة عمان
- ١٢- المهندس / ابراهيم المعولي – سلطنة عمان

الفصل الثاني : الإطار التنظيمي

١- الملخص التنفيذي

لا توجد حاليا احكام قانونية خاصة بالبيانات الضخمة (Big Data) ولكن تنطبق عليها الاحكام القانونية الحالية المرتبطة بالبيانات الالكترونية. ومن هنا تتلخص أهمية هذه الدراسة في وضع إطار تنظيمي متكامل حيث تتباين معاني الإطار التنظيمي ، ولكنها تتعلق عادة بالمعلومات عن اللوائح التنظيمية والتراخيص و الرسوم والضرائب وغيرها من المعلومات الهامة المتعلقة بالخدمة ، مثل الأحكام والقوانين ذات الصلة. علما بأنه يكمن أهمية ذلك للشركات الراغبة في العمل في دولة ما ، في تقييم المخاطر التنظيمية و القانونية في كل دولة من خلال مراجعة الالتزامات القانونية/ التنظيمية لفهم التكاليف والإجراءات الهامة التي يجب اتباعها عند تقديم الخدمة.

٢- المقدمة

هذه الوثيقة تقدم وصف لبعض التحديات والصعوبات المتوقعة عند تقديم خدمة تحليل البيانات الضخمة (BigData) وحفظها والمشاركة بها، كما تشير للاجراءات التنظيمية المقترح إتخاذها لتنظيم تقديم هذه الخدمة . علما بان هذه الاجراءات تشمل إصدار لوائح أو قواعد إرشادية أو تراخيص أو تعديل في القوانين ذات العلاقة.

٣- الاهداف

يهدف هذا الاطار إلى تنظيم التعامل مع خدمة تحليل البيانات الضخمة ، وذلك من خلال طرح أدوات تنظيمية تحمي المصلحة العامة وتعزز ثقة العموم في هذا القطاع ؛ ويكون ذلك بتنظيم التحديات التالية :

١- الخصوصية

يقصد بها هنا خصوصية بيانات المستخدمين/المنتفعين و الاجراءات الواجب اتباعها للحفاظ على البيانات من الاستخدام غير المخول.

٢- أمن البيانات

تعنى بشروط تأمين بيانات المنتفعين و شروط التعامل معها، وقد تشمل معالجة البيانات داخل وخارج الدولة.

٣- ملكية البيانات

أي وجود حق مشروع في حيازة واستخدام وتوزيع البيانات الالكترونية على مستوى الاشخاص ومؤسسات القطاع العام للدولة.

٤- حرية المعلومات (أو حرية البيانات)

جوانب تعزيز حق الاطلاع على معلومات الأفراد الشخصية والقطاع العام (مؤسسات وشركات) المتوفرة لدى الجهات العامة بغرض زيادة الشفافية ودعم المنافسة والاستثمارات، وتحقيق الأمن والاستقرار.

٥- تصنيف البيانات الالكترونية

يشمل تصنيف البيانات الالكترونية و شروط التعامل مع كل فئة . كما يشمل شروط نقل البيانات خارج الحدود.

٦- المسؤولية والمساءلة

كيفية ضمان الشفافية وحق الرفض لتوقعات البيانات الضخمة ، وذلك قبل اعتمادها في صناعة القرار .

٧- تنظيم النفاذ إلى البيانات الضخمة

٤- التعريفات

البيانات الضخمة مصطلح يستخدم لوصف مجموعات بيانات كبيرة للغاية أو على درجة من التعقيد أو التي تتطلب قدرًا كبيرًا من المعالجة السريعة (التي تسمى أحيانًا مشاكل الحجم / النوع / السرعة)، والتي يصبح من الصعب أو من المستحيل التعامل معها باستخدام قواعد البيانات التقليدية والأدوات التحليلية التقليدية، علما بأن معالجة بيانات بهذا الحجم يتطلب برمجيات تعمل بشكل متوازي على العشرات أو المئات، أو حتى آلاف من الخوادم.

البيانات الحكومية (بيانات القطاع العام): هي المعلومات، بما في ذلك المنتجات والخدمات الإعلامية، التي تم إنشاؤها وجمعها ومعالجتها، والحفاظ عليها وصيانتها ونشرها، أو تمويلها من قبل الحكومة أو مؤسسة عامة ، ومن الأمثلة على ذلك: المعلومات الجغرافية، والاحصاءات وبيانات الطقس وبيانات المشاريع البحثية الممولة من القطاع العام، والكتب الرقمية من المكتبات.

معالجة البيانات أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية عن طريق وسائل تلقائية أو غيرها أو جمعها أو تسجيلها أو تنظيمها أو تخزينها أو تعديلها أو

^٢ OECD ، منظمة التعاون الاقتصادي والتنمية

تحويلها أو استرجاعها أو مراجعتها أو الإفصاح عنها عن طريق إرسالها أو توزيعها أو إتاحتها بوسائل أخرى أو تنسيقها أو ضم بعضها لبعض أو حجبها أو محوها الغائها .

سياسة الخصوصية هي السياسة التي تحدد المتطلبات اللازمة لحماية الوصول إلى، ونشر، المعلومات الشخصية (Personally Identifiable Information) وحقوق الأفراد فيما يتعلق كيفية استخدام المعلومات الشخصية الخاصة بهم.

