ARID Journals

ARID International Journal of Social Sciences and Humanities (AIJSSH)

Journal home page: <http://arid.my/j/aijssh>

مَجَلَّةُ أُرِيدَ الدَّوْلِيَّةُ لِلْعُلُومِ الْإِنْسَانِيَّةِ وَالْإِجْتِمَاعِيَّةِ

المجلد الثالث، العدد الخامس، كانون الثاني 2021 م

Data Protection Laws & Ways to conformity

Radwan Eshkita

Personal Data Protection Laws- Erasmus University -Germany

قوانين حماية البيانات الرقمية وسبل التوافق معها

رضوان اسخيطه

تخصص في قوانين البيانات الشخصية- جامعة ERASMUS- المانيا

radwanesk@gmail.com

arid.my/0004-6263

<https://doi.org/10.36772/arid.aijssh.2021.353>

ARTICLE INFO

Article history:

Received 10/06/2020

Received in revised form 07/08/2020

Accepted 09/09/2020

Available online 15/01/2021

<https://doi.org/10.36772/arid.aijssh.2021.353>

ABSTRACT

This Research – Data Protection Laws and Ways to Conformity – talked about the data protection laws in Arabic countries and take the general data protection regulation as research main example. The main purpose of that is to show which point has developed the GDPR and to make a comparison with the legal situation in Arabic countries, the UAE was used as the main example of the Arabic countries in this research due to the advanced development level in technical and legal fields. This research uses mainly the books, electronic contribution and online guides as references and use the comparison as main research method.

The new points in the European laws and the expanding of GDPR application to every country in specific cases related to the main discussion points in this research.

The research comes to the results with recommendations about the best ways to be conform with the protection laws and the features behind this conformity.

Keywords: Data Protection, GDPR

الملخص

يتحدث البحث القانوني - قوانين حماية البيانات الرقمية وسبل التوافق معها - عن القوانين المتعلقة بحماية البيانات في الدول العربية ويأخذ اللائحة الأوروبية لحماية البيانات GDPR كمثال رئيسي للبحث ويبحث واقع قوانين حماية البيانات في الدول العربية مع التركيز على دولة الإمارات العربية المتحدة كمثال رئيسي عن الدول العربية لما فيها من تطور تقني وقانوني متميز.

هذا البحث يستخدم طريقة البحث المقارن والمراجع المختلفة المصادر الإلكترونية والورقية للوصول إلى النتائج باستخدام طريقة المقارنة ومناقشة نقاط الضعف والقوة في هذه القوانين.

يتضمن مسار هذا البحث مناقشة النقاط الجديدة في القوانين وعمل تقييم للقوانين الحالية في الدول العربية وتسليط الضوء على النقاط المتميزة في القوانين الأوروبية وكيفية الاستفادة منها في تطوير القوانين المحلية. كما يعتبر امتداد تطبيق اللائحة الأوروبية إلى كافة الدول في حالات معينة أحد الأمور الأساسية التي درسها هذا البحث وأعطى توصيات بخصوص كيفية الوصول للتوافق مع قوانينها والاستفادة من الحماية التي توفرها هذه القوانين.

الكلمات المفتاحية: البيانات الرقمية، اللائحة الأوروبية لحماية البيانات

1. مقدمة

أول ما يتبادر للذهن في معرض الحديث عن قوانين حماية البيانات هو الغاية الرئيسية من سن هذا النوع من القوانين. من خلال مقولة "المعلومات هي سلطة" نستطيع استشفاف أهمية وجود المعلومات في أيادي قد تسيء استعمالها، هذا ينطبق على بشكل رئيسي على البيانات الشخصية للمواطنين وغيرها من البيانات التي يجب حفظها بشكل يحول دون الوصل العاث إليها وسن قوانين لحمايتها ومعاقبة من يسيء استخدامها.

تتنوع المجالات التي تشملها قوانين حماية البيانات والمعلومات الشخصية ما بين حماية للبيانات الشخصية المخزنة إلكترونياً أو حماية المعلومات الموجودة لدى الحكومات والمنظمات لكي لا تكون وسيلة ضغط على الأفراد حيث لا بد من وجود ضوابط لاستعمالها ضمن الإطار التي تم جمعها لأجله، كما تمتد قوانين حماية البيانات لتشمل طريقة التعامل مع هذه البيانات من خلال حصر جمع البيانات أو معالجتها بأغراض تتماشى مع الغرض منها وبالحد الذي يمكن معه استعمال البيانات لأغراض تتعلق بالمصلحة العامة أو مصالح أصحاب البيانات. وتمتد القوانين لتعطي شروط مسبقاً من الناحية التقنية والأمنية لمنع حدوث أي اختراق أو لتقليل نسبة إمكانية حدوث انتهاك لهذه البيانات وذلك من خلال وضع معايير سلامة تقنية وأمنية لتضمن من خلال الحد المطلوب من الأمن لكل من يقوم بتخزين ومعالجة بيانات تتعلق بأشخاص قد يؤدي وصولها إلى أيادي غير آمنة إلى نتائج تهدد أمن وحرية وكرامة الأشخاص أصحاب البيانات.

مع التطور التكنولوجي الهائل ازدادت أيضاً كمية البيانات التي يتم جمعها وأصبحت تقنيات التخزين أكثر عرضة للاختراق نتيجة الحاجة للتخزين في خدمات خارجية نظراً لعدم إمكانية التخزين المحلي دائماً مع التضخم الكبير في استعمال التكنولوجيا وما نتج عنه من تبعات من دخول التكنولوجيا لكافة تفاصيل الحياة كما هو الحال في أنترنت الأشياء والذي يجعل كل مناحي الحياة والنشاطات المنزلية والتجارية عبارة عن بيانات تتم إدارتها في خدمات خارجية ليتم تقديم الخدمات المناطة بهذه التكنولوجيا بناء على النحو المناسب وبالتالي ازدياد كمية البيانات وأنواعها وازدياد الحاجة لتكون هذه البيانات في مأمن من وقوعها في اليد الخطأ. هذا الأمر في الوقت ذاته أمل على القوانين الخاصة بحماية البيانات أن تسن عقوبات رادعة لكل من لا يلتزم بمعاييرها والتزاماتها ولم تعد هذه القوانين كما كانت في البداية مجرد توصيات أو تعليمات ذات صفة إرشادية وإنما قوانين بالمعنى الصحيح للكلمة تلزم من يخالفها بعقوبات مالية جزائية كبيرة ولها القوة الزجرية الكافية لتحرك الدعاوى أمام أروقة المحاكم من خلال كم من يدعي تضرر حقوقه المحمية بموجبها وأصبحت في بعض الدول أحد فروع القانون ويتم تطويرها باستمرار لتتماشى مع التطور الهائل والسريع الحاصل في التكنولوجيات المستخدمة في هذا

المجال ولتكون مواثية لدرجة التقدم الحاصل في النشاطات والاستخدامات التي من المفترض أن تتم حمايتها من خلال هذه القوانين.

لم يقتصر الموضوع على سن قوانين محلية ملزمة بل تطورت الأمور لعمل إطار قانوني ملزم يشمل كافة الدول التي تنضوي تحت إطار مشترك كما هو الحال في اللائحة العامة لحماية البيانات الشخصية GDPR والتي شملت كافة دول الاتحاد الأوروبي وتم اعتبارها ملزمة لكافة الدول الأعضاء وتعدت لتكون نافذة في كثير من الأحوال مكان القوانين المحلية الخاصة بهذا الشأن في ظل التطلعات بأن تحذو التكتلات الدولية حذو الاتحاد الأوروبي في مجال سن قوانين تشمل اتحادات دولية تنضوي تحتها عدة دول في سبيل حسن تطبيق هذا النوع من القوانين كون المعلومات لها خاصية التنقل اللحظي بين كافة أرجاء المعمورة مما يستدعي وفي حالات شتى شمولية هذه القوانين وعدم محدوديتها بإقليم أو دولة محدد مما يجعل من تطبيقها في النزاعات بين الدول مربكاً من الناحية القانونية وتوحيد القوانين وتعميمها في هذا الشأن يوفر حماية أكثر مرونة وفعالية.

هذه الخصوصية المميزة التي تتمتع بها المعلومات من حيث لحظية الانتقال وخضوعها من حيث الاختصاص المكاني لعدة قوانين في الوقت ذاته يجعل القوانين النازمة لها ذات طبيعة خاصة تتطلب معايير مختلفة عن القوانين التقليدية وخصوصاً في معرض تطبيقها على قضايا تتعلق بدول متعددة تتعدد فيها التشريعات والتفاصيل القانونية المطبقة عليها. مما يجدر ذكره بالإضافة إلى ذلك كون الدساتير عموماً تشمل قواعد عامة تُجرم الأفعال الضارة عموماً مما يجعل القوانين الأساسية بما فيها القوانين المدنية ملجأً للمتضررين بقضايا حماية البيانات في حال غياب تشريعات مخصصة لحماية الجرائم المتعلقة بالمعلومات.

وتُعرف المعلومات الشخصية أحد أهم أنواع المعلومات التي تهدف التشريعات لحمايتها حسب المادة الرابعة من اللائحة الأوروبية GDPR بأنها البيانات الخاصة بالشخص كالاسم والعنوان ورقم الهاتف ورقم لوحة السيارة أو عنوان الأي بي الخاص بالكمبيوتر والذي من خلاله يمكن معرفة الشخص الذي يستخدمه وذلك على سبيل المثال لا الحصر.

وفقاً للوقائع التي تم سردها حول قوانين البيانات، سيتم في هذا البحث التطرق لبحث ماهية قوانين البيانات ومجالات الحماية التي تهدف إليها بالإضافة إلى ذلك لعمل نظرة مقارنة على القوانين الصادرة في البلدان العربية وعمل مقارنة مع أهم التشريعات العالمية المتعلقة بحماية البيانات والمعلومات. مخاطر ضياع البيانات والأخطار المحدقة بها ستكون أحد النقاط الرئيسية لهذا البحث. سيبحث العمل بشكل رئيسي في التقنيات المقترحة للمساعدة في تطبيق القوانين المتعلقة بحماية

البيانات وكيف لهذه التقنيات أن تجعل من تطبيق هذا النوع من القوانين ممكناً وأكثر جدوى، كما أن البحث سيُعنى بتطبيق القوانين العالمية خارج إطار الدول التي أصدرتها ومدى جاهزية الدول في العالم العربي لها، اقتراحات وتوصيات بخصوص تطوير القوانين الخاصة بالبيانات والمعلومات في الدول العربية سيتم العمل من خلال هذا البحث للوصول إليها وذلك من خلال تحليل المعطيات الواردة معنا.

1.1 هدف البحث:

يهدف البحث إلى تسليط الضوء على قوانين أمن وحماية المعلومات الرقمية من خلال تسليط الضوء على هذه القوانين في أوروبا وخصوصاً اللائحة الأوروبية لحماية البيانات الشخصية الصادرة وفهم ماهيتها بغرض مقارنتها مع واقع القوانين في الدول العربية وتوضيح أهمية الميزات الجديدة والاستفادة من تجارب الغير في تطوير القوانين المحلية. من أهداف هذا البحث أيضاً دراسة تأثير تطبيق القوانين الغربية وبشكل خاص اللائحة الأوروبية لحماية البيانات على أرض الواقع في الدول العربية حيث تمتد هذه القوانين لتُطبق في بلادنا العربية في حالات معينة حسب الاختصاص المكاني الموسع وبالتالي لابد من دراسة هذا التأثير لضمان التوافق مع أحكامها وتجنب الشركات والهيئات الحكومية تبعات مخالفتها لهذه القوانين وما يترتب على ذلك من عقوبات. ضمن هذا البحث سيتم دراسة خطوات وإرشادات تساهم في تسهيل عملية التوافق مع قوانين حماية البيانات الأوروبية وتفتح الباب أمام استخدام هذه الأدوات في إطار تطوير الهيكلية القانونية لقوانين حماية البيانات المحلية.

يبدأ هذا البحث بإلقاء نظرة على قوانين حماية البيانات الرقمية في الدول العربية ودولة الإمارات العربية المتحدة مثلاً ويبحث بعدها في اللائحة الأوروبية لحماية البيانات وتأثيرها داخل وخارج حدود دول الاتحاد الأوروبي كما يبحث أفضل السبل للتعاطي والتوافق مع القوانين الأوروبية لحماية البيانات. المسؤوليات في عالم قوانين حماية البيانات هي من النقاط الهامة في هذا البحث وسوف يتم التعرض لشروط وآليات نقل البيانات عبر الحدود بين الدول المختلفة.

تم اتباع طريقة البحث المقارن مع استخدام أمثلة بحثية رئيسية لإسباغ الطابع العملي والواقعي على البحث كما تم استخدام مراجع مختلفة المصدر تشمل الكتب والمقالات الإلكترونية والكتب الإرشادية الإلكترونية بالإضافة لأحكام المحاكم والهيئات المشرفة. هذا النوع من المصادر يناسب موضوع البحث حيث أن البحث يتجه ليكون إرشادي أكثر منه استقرائي ولا يتبع طريقة المقابلات والإحصاءات كون قوانين حماية البيانات مازال فتية في الدول العربية والبحث باستخدام الأبحاث والكتب المرجعية يعطيه بعداً توجيهياً ويناسب طبيعته المقارنة.

إن أهمية هذا البحث كذلك تكمن في كون قوانين حماية البيانات مائزلة فتية في بلادنا العربية، وإن نظرة ودراسة مقارنة مع القوانين الأوروبية الراءدة في هذا المجال تعتبر خطوة بحثية في الطريق نحو تطوير القوانين المحلية.

2. نظرة على قوانين المعلومات

2.1 القوانين في البلدان العربية - دولة الإمارات مثلاً

تشتمل الدساتير العربية شأنها شأن الدساتير معظم الدول في العالم على المبادئ الأساسية لحفظ الحقوق الأفراد ولكن بشكل محدود إذا ما قارنتها مع الدساتير في الدول الأوروبية على سبيل المثال، حيث إن غالبية دساتير التسعينات في الدول الأجنبية تضمنت نصوصاً واضحة وصريحة بشأن حماية البيانات الشخصية وحرية المعلومات بشكل صريح على نحو يمنع انتهاكها بالإضافة للحق في حماية البيانات الشخصية وتقييد أنشطة جمعها ومعالجتها واستخدامها على نحو يوفر حماية للأفراد من مخاطر تقنية المعلومات مع ورود تقييد في بعض الحالات وفقاً لاعتبارات المصالح الوطنية للدولة وحقوق الأفراد.[1] هذه الحقوق الدستورية الرقمية إن جاز التعبير غابت حتى وقت قريب عن الكثير من الدساتير في بلادنا العربية.

أما الحماية الواردة في بعض الدساتير على هذا الصعيد كانت تتعلق ببعض الحقوق الخاصة بالتواصل كحرمة المراسلات أو سريتها حيث وردت قيود على الإطلاع عليها في حدود القانون كما هو الحال في الدستور الأردني على سبيل المثال في مادته 18.

لتدارك ذلك ثمت هناك محاولات أحياناً مجدية وأخرى مائزلة في طور التحضير للحق الركب العالمي في مجال سن قوانين تُعنى بحماية المعلومات والبيانات الشخصية أسوةً بالدول المتقدمة في هذا المجال، هذه التجارب أثمر بعضها في إصدار قوانين تختص بحماية المعلومات بشكل رئيسي كما هو الحال في إصدار قانون حماية البيانات الشخصية الخاص بمركز دبي المالي؛ والذي يشمل تطبيقه المركز بشكل رئيسي والمتعاملين معه وكذلك في قانون حماية البيانات الشخصية في قطر الصادر عام 2016،[2] ووصل لمراحله النهائية في البحرين ويشتمل مشروع قانونه على 60 مادة تنقسم إلى باب يتضمن أحكام المعالجة، وباب ثان حول هيئة حماية البيانات، والثالث بعنوان مساءلة مدير البيانات ومراقب البيانات.[3] فيما لم يتم العمل على هذا النوع من القوانين مطلقاً في دول أخرى كثيرة واقتصرت الحماية على القانون المدني وفقاً للمبدأ الشهير "كل خطأ سبب ضرر للغير فيلزمه التعويض".

كمثال بحثي سنأخذ القوانين في دولة الإمارات العربية المتحدة حيث لم يكن هناك قانون بالمعنى الحقيقي لحماية البيانات الشخصية وتم بداية إصدار قانون حماية البيانات الشخصية الخاص بمركز دبي المال [4] صدر هذا عام 2007 وكان تلبية لحاجة المتعاملين الدوليين مع المركز لضمان حسن تعاطي المركز مع بيانات المتعاملين معه وذلك في ضوء غياب وجود قانون محلي ينظم هذا الأمر وتضمن النص على حماية جميع البيانات الشخصية، بما فيها البيانات الحساسة ونقل وتداول البيانات، وفقاً لأحكام وتوجيهات الاتحاد الأوروبي. يقوم بمهام حماية البيانات وفقاً لهذا القانون مفوض لحماية البيانات ويتولى إرساء نظام فاعل للحماية وفرض إجراءات قانونية صارمة ضد إساءة استخدام البيانات الشخصية [5].

من حيث المبدأ يضمن الدستور الإماراتي حرية التواصل والمراسلة بالبريد ووسائل التواصل المختلفة وحماية البيانات التي تتضمنها هذه المراسلات في المادة 31 منه وفي حال حدوث خرق لهذا الحق الذي ضمنه القانون يمكن للمتضرر اللجوء للقانون المدني. يعاقب القانون المدني الإماراتي لعام 1985 خرق الخصوصية في المادة 5 ويعطيه الحق في إيقاف هذا الخرق وفي التعويض. من المهم في القانون المدني الإماراتي كونه يُجرّم حتى الأفعال التي تؤدي إلى ضرر في السمعة أو الخصوصية وإن لم يكن هذا الضرر ملموساً كالجرح أو القتل إنما يكفي حصول فعل أدى إلى ضرر ليتم تجريمه [6].

أما القانون الجزائي لعام 1987 فينظر إلى حماية الأشخاص من إفشاء بياناتهم الشخصية من خلال المادة 3 على أنها حق يجب حمايته ويعاقب على فعل إفشاء وانتهاك خصوصية بيانات الأشخاص على أنها فعل مُجرّم وخصوصاً في حال إفشاء المعلومات المتعلقة بحياة الأفراد الخاصة وتصل العقوبة إلى الحبس مع الغرامة في بعض الحالات للفاعل الذي يفشي بيانات تتعلق بنشر بيانات شخصية لآخرين عبر الصحف العامة أو اختراق أسرار الحياة الأسرية الخاصة للأشخاص [6].

صدر أيضاً في عام 2006 قانون حماية التجارة الإلكترونية والذي يحمي من حيث المبدأ كافة التعاملات التجارية بين الأفراد ومن بينها البيانات المتعلقة بهم في معرض هذه التبادلات التجارية. بالإضافة إلى ذلك صدر قانون الجرائم الإلكترونية عام 2012 والمتعلق بالجرائم الإلكترونية وإساءة استخدام البيانات والمعلومات المتناقلة إلكترونياً. ضمن هذا القانون تقع البيانات التي تخص الأفراد على شبكات المعلومات تحت حمايته ويعتبر كل من يفشي معلومات من خلال المواقع الإلكترونية أو الشبكات الحاسوبية بدون تصريح أو سبب قانوني مرتكباً لفعل مجرم قانونياً [6].

بالإضافة إلى ذلك يتولى القانون رقم 26 لسنة 2015 المتعلق بتنظيم نشر وتبادل البيانات في إمارة دبي حماية بيانات المتعاملين تحت إشراف مؤسسة بيانات دبي. يُطبق هذا القانون من حيث الاختصاص النوعي على الجهات الحكومية الاتحادية التي تتوفر لديها أية بيانات تخص الإمارة وعلى الأشخاص الذين يمتلكون أو ينشرون أية بيانات تخص الإمارة

لتمكين إمارة دبي من إدارة البيانات وفق منهجية واضحة ومحددة والاستفادة المثلى من البيانات المتوفرة لدى مزودي البيانات، بالإضافة إلى تعزيز الشفافية وزيادة كفاءة الخدمات التي تقدمها الجهات الحكومية.[7]

كما تم وضع معايير لنشر وتبادل بيانات دبي بواسطة المنصة الإلكترونية تتضمن قواعد ووسائل الحماية التقنية الخاصة بأنظمة المعلومات وشبكات الحاسب وفرضت المادة 11 من القانون على الجهات المتعاملة مع البيانات الحكومية تعديل بنيتها التحتية من أجهزة وأنظمة معلومات لضمان نشر وتبادل بياناتها إلكترونياً بشكل آمن مع فرض عدم المساس بقواعد سرية البيانات أو بحقوق الملكية الفكرية كما أضافت المادة 10 التزامات تتعلق بفرض تجهيزات وبنى تحتية آمنة للمنصات الإلكترونية التي تتعامل مع البيانات الحكومية.

بالرغم من كونه قانون يشمل عدداً من الأنظمة المشابهة لما هو عليه في قوانين الدول الأوروبية النازمة لحماية البيانات كالمواد التي تتضمن التزامات بتوفير بنى تحية آمنة لضمان أمن البيانات، إلا أنه لا يعتبر كافياً في ظل غياب تشريع متكامل يضمن حقوق الأفراد على بياناتهم. هذا الرأي كان أيضاً لشركة التميمي للقانون التي انتقدت غياب تشريع مستقل أسوة بالدول الغربية واعتبرت أن قانون تنظيم وتبادل المعلومات يهدف بالدرجة الأولى لتنظيم تبادل البيانات المخزنة في الدوائر الحكومية لضمان حسن تسيير واستخدام هذه البيانات ولا يمثل قانوناً حافظاً لحقوق الأفراد على بياناتهم الشخصية.[8]

في ضوء هذه المطالبات تم إعداد مشروع قانون من قبل الهيئة العامة لتنظيم قطاع الاتصالات في الإمارات العربية المتحدة لحماية البيانات الشخصية للمستخدمين سيصدر قريباً.[9]

2.2 القوانين في البلدان الأوروبية - اللائحة الأوروبية لحماية البيانات GDPR مثلاً

سادت الدول الأوروبية بمعظمها وخصوصاً الغربية منها قوانين محلية تحكم مسألة حماية البيانات فكان هناك قانون حماية البيانات الشخصية للولايات الألمانية المسمى اختصاراً BDSG ويسري على كافة الولايات الألمانية ويتم تطبيقه من خلال المحاكم المحلية. كان ذلك الحال كذلك في دول أوروبية أخرى داخل الاتحاد الأوروبي مثل فرنسا وإيطاليا ويتولى الاتحاد الأوروبي عبر توجيهاته الصادرة عن البرلمان والمفوضية الأوروبية تنظيم التعاطي مع القوانين المختلفة بين الدول في حالات تطبيق أكثر من قانون وإعطاء تعليمات إرشادية. التوجيهات الإرشادية 95/46/EC والصادرة في 25 تشرين الأول 1995 عن المفوضية الأوروبية هي توجيهات تهدف لحماية البيانات الشخصية وتهدف لتسهيل تبادل البيانات بين دول الاتحاد الأوروبي وحماية البيانات الشخصية في الوقت ذاته من سوء الاستخدام خلال هذا الانتقال.

تُطبق هذه الإرشادات على المعلومات التي يتم معالجتها أوتوماتيكياً كما هو الحال في المخدمات وأجهزة الحاسوب، كما تطبق على المعلومات المخزنة يدوياً بشكل ورقي أو ما شابه ويخرج من نطاق تطبيقها كافة البيانات الشخصية التي تستخدم ضمن الإطار المنزلي أو تستخدم لأغراض تخدم المصلحة العليا للدولة [10] بالرغم من التعديلات المتتالية التي تمت على هذه التوجيهات الإرشادية الأوروبية فإن الحاجة أضحت ملحة لللائحة القانونية لها صفة الإلزام تحل محل القوانين المحلية وتنظم مسألة تناقل البيانات وحمايتها بشكل أكثر شمولية، هذا الأمر تطلب عدة سنوات تخطتها إصدار توجيهات لاحقة كما هو الحال في 2016/680 (EU) وهو التوجيه السابق لصدور اللائحة الأوروبية لحماية البيانات GDPR. هذه اللائحة التي صدرت في 25 أيار 2016 أعطت مدة سنتين من تاريخ صدور ما كفترة سماح ليتسنى للشركات والحكومات الاستعداد لتطبيق قوانينها وبدأت في 25 أيار 2018، هذه اللائحة هي نقلة في قوانين الأكبر خلال العشرين سنة الأخيرة في مجال قوانين حماية المعلومات والبيانات الشخصية، [11] هذه اللائحة جاءت بالكثير من التشريعات والتطبيقات الجديدة والتي تعتبر تطويراً مهماً لقوانين المعلومات وحمايتها كونها ثمرة جهود المشرعين في دول الاتحاد الأوروبي لسنوات طويلة.