البيانات المفتوحة: البيانات التي يتم تبادلها مع الجمهور بغية تعزيز مشاركة الجمهور ومستوى الابتكار.

٥- الاطراف في منظومة البيانات الضخمة

لكي يتم تنظيم أي خدمة يجب تحديد الاطراف المتعاملة مع هذه الخدمة وتحديد واجبات وحقوق كل طرف . تتكون منظومة البيانات الضخمة من عدة جهات تتفاعل في مابينها للوصول الى رؤية أعمال ، هذه المنظومة مكون من:

١- **موفر البيانات الضخمة (الموفر) ^٤** ، يعمل موفر البيانات الضخمة على توفير البيانات من مصادر مختلفة إلى مقدم الخدمة . وتشمل أنشطة موفري البيانات على التالي على سبيل المثال وليس الحصر:

- إنشاء البيانات .
- إنشاء المعلومات الوصفية (metadata) التي تصف مصدر البيانات والسمات ذات الصلة؛
- نشر المعلومات الوصفية .
- إيجاد مصادر البيانات المفتوحة (open-data) على الانترنت و إنشاء المعلومات الوصفية (metadata) لها .
- توفير بيان الخدمات (service catalogue) الى مقدم الخدمة عن البيانات القابلة للاستخدام.

٢- **مقدم خدمة البيانات الضخمة (مقدم الخدمة) ^٥** ، يقوم مقدم الخدمة بتحليل البيانات الضخمة وتوفير البنية التحتية اللازمة لها . وتشمل أنشطة مقدم الخدمة على التالي على سبيل المثال وليس الحصر:

^٣ ITU-T X.1252 (04/2010)

^٤ الاتحاد الدولي للاتصالات ، قطاع التقييس، Y.3600 ، متطلبات وقدرات للبيانات الضخمة المعتمدة على الحوسبة السحابية - المصدر السابق

- البحث في مصادر البيانات وجمع البيانات عن طريق الطلب المباشر من موثر البيانات أو البحث في الانترنت (Data Crawling)؛
 - تخزين البيانات؛
 - دمج البيانات؛
 - توفير أدوات لتحليل البيانات .
 - دعم إدارة البيانات مثل مصدر البيانات (Data Province)، خصوصية البيانات وأمن البيانات، وسياسة الاحتفاظ بالبيانات، وملكية البيانات.
- ٣- **عميل خدمة البيانات الضخمة (العميل)** هو المستخدم النهائي لمنظومة البيانات الضخمة أو هو نظام يستخدم النتائج أو الخدمات التي يقدمها مقدم الخدمة . كما يمكن للعميل أن ينتج خدمات جديدة أو معرفة، وذلك اعتماداً على نتائج تحليل البيانات الضخمة . وتشمل أنشطة العميل على سبيل المثال لا الحصر:
- طلب خدمات البيانات الضخمة من المزود؛
 - استخدام مخرجات خدمات البيانات الضخمة.

٦- التحديات

لا توجد قوانين وتشريعات تنظم حالياً البيانات الضخمة . لكن في نفس الوقت، يجب على الشركات التي تسعى لتقديم خدمة تحليل البيانات الضخمة التأكد من أن أنشطتها المقترحة تتوافق وتتواءم مع القوانين القائمة والتي تنظم البيانات الالكترونية . البيانات الضخمة هي بيانات إلكترونية في آخر الأمر ، وينطبق عليها الأحكام والقوانين الحالية مثل قانون الخصوصية وقوانين حماية البيانات . التحدي الأكبر هو تطوير هذه القوانين التي صدرت من عدة سنوات **بشكل مبتكر لا يعيق التقدم** . فيما يلي نستعرض بعض التحديات التي يعتقد أنها تشكل تحدي في عملية تنظيم تقديم هذه الخدمة.

أ. الخصوصية

يصبح ضمان خصوصية البيانات الشخصية أكثر صعوبة مع تضاعف حجم البيانات وسرعة تبادلها على نطاق واسع . نتائج تحليل البيانات الضخمة لا تنطوي دائماً على البيانات الشخصية. ولكن ، عند حصول ذلك ، ينبغي أن تمثل هذه البيانات لقواعد ومبادئ حماية البيانات . السؤال ليس ما إذا كان لتطبيق قانون حماية البيانات على البيانات الضخمة ،

^٦ المصدر السابق

ولكن كيفية تطبيقه بشكل مبتكر لا يعيق التقدم . تتلاقى البيانات الضخمة والبيانات الشخصية لتشكيل المنتجات الاستهلاكية عبر الإنترنت.