جاءت اللائحة بتغييرات وابتكارات جديدة بداية مع المادة الثالثة في الفقرة الأولى والتي تتناول متى اللائحة تطبق مكانياً على الشركات التي تقع فروعها ضمن دول الاتحاد الأوروبي في معرض ممارستها لنشاطها وعادت الفقرة الثانية لتضيف ما يعرف بمبدأ التسويق ويقضي هذا المبدأ بأن يُطبق هذا القانون في حال كانت هناك عملية جمع للبيانات الشخصية متعلقة بتوريد سلع أو خدمات وعليه فإن تطبيق اللائحة المكاني يُطبق على الشركات التي لها فروع في بلدان الاتحاد الأوروبي أو تمارس نشاط تسويقي متعلق بسلع أو خدمات في هذه الدول. وتطبق اللائحة كذلك خارج الاتحاد الأوروبي في حال كان هناك جمع أو معالجة لبيانات مواطنين من الاتحاد الأوروبي ولا يمكن الاتفاق على ما يخالف ذلك عقدياً. [12]

هذا الإدخال الجديد في اللائحة وسّع نطاق تطبيقه ليشمل كل مكان في العالم تمت فيه معالجة بيانات لأشخاص من سكان الاتحاد الأوروبي وهذا الذي جعل الشركات عموماً في حالة تأهب واستعداد وتحضير للتعامل مع اللائحة الجديدة ولو كان مقرهم خارج دول الاتحاد الأوروبي مادام عملها يتعلق بمعالجة بيانات تخص أشخاصاً أوروبين. حسب الفقرة الثانية من المادة الثالثة تأتي لتوضح كيف أن معالجة البيانات تعني المعنى المطلق للكلمة وهو كل ما يمس البيانات من جمع وتعديل ونشر وتبادل. الهدف الرئيسي وراء هذا التوسع هو توفير حماية أوسع لمواطني الدول الأوروبية من أن يُساء استعمال بياناتهم ولو خارج دول الاتحاد. [13]

من حيث الغرض، تم توسيع القيود على الغرض من استعمال البيانات وربط الاستعمال بالغرض الذي تم الجمع لأجله، حيث ألزمت المادة الخامسة والعشرون مراقب البيانات بالتأكد من الغرض من جمع البيانات والتدابير التقنية المتخذة لحماية البيانات للتأكد من كونها آمنة بشكل كافٍ وضمان عدم إمكانية الوصول غير الآمن لها.

من النقاط المهمة التي طرحتها اللائحة هي إلزامية تقييم التبعات، يقوم المبدأ على فكرة أن الدائرة الحكومية أو الشركة التي تنوي القيام بأعمال التي من شأنها جمع بيانات شخصية عن الأفراد أن تقوم حسب المادة 35 من اللائحة بعمل تقدير للتأكد فيما إذا كانت الطريقة التي يتم فيها جمع البيانات ومعالجتها وخصوصاً باستخدام التكنولوجيا الحديثة تشكل خطراً على حرية وحقوق وسلامة البيانات الشخصية.

فرضت كذلك اللائحة إلزاماً كان موجوداً سابقاً في القوانين المحلية لبعض الدول ولكن تم فرضه الآن بشكل مختلف الآن حيث تكون الجهة المعالجة للبيانات مسؤولة عن الإبلاغ عن أي خرق أو تسرب في البيانات للشخص موضوع البيانات وللجنة المشرفة على حماية البيانات في المدينة أو الإقليم الذي حدث فيه الخرق، هذا الإبلاغ يجب أن يكون خطياً إلكترونياً أو ورقياً خلال 72 ساعة من حدوث هذا الخرق.

الحق في حذف البيانات هو النص الذي جاءت به المادة 17 والذي يعطي الحق للشخص الذي تمت جمع بياناته بطلب حذفها في حال انتهى الغرض من استعمالها، هذا الحق يعتبر من النصوص الصارمة في اللائحة والذي تم إعطاء الأفراد سلطة من خلاله تمكنهم من حذف بياناتهم من أي مكان طالما انتهى الغرض منها. إن وضع هذا النص في التنفيذ يُشكل تحدياً تقنياً أيضاً للحكومات والشركات كونه يتطلب آلية تقنية تُمكن معالج البيانات من الاستجابة لطلب صاحب البيانات بحذف بياناته في الوقت المطلوب وفي حال كانت البيانات المخزنة ضخمة للغاية كما هو الحال في شركات التخزين السحابي أو الدوائر الحكومية التي تحوي ملايين السجلات من هذه المهم قد تكون شبه مستحيلة إلا في حال تم وضع أسس تقنية ملائمة تقوم بهذا العمل بالشكل والوقت الملائمين بشكل تلقائي. [14]

إن العقوبات التي جاءت بها اللائحة تعتبر صارمة وكبيرة وهذا يستدعي الوقوف طويلاً قبل التفكير في عدم احترام قوانينها حيث إنها تبلغ في بعض حالات الانتهاك 4% من قيمة المبيعات السنوية أو 20 مليون يورو أيهما أعلى حسب المادة 83 من اللائحة. [12]

2.2.1 تأثير اللائحة خارج الاتحاد الأوروبي:

إن التعديلات والمفاهيم الجديدة التي قدمت مع اللائحة الأوروبية جعلت الحكومات والشركات تعيد النظر بسياساتها تجاه المعلومات الشخصية للأفراد والتعامل معها، وقامت فعلياً الكثير من الدول بتغييرات جذرية تشمل البنى التحتية والأنظمة الداخلية وآليات التعامل مع تخزين البيانات بما يتماشى مع السياسات الجديدة لللائحة الأوروبية وهذا يقع على عاتق هذه الحكومات والمنظمات في جميع أرجاء العالم كون الاختصاص المكاني يمتد إليهم في حالات معينة وردت آنفاً. [15] فقيام شركة تسويقية في دولة الإمارات العربية المتحدة بمراقبة سلوك الزبائن المتواجدين في أحد دول الاتحاد الأوروبي بغرض معرفة اتجاهاتهم السلوكية في التسوق وتحليلها يعتبر معالجة لبياناتهم ويتطلب الامتثال لقوانين اللائحة الأوروبية بالرغم من عدم وجود الشركة بالمطلق ضمن الاتحاد:

أحد التحليلات التي صدرت خلال الفترة القصيرة بعد نفاذ اللائحة الأوروبية تحدثت عن توصيات معنية كطريقة للاستعداد للتعامل معها ولتجنب الإشكاليات المترتبة على مخالفة اللوائح والتعرض للغرامات. هذه التوصيات تتلخص في عدو نقاط منها تثقيف الموظفين الذين يمكن أن يكون لهم تعاطي مع معالجة البيانات، هذا الأمر يتطلب توضيح المقصود بالبيانات الشخصية وطريقة التعامل معها وطرق تجنب الوقوع في خروقات لمواد اللائحة. كذلك فإن القيام بوضع تجهيزات وخطط تمكن الجهات المعالجة للبيانات من وضع إجراءات وبروتوكولات لحماية هذه البيانات يعتبر أساسياً لضمان حظر الوصول غير المسموح للبيانات المحمية بموجب هذا القانون. [16]

كذلك فإن الواجبات الجديدة التي أملتتها اللائحة على معالجي البيانات كحق الشخص موضوع البيانات في حذف بياناته تعتبر واجبات مجهدة للجهة التي تعالج البيانات وبدون وضع آليات أو توماتيكية ومنظمة لا يمكن لهذه الجهات أن تلبى متطلبات هذه اللائحة. كما إن واجب الإثبات الملقى على الجهة معالجة البيانات بإثبات مدى استعدادها تقنياً وأمنياً لمعالجة البيانات بشكل آمن وثابت يتطلب أن تكون لدى الجهة المعالجة للبيانات آليات تقوم بتسجيل ومراقبة الأنظمة المخزنة عليها هذه البيانات حسبما ورد في المادة 32 من اللائحة حيث تنص على سلسلة من الإجراءات التقنية والتنظيمية والتي تشترط اللائحة اتباعها للوصول لمعالجة آمنة ومتوافقة مع قواعدها.

من المهم لكل دائرة أو شركة تعالج بيانات شخصية أن تتوخى الحذر بشأن الحصول على موافقة الشخص موضوع البيانات خصوصاً في حال معالجة البيانات ذات الطبيعة الحساسة مثل البيانات عن العرق والجنس والحالة الصحية، هذا الموضوع تم تناوله في المادة التاسعة من اللائحة واشترط موافقة صريحة وحالات محددة يتم السماح بها بمعالجة هذا النوع من

البيانات، لذلك على كل من يتولى معالجة هذا النوع من البيانات مراعاة شروط الموافقة من صاحب البيانات لتفادي العقوبات الصارمة في هذا المجال. إن تعيين مكلف بحماية البيانات على دراية بالقوانين النافذة يعتبر ضرورة في حالات كثيرة خصوصاً في الشركات الكبيرة أو التي تتعاطى مع البيانات الشخصية والحساسة بشكل كبير، هذا المكلف يجب أن يكون بارعاً في إدارة عمليات تكنولوجيا المعلومات وأمن البيانات ولديه فهم لآليات الامتثال القانوني لقوانين ولوائح حماية البيانات حسب ما أورده المادة 28 في حديثها عن مهام مراقب البيانات.

تفيد الدراسة نفسها إلى أنه بالرغم من التحذيرات بوجوب إجراء تعديلات لملائمة الأنظمة مع اللائحة فإنه لا تزال حوالي 60 بالمئة من الشركات لم تقم بالإجراءات اللازمة لضمان توافقيتها مع اللائحة الأوروبية، هذا يفتح الباب أمام التساؤل عن فرص حصول الأسواق التي لا تلتزم شركاتها بقوانين اللائحة على فرص تجارية مع دول الاتحاد الأوروبي، حيث إنه من المستبعد حسب قوانين الاتحاد الأوروبي التعامل أي شركة خارج دول الاتحاد مالم تكن هناك معايير تحددها المفوضية الأوروبية وتراقبها باستمرار وتعطي السماح بناء على هذه المراقبة أو الرضا بالتعامل أو نقل البيانات إلى أراضي الدول خارج الاتحاد. هذا الموضوع من أكثر المواضيع إثارة للجدل فيما يخص آلية نقل البيانات لدول خارج الاتحاد في حال لم تكن على المستوى المماثل من التجهيز والاستعداد كما هو مطلوب في اللائحة الأوروبية. [17]

2.2.2 تأثير اللائحة الأوروبية لحماية البيانات داخل الاتحاد الأوروبي:

من المؤكد أن التشريعات الأوروبية الجديد الخاص بحماية البيانات جاء للحد من الاستخدام غير المقيد لبيانات الأفراد والحد من سلطة الخدمات الرقمية التي باتت تستخدم البيانات الشخصية في الترويج لمنتجاتها دون قيود حقيقية في ظل القوانين السابقة.

ففي ظل العقوبات المالية الفوق اعتيادية التي جاءت بها اللائحة الأوروبية، بدأت الشركات الكبيرة بمشروع التوافقية مع اللائحة وتم إعداد خطط بحيث تكون جاهزة مع موعد التطبيق في أيار 2018، هذه الخطط شملت تغييراً جذرياً في البنية الأساسية للأنظمة وكذلك تغييراً جذرياً في طريقة التعامل مع الأفراد حيث إن مبدأ وافق أو اترك لم يعد مسموحاً به ضمن قوانين اللائحة التي سيعمل بها وحقوق الأفراد في الوصول لبياناتهم وحذفها أصبحت ضمن الخيارات المتاحة لكل مستخدم، وأحد الأمثلة المهمة في هذا المجال ماقامت به أحد شركات حماية المستهلك بمقاضاة غوغل لأن أحكام الموافقة الخاصة بها تعمل على مبدأ إقبل أو أترك وهذا يخالف مبدأ دعم مبدأ الشفافية في استخدام بيانات الأفراد. [18]

هذا الأمر بالطبع يضع الشركات تحت خيارين رئيسيين، إما البقاء في السوق والمنافسة والالتزام بقواعد اللائحة الأوروبية أو الخروج من السوق جزئياً أو كلياً وعدم الامتثال لها والوقوع في خطر التعرض لمخالفات مالية جسيمة.

أمام هذين الخيارين لم تتردد الشركات العملاقة في المثول لطلبات وقواعد اللائحة وها هي غوغل تُعلن أنها ستحذف من متجرها الإلكتروني للتطبيقات كل ما يخالف القوانين الأوروبية الجديدة ويساهم في نقل بيانات الأشخاص الشخصية إلى طرف ثالث كأحد أشهر الخروقات وأكثرها شيوعاً.

على النقيض قررت الكثير من الشركات المتوسطة الحجم والصغير الاستغناء عن تقديم خدماتها لمواطني دول الاتحاد الأوروبي وبالتالي لا تخضع تعاملاتها لقوانين اللائحة في مقابل تقليص نطاق نشاطاتها وحصره خارج الاتحاد الأوروبي.

وما بين الاثنين ماتزال بعض الشركات والعملاقة منها لم تُعدل كل ما يلزم وماتزال عرضة لعواقب مخالفة اللائحة الأوروبية وأحد الأمثلة الحية ماكتب عنه المحامي أرتود ميسود في فرنسا عن أن الموافقة على اتفاقية المستخدم الخاصة بتويتر تُخل بأهم شرط من شروط موافقة المستخدم ألا وهو أن تكون الموافقة اختيارية وإجبار تويتر مستخدميه على قبول الاتفاقية والتي تتضمن القبول بمعالجة البيانات من قبل طرف ثالث أو تعطيل الحساب في حال عدم الموافقة يُعتبر خرقاً واضحاً لأهداف اللائحة الأوروبية.

لكن بالرغم من ذلك، يعتقد "أرتور ميسود" محامي إحدى المنظمات الفرنسية المدافعة عن الحقوق والحريات الأساسية في العصر الرقمي أن الشركات الرقمية لن تلتزم من الناحية العملية بأحكام التشريع الأوروبي. ويُضيف رجل القانون، أنه مباشرة بعد بدء سريان اللائحة شرع موقع تويتر في عرض نافذة تطلب من المستخدم الموافقة على اتفاقية الاستخدام، وفي حال الرفض، ينقلك الموقع إلى صفحة تعطيل الحساب، وهو ما اعتبره المتحدث "موافقة تحت طائلة التهديد من نتائج سلبية".

هذا بالطبع يفتح الباب على التساؤل عن مستقبل الشبكات الاجتماعية والتي تُعنى بالمعلومات الشخصية بشكل خاص وخصوصاً بعد فضيحة العملاق فايس بوك والذي كان يستخدم بيانات عملائه في حملات ترويجية لشركات معلنة، ومع بدأ تطبيق اللائحة الأوروبية تراجع فوراً عن هذا الخرق وأعلن التزامه بسياسات اللائحة ولكن هذا الأمر حسب نظر الحقوقيين لن ينجح إلا في حال التوقف عن الإعلانات الموجهة كلياً.

إن التطبيق الحقيقي لللائحة الأوروبية سيحمي الأفراد من دون شك من سيطرة العملاقة الرقمية على بياناتهم الشخصية والعبث بها دون قيود ولكن شركات كبيرة أخرى ستتأثر جداً بقوانين اللائحة حيث إن سوق الإعلانات الرقمية لن يجد له طريق مع بدء تطبيقها. ذلك أن المادة 3 الفقرة 2 الفقرة الفرعية ب شملت ضمن قواعد الاختصاص المكاني كل من يقوم بمراقبة سلوك الأفراد أيضاً وجعلته يخضع لقوانين اللائحة وعليه على مقدمي الخدمات المتعلقة بتحليل ومراقبة سلوك

الأفراد الإلكتروني الاستعداد للعمل حسب القوانين الجديدة وهذا بالطبع يشمل عملاق تحليل تصرفات المستهلك Google Analytics .

هذا القيد سيرغم الشركات على تحويل توجهاتها وسيخلق سوق مفتوح غير محتكر كما هو الحال الآن من قبل الشركات العملاقة حيث إن زمن الخدمات المدفوعة لن يظل مصدر تمويل هذه الشركات وسيفتح الباب أمام إنشاء شبكات اجتماعية مفتوحة ولا مركزية.

من النقاط الجوهرية في اللائحة الأوروبية فرضها لزوم أخذ موافقة المستخدم في كل مرة يتم معالجة بيانات جديدة خاصة به، هذا يحد من إمكانية التلاعب التي كانت متوفرة سابقاً فجمع معلومات مثل الاسم والسن لتقديم خدمة معينة بعد موافقة المستخدم لا يعني الحق في جمع معلومات عن طريقة استخدامه للحاسب وميوله الشرائية ومكان تواجده، هذا بلا شك يفرض على الشركات تغيير أنظمتها ليظهر للمستخدم نوافذ جديدة تطلب منه الموافقة على كل تحرك جديد يخص جمع بيانات المستخدم لتتفادى الغرامات القاسية.

سيختفي أيضاً مع التطبيق العملي لللائحة الأوروبية الظاهرة المنتشرة حالياً والتي يتم فيها إرسال بيانات المستخدم لغايات تحليلية وإحصائية إلى مواقع مختلفة أخرى. هذا الأمر سيصبح مقيداً بذكر الجهة المرسل إليها ونوع المعالجة، فلن تستطيع شركة مايكروسوفت من خلال ضغطك للزر المشهور عند حدوث خطأ في نظام التشغيل أن ترسل بيانات من حاسبك لتحليل الخطأ دون الرجوع إليك وإخبارك بوجهة إرسال بياناتك.

هذا التشديد القانوني والأمني إن جاز التعبير جعل حتى العملاقة يقعون في متاهات المحاكمة والتعويضات فإن فايس بوك على سبيل المثال وبرغم الخطة الشاملة التي وضعها ونفذها لتتوافق سياساته وأنظمتها مع اللائحة الأوروبية يقف اليوم أمام المحاكم في قضايا مرفوعة ضده بقيمة مليارات الدولار بانتظار أن يتم حسمها. [19]

3. مفاتيح للتوافق مع قوانين المعلومات:

في ظل تزايد الهجمات الإلكترونية وازدياد الخطر من سرقة وضياع البيانات الرقمية المخزنة وخصوصاً المتعلقة بالبيانات الشخصية والحساسة والسرية وضعت قوانين الأمن الرقمي وحماية البيانات عموماً شروطاً قد تختلف بعض الشيء بين البلدان ما بين شديدة وروتينية ولكن تشترك بكونها تهدف لاشتراط بنى تنظيمية وتقنية محددة مسبقاً كشرط أساسي لمعالجة أية بيانات أو معلومات من قبل المكلفين بذلك. عملياً عند الحديث عن معالجة للبيانات فإننا نتحدث عن شركات أو هيئات حكومية تقول بتخزين بياناتها في مراكز حاسوبية ضخمة وهنا يتم التعاقد ما بين الجهتين للقيام بتخزين البيانات لدى هذه المراكز الحاسوبية في مقابل إمكانية وصول الجهة صاحبة التكليف لهذه البيانات لتقوم بنقلها أو معالجتها حسب الحاجة

لذلك. في خضم هذه العلاقة لابد لمعالجي البيانات وهم في أغلب الحالات مراكز الخدمة الحاسوبية السحابية أو المحلية والذين تشترط القوانين عليهم أن يوفرُوا كحد أدنى منصوص عليه قانوناً من الحماية والتجهيزات التنظيمية والتقنية وعلى الجهة التي تعطي التكليف بالمعالجة، وهي الجهة الحكومية أو الشركة، أن تتأكد من توفر هذه المعايير تحت طائلة مسؤوليتها عن أي ضرر يحصل للأشخاص أو الجهات التي تخصها هذه البيانات. هذه العلاقة المتعددة الأطراف تشترط تحمل كل طرف لمسؤولياته لضمان تناقل آمن للبيانات لا يضر بمصلحة الأفراد وخصوصيتهم.

هذه المعايير أو الشروط تُعرف اختصاراً ب TOM أو technical and organisational measures هذه المعايير تجدها في الكثير من قوانين الأمن الرقمية وحماية البيانات كشروط مسبقة يجب توخيها في كل عملية معالجة. لقد تحدثت اللائحة الأوروبية في المادة 32 الفقرة 1 عن إلزامية التأكد من اتباع المعايير التنظيمية والتقنية المناسبة كشرط لمعالجة البيانات الشخصية، تحت هذا المفهوم يندرج عدد كبير من المعايير وأدرجت المادة نفسها بعضاً من هذه المعايير وذلك على سبيل المثال لا الحصر، المعايير التي وردت في الفقرة الأولى هي:

- تشفير البيانات الشخصية.
- التأكد بشكل دائم من سرية وتوافر ومرونة أنظمة معالجة البيانات.
- القدرة على استعادة توافر البيانات الشخصية والوصول إليها بسرعة في حالة وقوع خلل تقني أو حادث طارئ.
- المراقبة الدورية وتقييم فعالية الإجراءات الفنية والتنظيمية لضمان أمن المعالجة.

وغيرها الكثير مما يندرج تحت بند بيئة آمنة ومستقرة وتحكم وسيطرة كاملة على عملية معالجة وتناقل المعلومات.

هنا سنلقي الضوء على بعض أهم هذه المعايير وطرق تطبيقها.

3.1 التشفير وقوانين المعلومات

يُعرف التشفير بأنه من أهم وسائل حماية البيانات خصوصاً في ظل تناقل البيانات اللحظي بين مواقع جغرافية متعددة وعبر مراكز حاسوبية مختلفة قد تُعرض هذه البيانات للخطر وذلك عبر تحويلها إلى عبر خوارزميات تشفير تجعلها غير مقروءة وباستخدام نفس الخوارزميات عند التلقي من الطرف الآخر يتم إعادة فكها وتحويلها لصيغتها الأصلية المقروءة.

تتنوع كذلك أساليب التشفير حسب الاحتياجات والغاية منه ويعتبر تخزين البيانات السحابي أو ما يعرف ب Cloud من أهم الأماكن التي يكون فيها التشفير ضرورة لابد منها حيث يتم الوصول للبيانات من خلال اتصال بين مكان المستخدم ومكان

التخزين الذي يكون في بلد مختلف هنا يتم استخدام اتصال مشفر ويتم نقل وتخزين البيانات بشكل مشفر بحيث يمنع وصول البيانات لطرف ثالث لأن مفتاح الوصول موجود فقط لدى الجهة المستقبلة وبشكل مركزي.

كأحد رواد التخزين السحابي شركة Amazon وخدماتها Amazon Web Service ، سنلقي الضوء كمثال تطبيقي على التقنيات المتبعة والتي ضمنت توافقيتها مع القوانين واعتمادها كمكان آمن لتخزين البيانات.

3.1.1 أمازون مزود خدمة التخزين السحابي (مثال بحثي)

يُعرف أمازون للتخزين السحابي نفسه على أنه مزود خدمة آمن للتخزين المعلوماتي، فتحدث عن اتصال آمن Virtual Private network بين المستخدم والخدمات المخزنة للبيانات وعن أقراص تخزينية مشفرة بالكامل ويُدار التشفير مركزياً عبر مفتاح وصول لا يمكن الوصول إليه من قبل أي طرف ثالث. [20]

بالطبع الغاية الرئيسية لكل مخدم أن يصل لجودة وأمن في تخزين ونقل البيانات بشكل يستقطب كافة قطاعات الزبائن، هذا يمكن فقط في حال تم توفير خدمة تشفير ذات مقاييس عالية كما ذكرت آنفاً، لذلك يقدم مزود خدمة التخزين السحابي أمازون خدمته التخزينية كخدمة ملائمة لمعايير الحماية المطلوبة قانونياً للدوائر والهيئات الحكومية. هذا الأمر يتطلب العمل على أن تكون القواعد المعمول بها لإجراء التشفير متوافقة مع الشروط المحددة قانونياً لتخزين هذا النوع من البيانات. من الناحية التقنية يمكن الحديث عن التقنيات التالية كأهم التقنيات المستعملة في تشفير البيانات لديه:

- التشفير باستخدام الترميز AES256

مع هذه الخدمة يمكن للمزود تقديم ضمان للمستخدم بأن المعلومات الحساسة والشخصية المخزنة في الخدمات السحابية لن يتم الوصول إليها إلا باستخدام مفتاح لفك التشفير يتوفر فقط مع المستخدم صاحب البيانات وتتم إدارته عن طريق مزود الخدمة Amazon.