١- الاحكام القانونية في الدول العربية:

- في القانون العماني^٧ الأصل هو الالتزام بالسرية والمحافظة على خصوصية البيانات ، ولا يجوز إفشائها إلا وفقا للحالات التي يحددها القانون صراحة (أوامر المحكمة ، موافقة الشخص الصريحة ، المصلحة العامة) .
- القانون الاماراتي والقطري ينص بضرورة اتخاذ الإجراءات اللازمة لمنع الاستخدام غير المصرح له للبيانات أو الكشف عن المعلومات الشخصية، واتخاذ الإجراءات في سبيل ضمان السرية والخصوصية بحكم أنها الأصل ، ولا يجوز الخروج عن هذا الأصل إلا في حالات محددة وصريحة ، وتحديد الغرض التي من أجله تم جمع البيانات .
- يتم العمل حاليا في المملكة العربية السعودية على نظام حماية خصوصية البيانات الشخصية ، يهدف هذا النظام إلى حماية خصوصية البيانات الشخصية لدى الأفراد في المملكة العربية السعودية، ومنها البيانات الائتمانية والصحية والشخصية (كالاسم، ورقم الهوية، والعنوان، وأرقام التواصل) وغيرها من البيانات المتعلقة بالأفراد. حيث يغطي النظام جوانب حفظ البيانات ومعالجتها، إضافة إلى جوانب تتعلق بالمشاركة والنشر لها بين الجهات المختلفة داخل المملكة وخارجها.
- أقر المغرب سنة ٢٠٠٩ قانونا يتعلق بحماية الأشخاص الذاتيين اتجاه المعطيات ذات الطابع الشخصي (قانون رقم ٠٨، ٠٩). ويمكن إيجاز الأهداف المتوخاة من إصدار هذا القانون كالآتي:
 - ١. دعم وتكريس حماية الحقوق الفردية والحريات الفردية والجماعية؛
 - ٢. تجاوب المغرب مع التزاماته المتعلقة بالتقارب التشريعي مع الاتحاد الأوروبي، كما ينص على ذلك اتفاق الشراكة بينهما وكما يقضي بذلك الوضع المتقدم الذي يحظى به المغرب منذ ٢٠٠٨.
 - ٣. تحسين شروط استقبال الاستثمارات الأجنبية بما يمكن المغرب من خلق إطار قانوني جذاب لفائدة أنشطة ترحيل الخدمات.
- كما صدر في المملكة المغربية في ٢٠٠٩، المرسوم رقم ٢، ٠٩، ١٦٥ لتطبيق القانون ٠٨، ٠٩ الذي يضبط بعض الأحكام القانونية ويحدد تركيبة اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي.

^٧ مرفق (ورقة عمل حول تنظيم البيانات الشخصية / الالكترونية وفق القوانين العمانية)

^٨ مرفق (ورقة عمل حول الأحكام التنظيمية/القانونية التي تنظم التعامل مع البيانات الإلكترونية في المملكة العربية السعودية)

^٩ مرفق (ورقة عمل حول الأحكام القانونية والتنظيمية المرتبطة بالبيانات الضخمة بالمغرب)

- القانون المنظم للاتصالات بالمغرب (قانون ٩٦-٢٤) يلزم المتعهدين ومقدمي خدمات الاتصالات باحترام سرية الاتصالات وبحمائية المعطيات الشخصية طبقا للقوانين المرتبطة بهذه المجالات (المادة ٢٦). ويوضح المرسوم رقم ٧٧١-٠٥-٢ هذه الإلزامية وكيفية التقيد بها.

٢. الاحكام القانونية في الاتحاد الاوروبي

في عام ١٩٩٥، سنّ الاتحاد الأوروبي تشريعا للخصوصية وهو توجيه الاتحاد الأوروبي، وقد ألزم هذا التشريع الموافقة المسبقة لجمع ومعالجة البيانات ، بحيث تكون تلك الموافقة صريحة لا لبس فيها، وأن لا تتعدى معالجة تلك البيانات على الحريات أو الخصوصية.

٣. الاحكام القانونية في استراليا

قانون الخصوصية الاسترالي الصادر في ١٩٨٨ والذي تم تعديله في ٢٠١٢ ينص على إلزامية الموافقة المسبقة لجمع أو استخدام البيانات مع تحديد الغرض الرئيسي من تلك البيانات ، وأن يتم جمع تلك البيانات بالطرق المشروعة والعادلة ، ويستثنى من ذلك النص الصريح بخلاف ذلك أو أمر من المحكمة.

ب. أمن البيانات

تحدي تأمين البيانات الضخمة تزايد مع تزايد سرعة انتقال البيانات و تنوع أنماطها و زيادة حجمها وتنوع مصادرها . أضف على ذلك طبيعة الإرسال المتواصل للحصول على البيانات . وبالتالي، الآليات الأمنية التقليدية والتي صممت لتأمين البيانات الثابتة في نطاق صغير محدود ، يمكن أن تكون غير كافية لتأمين البيانات الضخمة. تحليل هذه البيانات الضخمة خارج حدود الدولة المالكة للبيانات يشكل تحدي آخر في تأمين اية بيانات .

في القانون العماني^{١٠} يحظر تحويل البيانات للخارج إلا بعد موافقة الجهة المختصة مع ضرورة الأخذ في الاعتبار مستوى كافي من الضمانات فيما يتعلق بحمايتها والمحافظة على خصوصيتها ، والنظر في الاعتبار في (طبيعة البيانات الشخصية، مصدر المعلومات المضمنة في البيانات، الأغراض المراد معالجة البيانات من أجلها ومدتها، الدولة التي يتم تحويل البيانات إليها والتزاماتها الدولية).