- تقنية التشفير الشفافة Transparent Data Encryption

هي تقنية تستخدم بشكل أساسي لتشفير قواعد البيانات مثل SQL و Oracle ، بالطبع تعتبر قواعد البيانات من أساسيات عمل الشركات والدوائر الحكومية وتحتاج البيانات بداخلها لتقنية تقي بالغرض ويتم تشفيرها باستخدام تقنية المفتاح الأساسي Master Key يتغير بشكل دائم ويتم فك التشفير عن طريق شهادات رقمية تتضمن معلومات المستخدم وبالتالي تضمن الوصول إلى المعلومات فقط من قبل المخولين بالوصول فقط.

- تشفير أقراص التخزين المستخدمة في المخدمات

يتم تشفير الأقراص المحلية الموجودة على المخدمات والتي يتم تقديمها ضمن خدمة السيرفرات الافتراضية Elastic Computer Cloud من أمازون، هنا يتم التشفير للقرص بالكامل أو فقط لمجلدات معينة يختارها المستخدم وبالتالي تكون البيانات حتى محلياً.

• خدمة إدارة المفاتيح KMS

تقوم هذه الخدمة على جعل آلية التشفير مركزية بحيث يتم إدارة مفاتيح فك التشفير للنظام بأكمله من خلال وحدة مركزية وهذا يحول دون إمكانية وصول المفاتيح لطرف ثالث كون المفتاح الأساسي يوجد فقط بشكل مركزي وليس محلي.

الشكل (1): هيكلية التشفير في مزود خدمة التخزين السحابي أمازون. [21]

هذه الخدمة المركزية توفر أيضاً توافرية عالية للخدمة بحيث يتم إنشاء مفاتيح احتياطية في النظام وفي مناطق مختلفة بشكل يتم الوصول للمفتاح الأقرب جغرافياً لضمان سرعة وتوافرية الخدمة بالشكل الأمثل وحسب المعلومات الصادرة عن مزود الخدمة أمازون فإن نسبة توافرية هذه الخدمة تبلغ 99,999,999 وتخضع باستمرار لمراقبة مستمرة لمراقبة أي خلل ممكن. [20] إن خلال تقنيات التشفير والخطوة العامة المتبعة في هذه الشركة العملاقة تم الوصول إلى معايير يمكن من خلالها استضافة البيانات والمعلومات الخاصة بالدوائر الحكومية والجهات الرسمية والتشفير بالطبع هو أحد الجوانب التي على مزود الخدمة مراعاتها في طريقه لضمان التوافقية مع قوانين أمن المعلومات الرقمية وحماية البيانات، كذلك الأمر بالنسبة فإن تقييد الوصول حسب المستخدم وصلاحياته هي من الأمور التي يوفرها مزود الخدمة أمازون وضرورية

للمسائلة القانونية حسب قوانين البيانات حيث يجب التمييز ما بين المستخدمين من حيث صلاحياتهم وطرق وصولهم والتمييز ما بين حق التغيير أو القراءة أو الاطلاع على البيانات.[22]

● الشبكة الافتراضية الخاصة

يعتمد مزود الخدمة أمازون على بناء شبكة افتراضية بين العميل وبياناته الموجودة على مخدمات أمازون لضمان تشفير آمن عند نقل البيانات، هذه الشبكة تستخدم بروتوكول IPsec لبناء نفق تبادل بيانات آمن ومشفر من الحاسوب الخاص بالمستخدم وصولاً إلى الواجهة الخارجية لمخدمات أمازون والمسماة Virtual Private Cloud. بالطبع للتشفير تقنيات وأساليب متعددة وتتطور بشكل دائم ويُعزى ذلك إلى التطور الحاصل في الوقت ذاته في تقنيات فك التشفير والقرصنة والتي تجعل التشفير في بعض الحالات لا طائل منه في ظل وجود تقنيات متاحة تقوم بفك هذا التشفير بأسلوب قد يكون متاحاً للكثيرين. هذا الاختلاف ما بين المعلومات الممكن فك تشفيرها وبين التي لا يمكن فك تشفيرها له آثار قانونية ومن المهم التمييز بينهم لأن القانون يرى كل منهم بشكل مختلف. هذا ما يميز الإدارة المركزية للتشفير وبين التشفير المحلي حيث إن التشفير الذي يتم في الدوائر الحكومية والهيئات الدولية يخضع لسياسة مركزية مفتاح فك التشفير والذي يجعل الوصول للمفتاح الأساسي لفك التشفير غير متاح لأحد في حين أن التشفير التقليدي يكون المفتاح مخزن محلياً ومن الممكن في حال الوصول الفيزيائي للجهاز الوصول للمفتاح أيضاً وبالتالي لم تعد البيانات مشفرة ولن تنطبق عليها خصائص البيانات المشفرة وقوانينها كوسيلة لحماية خصوصية الأشخاص عن طريق منع الوصول غير المسموح إليها.[23]

يعتبر التشفير أحد مقومات البنية المحمية والأمانة لمعالجة وتخزين البيانات والتي ينادي بها كل قانون لأمن المعلومات كما هو الحال في نص اللائحة الأوروبية التي فرضت في المادة 32 منها وجود مجموعة من الشروط التقنية والتنظيمية كشارك أساسي للقيام بأي عملية معالجة للبيانات، يعتبر بالطبع التشفير أحد هذه الشروط ويوفر بالإضافة لذلك الكثير من الخيارات والإعفاءات بالنسبة للجهة التي تعالج البيانات والمعلومات بحيث إن نقلها بشكل مشفر يعفيها في حالات معينة من المسؤولية التي قد تكون جسيمة في حال تم النقل بشكل صريح وغير مشفر أو بشكل مشفر ولكن غير آمن بالشكل الكافي. لفهم الاختلاف القانوني أصدرت دائرة مراقبة حماية البيانات في مقاطعة بايرن الألمانية قراراً يقضي بأن معالجة بيانات مشفرة بطريقة آمنة عبر خوارزميات غير متاحة الوصول يعتبر معالجة لبيانات عامة وليس لبيانات شخصية حيث إن التشفير يجعل منها بيانات غير صريحة وبالتالي لا تنطبق عليها شروط الحماية المنصوص عليها في قوانين حماية البيانات الشخصية والتي تشدد في الحماية كونها تمس خصوصية الأفراد وحياتهم.

هذا بالطبع ينطوي على نتائج أخرى تفيد الجهة العاملة على البيانات فضياع هذه البيانات وهي بحالة التشفير يحمي عنها صفة الخطورة والنتائج التي تترتب على ضياع بيانات سرية أو شخصية من تعويض ومسؤولية جسيمة، وهذا ما أقرته محكمة العدل الأوروبية حيث رأت أن البيانات المشفرة والتي لا يمكن فك تشفيرها كما هو الحال في بعض أنظمة التشفير التي تجعل فك التشفير غير ممكن أو ممكن عبر مفتاح أساسي وليس محلي ولا يمكن الوصول إليه. إن الحالة التي تم الحكم بشأنها كانت تتعلق بعنوان أي بي الخاص بأحد أجهزة الكمبيوتر وكان طرح القضية يتعلق بالوصول إلى تحديد هوية الشخص عبر عنوان أي بي المخصص له، هنا قررت المحكمة أن تتأكد من إمكانية الوصول لهذا العنوان وبعد البحث فيما إذا كان هذا العنوان مشفراً بطريقة لا يمكن لطرف ثالث الوصول إليه، وبعد اللجوء لخبرة المختصين لتقييم هذه الحالة بشكل فردي وليس عام تم إقرار هذا العنوان كعنوان مشفر وبالتالي لا تنطبق عليه صفة البيانات الشخصية كون التشفير كان بشكل لا يمكن أن يتم فكه عبر طرف ثالث.

3.2 حماية الخصوصية عن طريق التصميم

تشترط قوانين المعلومات بشكل رئيسي أن تتم معالجة البيانات وخصوصاً الشخصية والحساسة منها ضمن بيئة تقنية وتنظيمية آمنة ولقد عبرت بعض القوانين الخاصة بحماية المعلومات الرقمية عن ذلك من خلال وضع أهداف كشروط مسبقة لأي عملية معالجة أو نقل للبيانات، هذه الشروط نجدها مثلاً في قانون حماية البيانات الألماني BDSG في المادة 9 حيث تطرقت المادة لعدة شروط يجب توفرها لضمان حسن سير عملية التعامل مع البيانات، كالرقابة على الدخول الفيزيائي لمراكز الخدمات الحاسوبية Data Center ومراقبة توافر الخدمة والإبلاغ عن الاختراقات وغيرها الكثير هي من الأمور التي تدرج تحت البنود الأساسية التي تتطلبها معظم تشريعات الحماية الرقمية.

من ضمن الأمور التي تم طرحها كوسيلة توافقية تُسهل عملية التوافق مع الأنظمة والقوانين الخاصة بالحماية الرقمية هو مبدأ حماية الخصوصية عن طريق التنظيم، تم الحديث عن هذا المبدأ في اللائحة الأوروبية لحماية البيانات الشخصية GDPR حيث تحدثت المادة 25 عن هذين المبدأين، وأهمية تنفيذ مبدأ الحماية من خلال التصميم لضمان فعالية المعايير التقنية والتنظيمية المتبعة في عملية معالجة المعلومات. [25]

تم تطوير هذا المفهوم من قبل Ann Cavoukian في فترة التسعينيات ولكن هذا المفهوم لم يتم استعماله بالشكل الحالي فتطور التقنيات وضع له أطر جديدة كالتالي فرضتها اللائحة الأوروبية لحماية البيانات الشخصية، حيث تفرض اللائحة الأوروبية تضمين مبادئ حماية البيانات ضمن خطة تطوير الأنظمة والبنى التحتية وأن تكون الأهداف هي التقليل من

عمليات معالجة ونقل البيانات إلى الحد الأدنى الممكن للتقليل قدر الإمكان من المخاطر وتعتبر الخطوات التالية هي القاعدة الأساسية الموصى بها في حال تطبيق هذا المفهوم عملياً:

- تنفيذ المفهوم كخطة وقائية وليس كخطة لاحقة.
- تضمين القواعد الموصى بها من قوانين حماية البيانات ضمن الخطة الأولية للعمل.
- فعالية كاملة للتجهيزات والبرمجيات بالتزامن مع كونها معدة حسب مقتضيات حماية البيانات.
- حماية خلال كافة مراحل دورة معالجة المعلومة.

هذا المبدأ يقوم على مراعاة إمكانية تنفيذ وتطبيق القوانين المتعلقة بالأمن الرقمي ابتداء من مرحلة التصميم حيث يتم تصميم البنى التحتية وكذلك البرمجيات الخاصة بمخدمات إدارة وتخزين البيانات من البداية بشكل متوافق مع القوانين الخاصة بذلك. هذا المفهوم هدف من حيث المبدأ إلى تنفيذ الخطط التي تضعها شركات ومزودات خدمة التخزين الرقمي لتصل إلى المعايير المطلوبة منها وفقاً للقوانين السائدة، هذه الخطط تتضمن عادة خطوات لتغيير وتعديل البنية الحوسبية والتنظيمية لتصبح منسجمة مع القوانين النافذة أو الجديدة. اعتماداً على هذا المفهوم تصبح عملية معالجة البيانات ونقلها متوافقة بشكل آلي مع القوانين النافذة لها.