الأمن المعلوماتي^{١١} في المغرب مؤطر بمجموعة من النصوص القانونية المرتبطة بالتبادل الإلكتروني للمعطيات القانونية وكذلك القوانين المتعلقة بمكافحة الإرهاب وبعض مواد القانون الجنائي:

^{١٠} مرفق (ورقة عمل حول تنظيم البيانات الشخصية / الالكترونية وفق القوانين العمانية)
^{١١} للمزيد التفاصيل مرفق (ورقة حول الأحكام القانونية والتنظيمية المرتبطة بالبيانات الضخمة بالمغرب)

١- قانون رقم ٥٣,٠٥ المتعلق بالتبادل الإلكتروني للمعطيات القانونية الذي يحدد في جزء منه النظام المطبق على المعطيات القانونية التي يتم تبادلها بطريقة إلكتروني، وفي جزء آخر المعادلة بين الوثائق المحررة على الورق وتلك المعدة على دعامة إلكترونية وكذلك كل ما يتعلق بالتوقيع الإلكتروني.

٢- قانون رقم ٠٧,٠٣ بتتيمم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعلومات ويحدد هذا القانون العقوبات المطبقة على كل من مس بنظام المعالجة الآلية للمعلومات.

٣- قانون رقم ٠٣,٠٣ يتعلق بمكافحة الإرهاب.

٤- قانون رقم ٠٩,٠٨ لسنة ٢٠٠٩ في هذا القانون تم وضع أساس قانوني لتأطير حرية تدفق المعلومات عبر الحدود في زمن العولمة والتطور السريع لتقنية المعلومات؛

- أما قانون الخصوصية الصادر من الاتحاد الأوروبي فقد إفاد أنه يجب أن تبقى البيانات التي تم جمعها آمنة ومأمونة من الإساءة المحتملة، أو السرقة، أو فقدان. كما ألزمت الدول الأعضاء الاشتراط على المتحكم اختيار المعالج الذي يوفر ضمانات كافية فيما يتعلق بالتدابير الأمنية التقنية والتدابير التنظيمية التي تحكم معالجة تلك البيانات وضمان الامتثال لتلك التدابير. وأن إجراء المعالجة عن طريق معالج معين يجب أن يحكمها عقد قانوني ملزم للمعالج من قبل المتحكم.

- وفي استراليا أوضح قانون الخصوصية بأن تتخذ المؤسسة التي تحتفظ بالبيانات الخطوات المعقولة لحماية البيانات من سوء الاستخدام أو من النفاذ الغير المصرح به أو التعديل . ويستثنى من ذلك أمر من المحكمة أو نص صريح بموجب قانون استرالي آخر.

ت. ملكية البيانات

عدم وضوح من هو المالك لبيانات القطاع العام او البيانات الحكومية^{١٢} يشكل تعقيدا في عملية مشاركة البيانات الحكومية مع موفر الخدمة. من الضروري تبيان ما اذا كانت البيانات مملوكة للحكومة أو للجهة التي تنتجها وتبيان صلاحيات المالك في التعامل مع هذه البيانات.

^{١٢} الرجاء الاطلاع على التعريف في الفقرة ٤ من هذا الفصل

في القانون المغربي^{١٣} ، إذا استثنينا البيانات الشخصية، لا يوجد نص قانوني يحدد صراحة ملكية البيانات. يستنبط من القانون ٠٩,٠٨ المتعلق بحماية المعطيات الشخصية أن البيانات الشخصية هي ملك لأصحابها ولا يمكن معالجتها إلا بشروط يحددها نص قانوني. وقد وضع في هذا السياق القانون ٠٩,٠٨ شروط محددة لمعالجة هذه المعطيات :

- المبدأ الأساس هو موافقة الشخص المعني؛
- هذا المبدأ يعرف استثناءات عندما تتبين ضرورة معالجة هذه البيانات لأغراض حصرها القانون (المواد ٤ و ٢١) وألحق شروطاً أخرى من أهمها الإجراءات لدى اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (المادة ١٢)، احترام شروط المعالجة (المادة ٣)، ضمان حقوق الشخص المعني بالمعالجة (المواد من ٥ إلى ١١) وحماية سرية البيانات الشخصية (المواد ٢٣ و ٢٤).

الاتحاد الأوروبي لم يحدد ملكية البيانات بشكل صريح في قانون الخصوصية، 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 بند الخصوصية. وكذلك الأمر في قانون الخصوصية الاسترالي إذ لا يوجد نص صريح يتحدث عن ملكية البيانات.

ث. تصنيف البيانات الالكترونية

عدم وجود تصنيف للبيانات الحكومية يحدد حساسية هذه البيانات و سبل التعامل معها من حيث التخزين وقابلية النشر أو المشاركة ، مما يشكل تحدي في تقديم خدمة تحليل البيانات الضخمة . في ظل غياب هذا التصنيف يمكن لأي جهة أن تتحفظ في نشر بياناتها الإلكترونية على شبكة الانترنت او حتى مشاركتها مع موفر الخدمة.

ينص القانون الاسترالي أنه ليس هناك حاجة إلى تمييز وقائي أو تصنيف أمني لكل البيانات. التصنيف ضروري فقط للبيانات الحساسة ، التي قد تضر المصلحة الوطنية أو الأفراد إذا تم اختراقها ، أو التي تتطلب حماية بموجب قانون الخصوصية، او قانون المحفوظات أو أي تشريع آخر. صنف قانون الخصوصية الاسترالي البيانات الى بيانات حساسة وبيانات غير حساسة، وحدد الأحكام لكل نوع بشكل واضح .

^{١٣} المصدر السابق

ج. المسؤولية والمساءلة (Responsibility and Accountability)

يقصد هنا بمسؤولية موفر الخدمة (الرقابة الداخلية) في التعامل مع البيانات . تتطلب الرقابة الداخلية وضع آليات داخلية وأنظمة التحكم القياسية التي تضمن الامتثال وتقديم الأدلة ، بما فيهم السياسات والاجراءات الداخلية و تقارير التدقيق لإثبات الامتثال للسلطات الرقابية. المساءلة ليست ممارسة لمرة واحدة، ولكن استمرارية موفر الخدمة للامتثال للقانون هو عنصر أساسي من عناصر المسؤولية.

على الرغم من أن هذه النقطة تعتمد على الاجراءات التي يتخذها مقدم الخدمة والموفر لضمان جودة الخدمة . ولكن ذلك لا يمنع ضرورة إلزام مقدم الخدمة والموفر على تقديم نتائج التدقيق الداخلي الى السلطة المختصة.

في القانون العماني ، يكون لصاحب البيانات الحق في تقديم شكوى لدى السلطة المختصة إذا رأى أو اعتبر أن معالجة البيانات الشخصية له لا تتوافق مع أحكام القانون كالإخلال بالخصوصية أو انتهاك السرية أو الإعتداء على سلامة البيانات (مسؤولية جزائية). يحق لأي شخص تكبد أضرارا نتيجة لمعالجة غير قانونية أن يستلم تعويضا عن الضرر الذي تكبده (مسؤولية مدنية) .

ح. تنظيم النفاذ إلى البيانات الضخمة

مفهوم البيانات المفتوحة يشير إلى فكرة أن بعض البيانات ينبغي أن تكون متاحة بحرية للاستخدام وإعادة استخدامها. علما بأن تطبيق مفهوم البيانات المفتوحة يهدف إلى التركيز على توليد القيمة المضافة من خلال إعادة استخدام نوع معين من البيانات مثل البيانات الحكومية (بيانات القطاع العام)^{١٤} . تتميز البيانات الحكومية المفتوحة بعدد من الخصائص، من أبرزها:

- البيانات العامة لديها امكانيات كبيرة لإعادة استخدامها في منتجات وخدمات جديدة.
- معالجة التحديات الاجتماعية - وجود المزيد من البيانات المتاحة علنا سيساعدنا على اكتشاف حلول جديدة ومبتكرة.
- تحقيق مكاسب الكفاءة من خلال تبادل البيانات داخل وبين الإدارات العامة وتعزيز العدالة في تنفيذ مشاريع التنمية الاقتصادية؛

^{١٤} الرجاء الاطلاع على التعريف في الفقرة ٤ من هذا الفصل

- تعزيز مشاركة المواطنين في الحياة السياسية والاجتماعية وزيادة الشفافية في الحكومة، وتحقيق الأمن والاستقرار.

يتم^{١٥} العمل حالياً في المملكة العربية السعودية على (نظام حرية المعلومات) يهدف هذا النظام إلى تعزيز حق المواطن في المملكة العربية السعودية للاطلاع على معلومات الأفراد الشخصية المتوفرة لدى الجهات العامة بغرض زيادة الشفافية وتعزيز العدالة في تنفيذ مشاريع التنمية الاقتصادية والاجتماعية وتحقيق الأمن والاستقرار. ومن المعلومات التي يغطيها النظام، معلومات ذات الطبيعة التجارية أو الصناعية أو المالية أو الاقتصادية، كمعلومات المتعلقة بالمنافسات والعطاءات والمزايدات التي يؤدي الإفصاح عنها إلى الإخلال بعدالة المنافسة. كما يغطي التنظيم المعلومات المتعلقة بالبحوث العلمية أو التقنية التي يؤدي الكشف عنها إلى المساس بحق معنوي.

تداول^{١٦} الحكومة المغربية لتنظيم الحق في الولوج إلى المعلومات وذلك لتطبيق الفصل ٢٧ الذي نص على أن "للمواطنين والمواطنات الحق في الحصول على المعلومات، الموجودة في حوزة الإدارة العمومية، والمؤسسات المنتخبة، والهيئات المكلفة بالمرفق العام" ونص كذلك على أنه "لا يمكن تقييد الحق في المعلومة إلا بمقتضى القانون، بهدف حماية كل ما يتعلق بالدفاع الوطني، وحماية أمن الدولة الداخلي والخارجي، والحياة الخاصة للأفراد، وكذا الوقاية من المس بالحريات والحقوق الأساسية المنصوص عليها في هذا الدستور..."

كما أطلقت الحكومة المغربية مبادرة "البيانات المفتوحة" لتسهيل الولوج للبيانات العمومية (www.data.gov.ma).