كمثال عملي على هذا المفهوم يتم اعداد نظام التخزين في الحواسيب لتقوم بشكل آلي بحذف البيانات من المخدمات في حال انتهاء الغرض منها وذلك وفقاً لللائحة الأوروبية التي تفرض معالجة البيانات فقط للغرض الذي تم جمعها من أجله، فالمعلومات التي تم جمعها عن شخص قام بالتقدم بطلب بطاقة مصرفية يجب أن يتم حذفها تلقائياً بعد انتهاء صلاحية هذه البطاقة. هذه الآلية يجب أن تكون معدة مسبقاً عند تصميم البيئة الحاسوبية والبرمجية بحيث تنفذ هذه الخطوات بناء على معطيات معطاة مسبقاً. [26]

أحد التطبيقات الأخرى التي تأتي متوافقة مع القوانين الأوروبية في مجال الحماية من حيث التصميم يمكن توضيحها من خلال مثال عن برمجة التطبيقات التي تبحث عن فعاليات بالقرب من مكان تواجد الشخص، هذا النوع من التطبيقات يستعمل بيانات الموقع الخاصة بالشخص للوصول إلى النتائج، إن برمجة هذه التطبيقات مثلاً يجب أن تراعي عدم طلب الوصول إلى بيانات الشخص من موقع وما إلى ذلك مباشرة بعد تنزيل التطبيق على الهاتف وإنما فقط في حال قام الشخص بالبحث عن مطعم مثلاً بالقرب من مكان تواجده، هذا المفهوم قلل في هذه الحالة من عمليات الوصول إلى البيانات الشخصية وجعلها فقط حين الحاجة وتم تطبيق هذه السياسة من خلال التصميم البرمجي للتطبيق مسبقاً وهذا النهج في

تصميم التطبيق يمكن أن يكون ضمن مستند لإثبات الالتزام بقوانين حماية المعلومات في حال التعرض لمساءلة قانونية. [27]

3.3 حماية الخصوصية افتراضياً:

يعتبر هذا المفهوم جزءاً من مفهوم الحماية من حيث التصميم، ويقضي بأن الإعدادات الافتراضية لكل نظام يقوم بمعالجة البيانات يجب أن تكون معدة لتسمح فقط بالحد الأدنى من معالجة البيانات افتراضياً ويتم توسيع الصلاحيات حسب حاجة المستخدم، وعليه يجب أن تكون الخيارات بداية معدة بشكل تضمن أقل استعمال ممكن لبيانات المستخدم، أحد الأمثلة على ذلك منادات به بعض التشريعات الخاصة بحماية البيانات من أن المواقع الإلكترونية التي تعطي خيار بحفظ ايميل المستخدم لاستخدامه في رسائل دعائية لاحقاً أو ما يعرف بـ Opt in يجب أن يكون في حالة Opt out والمستخدم هو من يقوم طواعية بتفعيله في حال رغبته الاشتراك بهذه الرسائل. [27]

هذا الخيار بالرغم من جنوحه إلى حفظ أمن المستخدم إلا أنه قد يجعل استعمال الكثير من التطبيقات والبرامج أكثر صعوبة وأقل متعة من قبل المستخدم ذلك أن بعض الخيارات يُفضل أن تكون مفعلة ولو كانت تتضمن استعمالاً أكثر لبيانات المستخدم إلا أنها تعتبر أكثر فائدة للمستخدم، كحل وسيط يمكن أن يقوم مزود الخدمة أو التطبيق بإعطاء المستخدم خيارات متعددة من البداية عن نوع التشكيل الجانبي الذي يفضل ويمكن للمستخدم اختيار التشكيل الذي يتضمن استعمال أوسع لمعلوماته مقابل مرونة أكبر باستخدام الخدمة أو تشكيل أقل مرونة وأكثر تقييداً في استخدامه لبياناته. [28]

4. توزيع المسؤولية القانونية في قوانين حماية البيانات:

عند وقوع خرق لأحد قوانين أمن المعلومات والبيانات فإن أول ما يتبادر للذهن هو على من تقع المسؤولية والتبعات وماهي محددات توزيع المسؤولية بين الأطراف المعنية بهذا الخرق. هذا الأمر بالطبع ينظمه القانون الخاص بحماية البيانات التي تم حدوث خرق بشأنها، إن بحث ماهية المسؤولية عن هذا النوع من الخروقات يتطلب بداية بحث كافة تدرجات الدول في مجال قوانين أمن المعلومات وحماية البيانات.

4.1 مسؤولية معالج البيانات:

كما مر سابقاً معناه، لا تتوفر بعض الدول على قوانين خاصة بحماية أمن المعلومات ولا تتعدى الحماية أكثر من كون الدستور أو القانون المدني أو حتى الجزائي يتضمن نصوص عامة تتحدث عن أحقية المتضرر بملاحقة المسبب للضرر، هنا يندرج الضرر الناتج عن سوء استخدام البيانات أو عدم مراعاة الحيطه والحذر في خانة الضرر التقليدي والذي يُخول صاحبه

الحق في ملاحقة المتسبب بذلك ولا يعتبر هنا الضرر الناتج عن خرق لأمن المعلومات ذو طبيعة مختلفة عن بقية الأضرار وإنما تتم ملاحقته وفقاً للقواعد العامة للقانون. في ظل هذا الوضع القانوني تقوم المسؤولية حسب العلاقة ما بين الضرر والمتسبب.

أما في حال توفر قانون متخصص بحماية البيانات يتم عندها الرجوع لهذا القانون فيما يخص معرفة قواعد المسؤولية الخاصة بالنشاطات المتعلقة بأمن المعلومات والبيانات حيث يتم توزيع المهام إما طوعياً حسب العقد المبرم ما بين معالج البيانات وهو عادة شركة تخزين البيانات أو مزود خدمة التخزين السحابي وما بين المسؤول أو المستخدم وهو الشركة أو الدائرة الحكومية أو الخاصة، هذا العقد يتضمن توزيع المسؤوليات بين أطراف العقد حسب طبيعة المهام الموكلة لكل طرف، هذا ما لم ينص القانون على حالات معينة يلتزم فيها أحد الأطراف بأنواع معينة من الالتزامات لا يمكن تفويضها للطرف الآخر بموجب العقد.

فمثلاً تقوم مسؤولية مزود خدمة التخزين السحابي بشكل حصري عن كل ما يخص توفير بيئة آمنة لمعالجة البيانات وإلا تعرض للعقوبة وفقاً لللائحة الأوروبية لحماية البيانات المادة 83 الفقرة 4 أ. هنا يجب على مزود الخدمة إثبات أنه قام بتوفير ما يلزم لحماية البيانات ولضمان معالجتها في بيئة آمنة لإخلاء مسؤوليته في حال تعرض البيانات لاختراق أو تلف، هنا تجدر الإشارة إلى أن الشركة أو الهيئة التي قامت بالتفويض ملزمة قانوناً باختيار مزود خدمة تخزين لبياناتها تتوفر فيه الشروط المنصوص عليها قانوناً وفي حال لم يتم إثبات أن الاختيار تم وفقاً لمعايير السلامة التي يتطلبها القانون لمعالجة البيانات خصوصاً الحساسية منها يقع هنا عبء المسؤولية على المستخدم أو المفوض بالخدمة وليس فقط على مزود الخدمة وهذا ما يسمى المسؤولية المشتركة والذي تحدثت عنه اللائحة الأوروبية في عدد من موادها. [29]

حسب القوانين الأوروبية توسعت مسؤولية معالج البيانات تجاه المفوض أو المستخدم حيث للمستخدم الحق في المطالبة بالتعويض حسب المادة 82 الفقرة 1 و 4 من اللائحة الأوروبية لحماية البيانات.

هذا التوسع في المسؤولية التي تقع على معالجي البيانات وهم عادة شركات تخزين البيانات في كثير من الحالات أعطى الحق بالمطالبة بالتعويض في حال حصول ضرر نتيجة عدم التزام المعالج للبيانات بالقوانين المعمول بها في مجال حماية البيانات لذلك من الضروري قانونياً أن يقوم مزود خدمة التخزين في إطار معالجته للبيانات بعمل عقد يتضمن تفاصيل المعالجة لكي يعفي نفسه من المسؤولية أو يحددها في حال كان الخطأ نتيجة تفويض من المستخدم. ولكن معالج البيانات يبقى حسب المادة 28 الفقرة 3 و 4 و 5 تحت المسؤولية القانونية وخاصة فيما يتعلق بالالتزام بالنقاط التالية:

- القيام بمعالجة البيانات حسب الغرض الذي تم التفويض به.
- عدم الالتزام بالمعايير التقنية والتنظيمية والتي تعرف اختصاراً TOM.
- الإبلاغ عن حدوث خرق للبيانات خلال 72 ساعة.
- حذف البيانات بعد الانتهاء من الغرض الذي تم جمعها من أجله.

هنا تبرز أهمية إبرام عقد بين الطرف الذي يقوم بمعالجة البيانات والطرف المسؤول عن البيانات أو المستخدم موضوع البيانات، فإبرام عقد بين الطرفين يتضمن توضيح ماهية البيانات والغرض منها وكافة المعلومات المتعلقة بالأشخاص موضوع البيانات وفيما إذا سيتم نقلها لبلد خارجي حتى يكون العقد بمثابة دليل خطي بيد الطرفين في حال أخل أحد الأطراف بشروط العقد.[30]

إن المسؤولية المنصوص عليها في المادة 82 من اللائحة الأوروبية تتضمن مسؤولية مدنية تتمثل بالتعويض وتتضمن أيضاً مسؤولية جزائية في حال لم يتم تقييدها من خلال شروط عقد يبرم بين الطرفين. هذا العقد يُعرف بـ Data Processing Agreement.

أحد التطبيقات العملية في مجال المسؤولية المشتركة نراه في شركة أمازون لخدمة التخزين السحابي AWS حيث صرحت في خطتها للتوافق مع القوانين الأوروبية لحماية البيانات عما يعرف بمفهوم المسؤولية المشتركة حيث ينظم العقد الذي تبرمه شركة أمازون مع المستخدم توزيع المسؤوليات بين الطرفين فينص العقد صراحة على أن يتولى مزود الخدمة أمازون المسؤولية عن البنى التحتية التقنية من مخدمات وأجهزة شبكية وأنظمة تشغيل خاصة بالمخدمات وكذلك عن سلامة البنية الفيزيائية والأمنية لمقر تخزين البيانات ومنع الوصول غير المرخص لها. في حين تقع على عاتق المستخدم مسؤولية الحفاظ على المعلومات التي يقوم بتخزينها على هذه المخدمات من الحذف أو الضياع وكذلك عن البرامج التي يقوم باستعمالها على هذه الأجهزة. لتوضيح توزيع المسؤوليات بين الأطراف يفصل الشكل البياني الذي تم طرحه من قبل شركة أمازون ضمن الكتاب الإرشادي للتوافق مع اللائحة الأوروبية كيف أن المسؤوليات تقع ضمن منطقتين أساسيتين، منطقة مزود الخدمة ومنطقة العميل، هذا الفصل بين المسؤوليات يمنح المستخدم أيضاً فرصة التعرف على مسؤولياته وإمكانية ملاحقة مزود الخدمة قضائياً في حال أخل المزود بالتزاماته.

الصورة التوضيحية -1- نموذج المسؤولية المشتركة لدى مزود خدمة التخزين السحابي أمازون

4.2 مسؤولية مسؤولي البيانات أو المستخدمين:

على الطرف الآخر تفرض بعض قوانين حماية البيانات واجبات ملزمة على المستخدمين، فعليه مثلاً التأكد من توفر المعايير التقنية والتنظيمية لدى معالج البيانات كذلك عليه التأكد أن البيانات لن يتم تخزينها على مخدمات تقع في دول أخرى والتي قد لا تلتزم بالقوانين الخاصة بحماية البيانات وحقوق الأشخاص.