٧- الإطار التنظيمي المقترح

لتنظيم تقديم خدمة البيانات الضخمة ، على الجهة التنظيمية العمل على إصدار التشريعات التي تنظم هذه الخدمة للتغلب على التحديات السابق ذكرها . يمكن أن يشمل التنظيم إصدار اللوائح أو القواعد الإرشادية أو التراخيص أو التعديلات على القوانين ذات العلاقة ، ويكون ذلك على النحو التالي:

أ. يجب تنظيم عمل مقدم الخدمة والموفر والعميل^{١٧} لضمان استيفاء الشروط المذكورة أدناه.

^{١٥} مرفق (ورقة عمل حول الأحكام التنظيمية/القانونية التي تنظم التعامل مع البيانات الإلكترونية في المملكة العربية السعودية)

^{١٦} مرفق (ورقة عمل حول الأحكام القانونية والتنظيمية المرتبطة بالبيانات الضخمة بالمغرب)

^{١٧} يمكن للعميل أن ينتج خدمات جديدة مبنية على نتائج تحليل البيانات الضخمة ، لذا وجب إضافته هنا.

ب. مسألة الخصوصية

- يلزم مقدم الخدمة و الموفر بضرورة اتخاذ الإجراءات اللازمة لمنع الاستخدام غير المصرح له للبيانات أو الكشف عن المعلومات الشخصية.
- يلزم مقدم الخدمة و الموفر بالحصول على الترخيص الملائم لمعالجة البيانات الحساسة، على أن تكون أسباب تلك المعالجة للمصلحة العامة كمجال الصحة العامة والحماية الاجتماعية، على أن يتعين علي مقدم الخدمة و الموفر توفير ضمانات محددة ومناسبة لحماية الحقوق الأساسية والخصوصية.
- على مقدم الخدمة و الموفر الالتزام بالمعايير القياسية (Standards) كداعم لتوفير ضمانات، مع الحاجة إلى التقييد المستمر بالمعايير المعتمدة ووفقا للتطورات والتحديثات التي يطرأ عليها.
- في حالة فشل مقدم الخدمة في الالتزام بحقوق وحرريات معالجة البيانات، يحق لأي شخص تعرض لأضرار نتيجة عملية المعالجة الغير قانونية أو كانت عملية المعالجة تتعارض مع أحكام القوانين الوطنية المعتمدة وفقا لهذا التوجيه، أن يحصل على تعويض من مقدم الخدمة حسب الأضرار التي لحقت بهم. كما يجوز أعفاء مقدم الخدمة جزئيا أو كليا في حالة تم إثبات أن المتحكم ليست مسؤولة عن هذا الحدث الذي أدى الى ذلك الضرر.

ت. أمن المعلومات

- إنشاء مركز وطني لأمن المعلومات في كل دولة يعمل على تحليل المخاطر والتهديدات الأمنية الموجودة في الفضاء الإلكتروني و يعمل على توصيل هذه المعلومات لجميع مستخدمي خدمات الانترنت ووسائل تقنية المعلومات، سواء كانوا من المؤسسات العامة أو الخاصة أو الأفراد.
- إلزام مقدم الخدمة و الموفر بعدم نقل البيانات الحكومية وبيانات البنوك و بيانات الافراد عند الشركات الخاصة خارج الحدود.
- إلزام مقدم الخدمة و الموفر بحماية جميع البيانات، وذلك عبر إستخدام آليات أمنية، عند تخزين البيانات ونقلها ومعالجتها؛
- إلزام مقدم الخدمة و الموفر بحذف البيانات ذات الصلة، والنتائج التحليلية وفقا للمدة التي يحددها العميل أو بناء على طلب العميل ووفقا للأنظمة المعتمدة . كما يجوز للعميل تعديل أو تصحيح البيانات اذا اقتضت الحاجة.

- إلزام مقدم الخدمة و الموفر بتنفيذ التدابير الفنية والتنظيمية المناسبة لحماية البيانات الشخصية من التدمير المتعمد أو غير القانوني أو فقدانها وتعديلها أو الكشف غير المصرح به أو النفاذ إليها، وبخاصة ما ينطوي على معالجة ونقل البيانات عبر الإنترنت ، وضد الأشكال الأخرى غير المشروعة في المعالجة.

ث. تصنيف البيانات

- إصدار تصنيف الوثائق/البيانات الحكومية باستخدام نظام تصنيف يحدد أهمية ومستوى سرية هذه البيانات. ويكون ذلك عبر إصدار مبادئ توجيهية تساعد الجهات الحكومية و مؤسسات القطاع العام في تحديد قيمة المعلومات و طرق التعامل مع كل فئة من فئات هذا التصنيف. يحدد هذا التصنيف البيانات الى فئات مثل - سري و سري للغاية ، وقابل للمشاركة مع الجهات الحكومية الأخرى ، وقابل للنشر . كما يصنف البيانات الشخصية الى بيانات حساسة وبيانات غير حساسة.