وكذلك أضافت قوانين عديدة مهمة جديدة للمستخدم تتمثل بأجراء تقييم للمخاطر التي قد تترتب على معالجة البيانات ونقلها واستبعاد ذلك في حال كان هناك احتمال قوي لتعرض البيانات أو حقوق الأشخاص للضياع أو إساءة الاستعمال. [31] تقدير التبعات تم تضمينه في تشريعات سابقة مثل قانون حماية البيانات في ألمانيا حيث ورد في المادة 4 ث الفقرة الفرعية 4 و5 وتم أيرادها في القوانين الصادرة حالياً كما ورد في المادة 35 من اللائحة الأوروبية لحماية البيانات. توصي كذلك المادة بأن يقوم المسؤول عن البيانات أو المستخدم بعملية تقدير التبعات وفقاً للمادة 4 الفقرة 7 من اللائحة الأوروبية. أما عن الخطوات فيجب أن تتم بشكل دقيق لكل حالة على حدة، فيجب أن يتم فحص حجم البيانات التي سيتم معالجتها وكذلك الغرض منها وحجم المخاطر المتأتية من تسرب هذه البيانات وما يمكن لخرق حماية هذه البيانات من تأثير وخطر على حقوق وحريات الأشخاص الطبيعيين حسب ما تنص عليه المادة 35 الفقرة 1 الفقرة الفرعية الأولى من اللائحة الأوروبية. توصي اللائحة بشدة كذلك بالقيام بعملية تقدير التبعات في الحالات الواردة في المادة 35 الفقرة 3 أ ب ت؛ والتي تتضمن

على سبيل المثال معالجة بيانات ذات طبيعة خاصة مثل المعلومات الحساسة الواردة في المادة 9 والتي تتضمن معلومات عن الأصل العرقي والإثني، والآراء السياسية، والمعتقدات الدينية أو الإيديولوجية أو المادة 10 والتي تتضمن معلومات تتعلق بجناية أو ملاحقة قضائية لما لهذا النوع من المعلومات من أثر كبير على حريات الأشخاص ويجب هنا أن يقوم المستخدم أو المسؤول عن البيانات التابع للهيئة الحكومية أو المنظمة بعملية تقدير للتبعات من دون تردد وفي حال كانت هناك خطورة كبيرة تحيط بعملية المعالجة يجب هنا العدول عنها أو توفير أساليب حماية أكثر فعالية إلا يُسأل عن تصرفه باعتباره لم يتخذ الواجب الملقى على عاتقه بإجراء التقديرات المسبقة المناسبة. [32]

فيما يتعلق الخطوات الموصى بها يوجد هناك العديد من الخطط والاقتراحات عن كيفية عمل هذا التقدير بالشكل المطلوب وتنتشر بعض اللجان أو الهيئات الموكلة إليها حماية البيانات في بعض الدول توصيات وإرشادات حول أفضل الآليات لتنفيذ هذه الخطوات.

أصدرت وزارة العدل البريطانية تعليمات بهذا الخصوص مثلاً تتناول خطوات تنفيذية بهذا الشأن. هذه الخطوات هي:

- هل سيتم معالجة بيانات شخصية؟ كم عدد الأشخاص الذين ستتم معالجة بياناتهم؟
- ماهو مصدر هذه المعلومات؟
- هل سيتم معالجة البيانات لأغراض غير التي تمّ الجمع لأجلها؟
- ماهو المبدأ القانوني الذي سيتم الاستناد عليه في عملية المعالجة؟
- هل تمّ ملائمة كفاية البيانات مع الغرض منها؟
- كم سيدوم الاحتفاظ بالبيانات؟
- هل من الممكن تقنيا الاحتفاظ بالبيانات بشكل آمن؟
- هل لدى الأشخاص موضوع البيانات القدرة على الاعتراض أو الموافقة على معالجة بياناتهم؟
- هل سيتمّ تنقل البيانات خارج حدود الدولة التي تتبع لها هذه البيانات؟
- هل تمّ أخذ الموافقة الصريحة من الشخص موضوع البيانات؟ أم تمّ جمع البيانات في إطار عمل قضائي أو كبيانات منشورة للعموم؟
- هل هناك قيود مرتبطة بمعالجة هذه البيانات؟
- هل سيتمّ تشفير هذه البيانات؟ سيتمّ عمل نسخة احتياطية منها؟
- كيف سيتمّ توزيع صلاحيات الوصول إليها من قبل المستخدمين المخولين بذلك؟

- هل سيتم تتبع هذه البيانات ومراقبتها؟

من خلال طرح الأسئلة السابقة والإجابة عليها، يتم تحليل البيانات ومدى خطورة معالجتها وعمل تقييم للحالة الراهنة لها وبالتالي تفادي خطر اختراقها أو ضياعها وما لذلك من تأثير على حرية الفرد وحقوقه بحفظ بياناته.[33]

5. نقل البيانات إلى دولة أخرى:

بطبيعتها، تنتقل البيانات بسرعة هائلة بين الدول ويتم تبادلها على مدار الوقت وهذا بالطبع يختلف من حيث الطبيعية القانونية فإن بعض أنواع البيانات الشخصية كالحساسية منها تتطلب وفقاً لقوانين بعض الدول شروطاً معينة للنقل لا يمكن أن يتم النقل بدون مراعاتها إلا أن يكون المسؤول عن ذلك عرضة للمساءلة. وعليه فإن نقل البيانات إلى بلد لا تتوفر فيه معايير حماية البيانات وقوانين تصون حقوق الفرد يمكن أن يؤدي إلى ضياع حقوق الشخص موضوع البيانات على بياناته في حال تم تخزينها في دولة كهذا. هذا الأمر يجب أن يتأكد منه المستخدم مسبقاً لذلك أفردت بعض مزودات الخدمة خاصية تتيح للمستخدم اختيار المنطقة الجغرافية والبلد الذي سيتم فيه تخزين بياناته، بالإضافة لذلك يتم إطلاق قائمة بالدول التي تضمن قوانينها حقوق الإنسان وحماية البيانات الشخصية والسرية والحساسية وهذه القائمة يتم إصدارها من الجهة المصدرة والمراقبة للقوانين، فمثلاً في أوروبا تتولى المفوضية الأوروبية إصدار نشرة دورية على موقعها الإلكتروني يتضمن قائمة بالدول التي تتوفر فيها المعايير المناسبة؛ والتي يُسمح بنقل البيانات بينها دون أن يُشكل ذلك تهديداً لأمن وسلامة الأشخاص وبياناتهم، وهنا يبرز دور الهيئات المشرفة على حماية البيانات في الدولة بعمل تقييم ودوري للدول وتصنيفها حسب مستوى الحماية المتوفرة لديها مما يسهل على معالجي البيانات تقدير تبعات معالجة ونقل بياناتهم إلى هذه الدول، ولقد تم سرد المعايير في المادة 45 الفقرة 2 حتى 9 والتي تتعلق بسياسة تقييم الدول من قبل المفوضية الأوروبية والتي تشكل مثلاً يحتذى من حيث تنظيم إجراءات هذا التصنيف لضمان وضع معايير محدثة باستمرار لنقل البيانات بين الدول.

من الحالات الشائعة أن يقوم مزود خدمة التخزين بنقل البيانات بين مراكز حاسوبية في دول مختلفة من العالم وذلك حسب توافر المساحات التخزينية هنا لا بد من أخذ موافقة المستخدم على نقل بياناته إلى دولة أخرى وخصوصاً إذا لم تكن ضمن قائمة الدول التي يُسمح بالنقل إليها.

وتتابع المادة 45 لتوضح أن نقل البيانات وجمعها في دولة خارجية يجب أن يُسمح به في حال اعتبرت اللجنة الأوروبية هذه الدولة أو المنظمة التي تقع ضمن هذه الدولة لديها المعايير الكافية لحفظ البيانات بشكل آمن وضمن معايير الإتحاد الأوروبي، وأدرجت المادة في فقرتها الثانية هذه المعايير ابتداء من كون هذه الدولة تحترم حقوق الإنسان ولديها القدر الكافي من الحريات وكذلك وجود تشريعات متعلقة بحماية البيانات وتابعت المادة في الفقرة 2 ب توصيف هذه المعايير

بالحديث عن وجوب وجود هيئة إشراف في هذه الدولة تتولى مهمة تقييم ومراقبة معالجة البيانات، وتأتي الفقرة الثالثة من المادة نفسها لتتحدث عن دور اللجنة الأوروبية في تصنيف الدول خارج الاتحاد الأوروبي وفقاً للمعايير المذكورة آنفاً في المادة الثانية، وهذا التصنيف يُبين فيما إذا كانت الدولة مؤهلة لتتم عملية نقل البيانات إليها، وأضافت الفقرة نفسها ما يفيد بأن هذه التصنيف لا بد أن يتم بشكل دوري نظراً للتغيرات التي قد تطرأ على الدول من حيث استيفائها للمعايير المطلوبة وعليه فإن هذا التصنيف يجب مراجعته كل أربع سنوات على الأقل.

وفقاً لمبدأ لكل قاعدة استثناء، تعود المادة 49 لتوصّف لنا بعض الحالات التي يمكن نقل البيانات فيها إلى دول لا تتوفر فيها المعايير السابقة، ففي الفقرة الأولى تشرح لنا المادة الاستثناء الأول الذي يُجيز نقل البيانات إلى دولة خارجية بالرغم من كونها ليست ضمن التصنيف الذي وضعته اللجنة الأوروبية في حال كان هناك موافقة من قبل الشخص الذي تتعلق به البيانات، وهنا يجب أن ننوه إلى كون اللائحة أشارت إلى الموافقة مع كلمة الصريحة وهذا يعني أن الموافقة لا بد أن تكون بشكل واضح وصريح لا لبس فيه. في الفقرة الثانية نجد استثناء آخر مفاده أن عملية نقل البيانات يمكن أيضاً أن تتم في حال كان هناك عقد يفيد بالموافقة على النقل بين الشخص الذي تخصه البيانات وبين الطرف الآخر الذي قام بعملية النقل، أحد الاستثناءات الأخرى هو في حال كان هذا النقل لحماية مصالح حيوية تتعلق بالشخص صاحب البيانات أو أشخاص آخرين كما أن النقل يمكن أن يتم لأسباب تتعلق بالمصلحة العامة أو في حال كان النقل بناء على متطلبات ادعاء قانوني أو حماية قانونية. [34]

كذلك يمكن أن يكون النقل بناء على وجود شهادة موثوقة تسمح بالنقل الآمن للبيانات حسب ما نصت عليه المادة 42 من اللائحة الأوروبية وتحدث المادة 49 عن إمكانية النقل مع وجود Safeguard حيث يتم الاتفاق بين الهيئات المشرفة في دول مختلفة على ضمان التبادل الآمن للبيانات والتي يتم المصادقة عليها من قبل المفوضية الأوروبية. [35]

لا بد من الإشارة هنا أن نقل البيانات بين الدول لأغراض تتعلق بمصلحة الدول العليا وفيما يتعلق بجرائم وإجراءات قضائية يقع ضمن الاستثناءات المنصوص عليها في القوانين وهذا مانجده في المادة 49 من اللائحة الأوروبية في الفقرة 1 ث - ج مع عدم ذكر تفاصيل عن ماهية الأغراض التي تعتبر ضمن مصالح الدول العليا وتركت هذا الأمر لتقدير الهيئات واللجان المشرفة على تطبيق قوانين حماية البيانات.

النتائج البحثية:

من خلال سرد المعطيات في هذا البحث يمكننا تحديد بعض النتائج وإصدار بعض التوصيات المتعلقة بهذا الشأن. فعلى نطاق قوانين حماية المعلومات والبيانات نجد أن واقع هذه القوانين في البلدان العربية ما يزال فقيراً وحين نجد بعض الدول قد

قامت بإصداره فإنه مايزال قانوناً غير كامل الأركان يتضمن شروطاً وأحكاماً عامة لاتصل لمرتبة التشريعات العالمية المماثلة والتي تدخل في كامل التفاصيل والإجراءات. هذا يرجع إلى كون الدول العربية لاتولي إهتماماً كبيراً من الناحية القانونية للتطور التقني الحاصل وبالتالي ينعكس ذلك سلباً على حريات الأفراد القاطنين في هذه الدول من حيث ضعف الحماية القانونية المتعلقة ببياناتهم. بعض الدول العربية وخصوصاً المتقدمة منها تقنياً وعلمياً أدركت أهمية العمل على إصدار هكذا قوانين ذلك أن الحماية القانونية في ظل التطور التقني المتسارع ضرورة ملحة جداً. هذا الأمر نجده جلياً في دولة الإمارات العربية المتحدة التي كانت مثلاً بحثياً في بحثنا هذا ونجد كيف بدأت القوانين الخاصة بحماية البيانات على مختلف النطاقات بالظهور تلبية لحاجات المجتمع المتنامية في ظل التطور التقني الذي تشهده هذه الدولة. وكيف أن قانون حماية البيانات في مركز دبي التجاري كانت طليعة هذه القوانين وصولاً لمشروع قانون متكامل اقترب من اكتماله.