- تصنيف البيانات الشخصية الى المستويات التالية^{١٨} :

المستوى الاول:

- ١- الاسم الكامل
- ٢- عنوان المنزل
- ٣- البريد الإلكتروني
- ٤- الرقم القومي/الرقم المدني
- ٥- عنوان بروتوكول الإنترنت (IP Address)
- ٦- رقم بطاقة الإئتمان
- ٧- الهوية الإلكترونية

المستوى الثاني:

- ١- بيانات الديون
- ٢- الراتب
- ٣- الأمراض/الأدوية

المستوى الثالث:

- ١- الديانة / المذهب

^{١٨} المصدر : هواوي ، Huawei data openness management policy

- ٢- الأصول العرقية
- ٣- العمر
- ٤- مكان العمل
- ٥- مكان الدراسة
- ٦- المنصب

المستوى الرابع:

- ١- الادوية التي لا تحتج وصفة طبية
- ٢- عيادة الاسنان
- ٣- طبيب العيون/ النظارات الطبية
- ٤- الهوية الالكترونية غير محددة الشخصية (Anonymized User ID)

- بالاشارة الى التصنيف السابق ، يوصى بالتالي:
 - ❖ عدم نشر بيانات المستوى الاول والثاني على شبكة الانترنت .
 - ❖ عدم تخزين بيانات المستوى الاول والثاني خارج الحدود.

ج. المسؤولية والمساءلة (الرقابة الداخلية)

- يمكن أن يتم طرح النقاط التالية على شكل قواعد إرشادية لمقدم الخدمة او الموفر.
- هناك العديد من العناصر التي تشكل ممارسات جيدة للرقابة والاجراءات الداخلية لمقدم الخدمة او الموفر.
 - ١- ضمان الخصوصية وحماية البيانات مسبقا حسب التصميم وبشكل افتراضي (by design and by default)
 - ٢- قيام مقدم الخدمة بعمليات داخلية لتقييم جهود حماية البيانات والتدقيق.
 - ٣- توافر الخبرة في مجال حماية البيانات ، وتشمل تعيين ضابط حماية البيانات، داخل الشركة قد تسهم جميعها وتشكل جزء لا يتجزأ من نظام الرقابة الداخلية لموفر الخدمة.
- يجب أن يخطر مقدم الخدمة او الموفر مؤسسات السلطة الرقابية الوطنية عند حصول عمليات اختراق للبيانات الخطيرة في أقرب وقت ممكن (في غضون ٢٤ ساعة ، إذا كان ذلك ممكنا).

ج. ملكية البيانات

- إلزام حق نقل البيانات (Data Portability) على موفر الخدمة (أو مشغلي الاتصالات) بالشكل الذي يسمح للعميل باستخراج البيانات الشخصية من موفر خدمة واحد ونقلها إلى آخر. سيتمكن هذا الحق الشركات الصغيرة الناشئة من القدرة على الوصول إلى أسواق البيانات التي تهيمن عليها الشركات الرقمية العملاقة وجذب المزيد من المستهلكين.
- من حق المستخدمين 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.

خ. النفاذ الى البيانات الضخمة

- إلزام الجهات الحكومية و مؤسسات القطاع العام والخاص بتوفير البيانات المفتوحة (Open Data) التي تملكها عبر الانترنت ، حتى تتيح فرصة اكبر للاستفادة من هذه البيانات . وهذه البيانات يجب أن تكون متاحة بشكل (Format) يسهل إعادة إستخدامها من الجهات الاخرى.
- يجب على السلطة التنظيمية/التشريعية تحديد عمليات المعالجة التي يمكن أن تشكل مخاطر على الحقوق والحريات .
- يجب على السلطة التنظيمية/التشريعية إجراء مراجعة لعمليات المعالجة التي يمكن أن تشكل مخاطر على الحقوق والحريات، فور استلامها لاشعار مقدم الخدمة.

د. المعايير

- إلزام مقدم الخدمة والموفر بالالتزام بالمعايير القياسية مثل التوصية Y.3600 حول (المتطلبات والقدرات للبيانات الضخمة المعتمدة على الحوسبة السحابية) ، والصادر عن الاتحاد الدولي للاتصالات ، قطاع التقييس (٢٠١٥/١١) ،

ذ. أحكام عامة

- يجب على العميل و الموفر عدم جمع أية معلومات حساسة عن أي فرد إلا في الحالات التالية:

- ١- الموافقة المسبقة من الفرد لجمع تلك المعلومات.
- ٢- أن يتم جمع البيانات بموجب القانون أو أمر من المحكمة.

- ٣- أن يكون جامع البيانات منظمة ومسموح لها بجمع البيانات الصحية
 - ٤- أن يكون جامع البيانات هيئة تنفيذية وأن تكون البيانات التي تقوم بجمعها تتصل اتصالاً بها أو أحد الأنشطة المتعلقة بها أو
 - ٥- أن يكون جامع البيانات منظمة غير ربحية على أن تكون تلك البيانات متعلقة بأنشطة المنظمة أو بأعضاء المنظمة أو للأفراد الذين لديهم صلة مباشرة بأنشطة المنظمة
- يحظر على مقدم الخدمة 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:
 - ١- هناك موافقة صريحة على معالجة تلك البيانات
 - ٢- المعالجة ضرورية لحماية المصالح للموضوع أو بيانات شخص ما غير قادر على إعطاء الموافقة الصريحة قانونياً.
 - ٣- 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.
 - ٤- تتم معالجة البيانات المتعلقة بالجرائم، والإدانات الجنائية أو الإجراءات الأمنية ، فقط تحت سيطرة السلطة الرسمية.
 - ٥- تتم معالجة البيانات المتعلقة بالجزاءات الإدارية أو الأحكام في القضايا المدنية على أن تكون المعالجة تحت سيطرة السلطة الرسمية.
 - يجب على السلطة التنظيمية وضع الخطوات اللازمة لضمان بأن متلقي البيانات خارج حدود لا يتعارض مع مبادئ حماية البيانات في الدولة.
 - يجب على الموفر والعميل وضع الخطوات اللازمة لضمان جودة البيانات.
 - على السلطة التنظيمية وضع الخطوات اللازمة لتشجيع تغيير ثقافة الجهات لتبادل البيانات .

٨- الأدوات التنظيمية

قبل وضع إطار تنظيمي للبيانات الضخمة يجب فهم التحديات القائمة والتي تواجه تقديم الخدمة ، حتى يسهل تحديد الأدوات والسياسات اللازمة لتنظيم تقديم خدمة البيانات الضخمة. تعمل المنهجية التالية على إيجاد إطار تنظيمي يحدد الأدوات التنظيمية والسياسات والإجراءات اللازمة لتقديم خدمة البيانات الضخمة .

- الخطوة ١: استعن **بالفقرة ٦** لتحديد التحديات التنظيمية للبيانات الضخمة .
- الخطوة ٢: استعن **بالفقرة ٦** لتحديد الأحكام والقوانين ذات الصلة النافذة حالياً.
- الخطوة ٣: استعن **بالفقرة ٧** لتحديد التوصيات ذات العلاقة بكل تحدي.
- الخطوة ٤: استخلص الأدوات التنظيمية والسياسات والإجراءات اللازمة لتنظيم تقديم خدمة البيانات الضخمة .

٩- المبادئ التوجيهية

من المهم تطبيق بعض المبادئ التوجيهية عند تطوير الأدوات التنظيمية والسياسات . هذه المبادئ تهدف في الأساس الى التقليل من التكاليف على المجتمع. على وجه الخصوص، نقترح ، تطوير الأدوات التنظيمية والسياسات أن تتم وفقاً لمبادئ:

- **الشفافية** ، يجب أن تكون أهداف السياسة محددة بوضوح ومفهومة بسهولة من قبل جميع أصحاب المصلحة؛
- **الملاءمة** ، يجب أن تكون أن أهداف السياسة مختارة بحيث تستجيب لحاجة اجتماعية واقتصادية حقيقية؛
- **الاتساق** ، يجب أن تكون أهداف السياسة متسقة مع السياسات الحكومية الأخرى والبرامج والأهداف.

١٠- الخلاصة

- على خلفية التطور السريع للاقتصاد الرقمي وللسوق البيانات الضخمة بالتحديد على حساب الحقوق الأساسية مثل الخصوصية وحماية البيانات الشخصية والمصالح العامة والحقوق الأساسية ، نجد أنه من الضروري تحقيق بعض التقارب بين التشريعات والأدوات التنظيمية الحالية وهذه الخدمات.

- عدم التفاعل في وضع السياسات مع هذا التطور يؤثر بشكل سلبي على المنافسة وحماية بيانات المستهلك. وهذه الآثار السلبية قد خفضت كل من فعالية إنفاذ قواعد المنافسة والحافز لتطوير الخدمات التي تعزز الخصوصية وتقليل احتمالات الاذى بالنسبة للمستهلك.
- الخدمات عبر الإنترنت هي التي تقود النمو الهائل في الاقتصاد الرقمي. ويتم التسويق للعديد من تلك الخدمات بأنها 'مجانية' ولكن في الواقع استخدام تلك الخدمات يتطلب الدفع على شكل معلومات شخصية من العملاء. في الاقتصاد الرقمي تمثل المعلومات الشخصية من الأصول غير الملموسة ذات القيمة الكبيرة ، وتعتبر كعملة في العالم الرقمي تستخدم في تبادل الخدمات عبر الإنترنت.
- عززت المعلومات الشخصية النمو المطرد في الاقتصاد الرقمي. عليه، ينبغي أن يكون للمستهلكين القدرة على التمتع بحصة أكثر عدلاً من ثمار هذا النمو. تقدم حماية البيانات فرصة فريدة لمنح الأفراد الأدوات اللازمة لحماية أنفسهم وجعل تطبيق قواعد المنافسة العادلة وحماية المستهلك أكثر فعالية.

١١ - المراجع

- أ. الحكومة الاستراتيجية، المبادئ التوجيهية لإدارة أمن المعلومات ، ٢٠١٤، الرابط < <http://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationssystem.pdf>
- ب. الاتحاد الدولي للاتصالات ، قطاع التقييس، Y.3600 ، متطلبات وقدرات للبيانات الضخمة المعتمدة على الحوسبة السحابية " ، ٢٠١٥/١١ ، الرابط < https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3600-201511-I!!PDF-E&type=items
- ت. المفوضية الأوروبية ، وثيقة حماية البيانات في الاتحاد الأوروبي والبيانات الضخمة، ٢٠١٥/٤ ، الرابط < http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf
- ث. OECD 2008 ، توصية منظمة التعاون الاقتصادي والتنمية في المجلس من أجل الوصول المحسن واستخدام أكثر فعالية للمعلومات القطاع العام، 36 (2008) C ٢٠ أكتوبر ٢٠١٢ ، < <http://www.oecd.org/sti/44384673.pdf>