من النتائج الهامة لهذا البحث هو ما وجدناه من تطور تشريعي في اللائحة الأوروبية والتي طورت مفاهيم موجودة سابقاً وأدخلت مفاهيم جديدة حيث وجدنا مفاهيم قد تم تطويرها مثل تقييم التبعات الناتجة عن معالجة البيانات وأثرها وشروطها وأهميتها في بعض الحالات كذلك وجدنا بعض النقاط الجديدة مثل توسيع الاختصاص ليشمل كل من يقوم بنشاط تجاري موجه لأفراد يقطنون ضمن دول الاتحاد الأوروبي وذلك ضمن مبدأ التسويق وهذا فتح الباب أمام نقطة مهمة أخرى وهي مدى استعداد الدول العربية لتطبيق قوانين اللائحة في الحالات المنصوص عليها والتي تُطبق فيها اللائحة خارج حدود الاتحاد الأوروبي. حسب ما تبين في هذا البحث من خلال المراجع المستخدمة فإن نسبة كبيرة من الشركات العاملة في البلاد العربية تقع تحت الاختصاص لللائحة الأوروبية وبالتالي عليها التقيد بالتعليمات الخاصة بهذه اللائحة ولكن فعلياً لم تقع هذه الشركات حسب الإحصاءات بالإجراءات اللازمة بعد مما يعرضها للمساءلة والغرامات. إن ما يخلص إليه البحث في هذا الصدد إن الشركات التي لاتتخذ إجراءات على طريق التوافق مع القوانين الأوروبية لحماية البيانات تُبعد نفسها عن دائرة المنافسة في سوق العمل، حيث ستأى الشركات العالمية نفسها عن التعامل معها كونها لاتلتزم بمعايير حماية البيانات.

يخلص البحث أيضاً إلى أن التوافق مع القوانين الخاصة بحماية البيانات يتطلب خطوات منتظمة ومدرسة تسهل عملية الوصول إلى التوافقية وناقش البحث بشكل أساسي أهمية التشفير كضمانة لمعالج البيانات من الوقوع في إشكاليات قانونية في حال ضياع البيانات، حيث خلص البحث إلى أن البيانات الشخصية المشفرة لاتأخذ حكم البيانات الشخصية غير المشفرة مادام فك التشفير غير ممكناً من قبل طرف ثالث. كذلك تطورت مفاهيم حماية الخصوصية من خلال التصميم وحماية الخصوصية افتراضياً فتعتبر هذه المفاهيم حجر الأساس لكسب التوافق مع القوانين المتعلقة بحماية البيانات وينصح هذا البحث باعتماد هذه المفاهيم من قبل معالجي البيانات كون الالتزامات الجديدة المفروضة من قبل القوانين الحديثة تشكل عبئاً

كبيراً في حال تطبيقها بالطريقة التقليدية لذا تعتبر طريقة حماية الخصوصية من خلال التصميم المسبق والإعداد المسبق للمكونات التقنية بشكل تكون متوافقة من البداية مع القوانين المعمول بها في هذا الإطار مما يسهل عملية الالتزام بالواجبات التي تفرضها قوانين حماية البيانات وتُسهل التطبيق الحقيقي للقوانين كون البنى التقنية والتنظيمية معدة مسبقاً ومضبوطة حسب هذه المعايير.

من خلال البحث يمكننا أيضاً استخلاص أهمية تقسيم المسؤوليات في عملية معالجة البيانات بين المستخدم وشركات التخزين أو المعالجة، فتوزيع الأدوار القانونية مهم جداً لتحديد الطرف المسؤول عن كل مرحلة ويجب أن يتوخى المستخدم والمعالج الحذر في تبيان مواضع المسؤولية من خلال العقد المبرم بينهم. وأبرز البحث أهمية مفهوم تقدير التبعات الذي يقع ضمن مسؤوليات المستخدم أو المسؤول عن حماية البيانات حيث يمكن من خلال المثال البحثي الخاص بوزارة العدل البريطانية التنبيه إلى الخطوات المُوصى بها في مجال إجراء هذه العملية والتي تبحث تفاصيل البيانات المراد معالجتها والظروف المحيطة بالمعالجة من أجل ضمان معالجة آمنة للبيانات والامتناع عنها في حال وُجدت ظروف غير آمنة للمعالجة.

إن هذا البحث يدرس الواقع التشريعي لقوانين حماية البيانات ويوصي بمتابعة البحث في هذا الاتجاه كون قوانين حماية البيانات في الشرق الأوسط عموماً لم تصل بعد لمستوى يُؤمن الحماية اللازمة للفرد وللشركات والحكومات، وإن متابعة الأبحاث في مجال القوانين الخاصة بحماية البيانات وتأثير القوانين الغربية المطبقة في بلادنا العربية ومدى الملائمة الذي تتمتع به شركاتنا وهيئاتنا مع هذه القوانين تعتبر مادة بحثية دسمة للأبحاث القادمة. أضف على ذلك أن الأبحاث في مجال حماية البيانات تعتبر أيضاً ضئيلة نسبياً بالمقارنة مع المجالات القانونية الأخرى وعليه سيكون هذا البحث فاتحة لسلسلة من الأبحاث المتتالية التي تدرس الواقع القانوني المتعلق بحماية البيانات وآثاره وسبل تطويره.

المصطلحات والتعاريف:

المعالجة: هي عملية تعديل أو حذف أو نشر أو أي إجراء يتم على البيانات الرقمية

المعالج: هو الشخص الذي يقوم بإجراءات على البيانات من حذف أو تخزين أو نقل أو تعديل وكل ما يتبع ذلك.

مسؤول حماية البيانات: هو الشخص المكلف بحماية البيانات وتفويض آخر لمعالجتها وهو عادة المسؤول في الدائرة الحكومية أو المنظمة أو المستخدم نفسه.

اللائحة الأوروبية: هي اللائحة الأوروبية لحماية البيانات الشخصية والمعروفة اختصاراً بـ GDPR والصادرة عن المفوضية الأوروبية والتي بدأ العمل بها في 25 أيار 2018.

AWS: هي اختصار لاسم شركة أمازون لخدمات الويب والتخزين السحابي.

المخدمات: هي السيرفرات وأجهزة الحاسوب والتي توجد عادة في مراكز تخزين البيانات الضخمة وتقوم بعمليات ضخمة في وقت واحد.

قائمة المصادر والمراجع:

- [1] يونس عرب، الخصوصية وحماية البيانات في البيئة العربية، اتحاد المصارف العربية، 2002.
<http://doc.abhatoo.net.ma/IMG/doc/dro21.doc>
- [2] البوابة القانونية القطرية 2016.
<http://www.almeezan.qa/LawPage.aspx?id=7121&language=ar>
- [3] صحيفة الوطن الالكترونية، "تشريعية النواب" تناقش "حماية البيانات الشخصية"، شباط 2018.
<https://alwatannews.net/article/758733?rss=1>
- [4] اتفاقية تفاهم بين مركز دبي العالمي ومفوض حماية البيانات البريطاني، 2013
https://www.difc.ae/download_file/273/9212
- [5] وكالة الانباء الكويتية، مركز دبي المالي العالمي يصدر قانونا لحماية البيانات الشخصية، 2017.
<https://www.kuna.net.kw/ArticlePrintPage.aspx?id=1701263&language=ar>
- [6] Victoria Wood حماية البيانات والخصوصية في الإمارات العربية المتحدة، 2018.
<http://www.hadefpartners.com/News/329/Privacy-and-data-protection-in-the-UAE>
- [7] صحيفة البيان، قانون لحماية سرية وخصوصية بيانات المتعاملين، 03 أيار 2016.
<https://www.albayan.ae/across-the-uae/news-and-reports/2016-05-03-1.2631706>
- [8] موقع شركة التميمي للمحاماة – مقالة عن قانون تنظيم البيانات بقلم نيك كونل تشرين الأول 2015
- [9] جريدة الاتحاد، مقالة الكترونية، حماية البيانات الشخصية، 2018
<https://www.alittihad.ae/WejhatArticle/99484/>
- [10] موقع Eur-Lex الطريق إلى القوانين الأوروبية.
<https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046>
- [11] Sheila Pancholi، اللائحة الأوروبية القفزة الأكبر في عالم القوانين منذ 20 سنة، شباط 2018.
<https://www.ibtimes.co.uk/gdpr-biggest-change-data-laws-over-20-years-are-companies-ready-1663405>
- [12] نظرة عامة على تنظيم حماية البيانات العامة، أيار 2018.
<https://www.stalawfirm.com/ar/blogs/view/gdpr-compilant-or-not.html>
- [13] Ashford Warwick عشرة حقائق عملية تحتاج لأن تعرفها عن اللائحة الأوروبية لحماية البيانات الشخصية، أيار 2016.
<https://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR>
- [14] Bajramović Sanjin مشكلة التطبيق الموحد لللائحة الأوروبية لحماية البيانات 2017
- [15] aitnews كل ما تود معرفته عن اللائحة العامة لحماية البيانات GDPR، أيار 2018.
- [16] الامارات اليوم 10 إجراءات للتوافق مع قانون حماية البيانات الأوروبي، أيار 2018.
<https://www.emaratalyoun.com/technology/electronic-equipment/2018-05-15-1.1099143>
- [17] المكتب الليبي الأوروبي، قانون حماية البيانات الشخصية الأوروبي الجديد GDPR 2018، أيار 2018.
<https://www.euolibya.com/2018/05/2018-gdpr.html>
- [18] عادل راوتي، ما تأثير تطبيق اللائحة حماية البيانات الأوروبية؟، 2018
- [19] فراس اللو، هل ستُغيّر سياسات الخصوصية الأوروبية "GDPR" مستقبل الإنترنت؟ 2017.
- [20] Dan Sullivan خيارات لتشفير البيانات في خدمة التخزين من أمازون، أيار 2015.
<https://searchcloudsecurity.techtarget.com/answer/Encryption-key-management-AWS-encryption-keys-got-exposed-now-what>
- [21] دليل التوافقية من أمازون، تشرين الثاني 2017.
[https://d1.awsstatic.com/whitepapers/compliance/De Whitepapers/GDPR Compliance on AWS.pdf](https://d1.awsstatic.com/whitepapers/compliance/De%20Whitepapers/GDPR%20Compliance%20on%20AWS.pdf)
- [22] Bruno Quint الطريق الجديد إلى بيانات آمنة في السحابة الحاسوبية، 2015

<http://www.bobstechtalk.com/blog/2015/6/24/practical-it-what-is-encryption-and-how-can-i-use-it-to-prot.html>

[23] McKerchar ماهو التشفير وكيف يمكنني استخدامه لحماية بيانات الشركات، 2015

<http://www.bobstechtalk.com/blog/2015/6/24/practical-it-what-is-encryption-and-how-can-i-use-it-to-prot.html>

[24] Stefan Städler ادارة الهوية القانونية في الحوسبة السحابي ، 2017

[25] Pierre Gronau ،الحماية عن طريق التصميم في مشاريع التوافق مع اللائحة الأوروبية 2018

[26] Yves Gogniat،ماذا تعني الحماية من حيث التصميم والحماية افتراضياً 2018

<https://morethandigital.info/was-bedeutet-privacy-by-design-and-default/>

[27] Kuner ، ثورة في قوانين حماية البيانات الأوروبي، 2012

[28] المادة 4 الفقرة 7 و 8، المادة 24 ، 26 ، 28 ، 29 اللائحة الأوروبية GDPR

[29] Bitkom الكتاب الارشادي في معالجة البيانات 2017

[30] Oliver Schonschek ماذا يجب على مستخدم التخزين السحابي أن يعلم 2017

[31] Linda Boegelen ، تقدير التبعات، هل تعرف المخاطر؟ 2017

<https://it-service.network/blog/2017/09/28/auftragsdatenverarbeitung-adv-vertag-aendert-sich/>

[32] مختبر البيانات، تقدير التبعات، وزارة العدل البريطانية الصفحة 5 - 23

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709978/jdl-data-protection-impact-assessment.pdf

[33] Anna Myers ،نقل البيانات خارج الحدود، Privacy Advisor، 2017

<https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/>

[34] اللائحة الأوروبية لحماية البيانات الشخصية المادة 40، 44، 45

[35] رضوان اسخيمة، إضاءة على اللائحة الأوروبية لحماية البيانات الشخصية، نيل وفرات للنشر، 2018، صفحة 23-22.