الإتحاد الدولي للإتصالات

الحوسبة السحابية في الدول العربية: الجوانب القانونية والتشريعية، واقع وآفاق

تقرير الإتحاد الدولي للإتصالات

إعداد: الدكتورة جنان الخوري

بيروت – 30كانون الأول/ديسمبر ٢٠١٥

المحتويات

الملخص التنفيذي

تهدف هذه الدراسة إلى **مراجعة الجوانب القانونية والتشريعية للحوسبة السحابية في الدول العربية: واقع وآفاق**، وما تُثيره من إشكالياتٍ متعددة الأوجه، أبرزُها التحدياتُ التشريعيّةُ، والتنفيذيةُ، والإداريّةُ، والفنيّةُ، والتطبيقيّةُ؛ إضافةً إلى مسائلَ أُخرى، كالأمنِ في الحوسبةِ السحابيةِ، وحمايةِ البياناتِ، ومُعالجتِها، ونقلِها، وأمنِ التطبيقاتِ، ونِظام إدارةِ الهويّةِ... بحيث يتضمّنُ الجانبُ القانونيّ للحوسبَةِ السحابيةِ أبعاداً ثُلاثيةٍ رئيسيةٍ: البُعدُ الوظيفيّ والتِقنيّ، والبُعدُ القانونيّ، والبُعدُ التَعاقُدي... مما يطرحُ أهميةُ مُناقشةَ ما إذا كان هناك رُؤيةٌ عربيةٌ (إقليمية ومحلية) رسميةٌ، لإرساء بنيةٍ تحتيةٍ رقميةٍ للإندماجَ في البيئةِ الرقميةِ العالميةِ، لا سيما أنّ هناك العديدَ من الهواجسِ التي تُرافقُ هذه الخدمَةَ في الدوَلِ العربيةِ، أبرزَها معاييرُ أمنِ المعلوماتِ وإنقطاع الإنترنتِ، أو ضُعف خدماتِها، والمخاوفِ البيئيةِ، وفِئَة عقودِ الإذعان التي تفرضُها الشركاتُ مُوردةُ الخدماتِ، مما يُعيقُ حركةَ البياناتِ، والخدماتِ والتطبيقاتِ؛ والأمرُ الذي يُسبّب في تأخُّر المنطقَةِ العربيَّةِ في هذا المِضمار. إضافةً إلى العديدِ من الإشكالياتِ القانونيّةِ والمَوضوعيّةِ والإجرائيّةِ المُثارة، ومدى تعاوُن الدُولِ فيما بينها، وإشكالياتَ تقنية وفنية بالدرجة الأُولى، لا بل بمدى تعاون الوِزارات المُختصّة محلياً، والتعاون بين القِطاعين العام والخاص، مُروراً بالتكلِفَةِ الماليةِ للدُول العربيةِ للإنخراطَ في عالمَ الحوسبةِ السحابيةِ، ومدى بِناء قُدُراتٍ عربيةٍ مُختّصة، وتَخصص جامعيّ أكاديمي، ومدى توعيةِ الرأي العامِ، ونشرِ ثقافةً وطنيةً وإقليميّةً للحوسبة السحابيةِ. أما الموضوعُ الأهم، فيتعلّقُ بالسيادةِ الوطنيةِ، على قواعدَ البياناتِ، بحيث تبرُزُ تحدياتٍ تعاقديّةً وهواجسَ مُتعدّدةً، لا سيما لِناحيةِ مركزِ حُفظِ البياناتِ، والقانونِ الذي تخضعُ له. لمُناقشَةِ كُلّ هذه المسائِل، لا بُدّ من مراجعةَ الإطارِ التشريعيّ للحوسَبَةِ السحابيةِ في المَنطقةِ العربيةِ بشكلٍ عام، وعلى الصعيدِ المَحليّ **للدولَ العربيةِ الإثنتَي والعشرين** (الأردن، الإمارات العربية المتحدة، البحرين، الجزائر، السعودية، الكويت، تونس، جزر القمر، جيبوتي، سوريا، السودان، الصومال، العراق، عمان، فلسطين، قطر، لبنان، ليبيا، مصر، المغرب، موريتانيا، اليمن)، **عِبر بحثِ العديدِ من النِقاطِ التاليةِ، وأبرزها:** مفهومُ الحوسبةُ السحابيةِ، والإشكالياتِ القانونيّةِ والتِقنيّةِ والإداريّةِ والسياسيّةِ والتَطبيقيّةِ (مخاطرها)، والمُمارساتِ الأَفْضَل في الحوسبَةِ السحابيةِ (التجاربُ الغربيّة الأوروبيّة والأميركية)، والدورِ الفاعِلِ، للاتحاد الدوّلي للإتصالات؛ وطرحِ العديدِ من المُقترحاتِ، أبرزُها، إتفاقٍ عربيّ للملاذ الآمنِ Arab Safe Harbor، قبل التوصّلِ إلى الخاتِمَةِ، حيث سَنعْرُض لبعض الإستنتاجاتِ والمُقترحاتِ، مع نافذَةٍ على المُستقبلِ.

مقدمة بحثية

يُسجلُ كلّ عصر من حياةِ البشريةِ رِهاناً خاصاً، تدورُ حوله، بشكل مباشر أو غير مُباشر، كُل المُنظماتِ والمُفاوضاتِ والعلاقاتِ الدوليةِ. هذا الرهانُ اليوم، هو العولمَةُ التكنولوجيّةُ، التي شكّلت، محطةً رئيسيةً من حياةِ المجتمعِ الدوليّ.وقد تجلّتْ أبرزُ مُفرزاتِها فيما بات يُعرفُ بالحوسبةِ السحابيةِ Cloud computing، التي تُعدُّ بدورِها أحد أهم التحوّلات والتطوّرات التكنولوجيّة الكُبرى في العالم، مُقدّمةً العديدَ من الفوائد والخدمات عبر شبكة الإنترنيت، خدماتٌ بعيدةُ المدَى وواسعةُ النِطاقِ، لا سيما في التخزينِ، والنسْخ الإحتياطيّ، والشبكات، والأمن، وأنظمة الإدارة، ونقلِ البيانات، واستخدام البرمجيات وتطويرها، واستحداث فُرص عمل، وتنمية قطاع تكنولوجيا المعلومات والاتصالات بشكل عام...

إنما، وفي المقابل، فهي تُثير الكَثير من الإشكاليات في الدول العربية بشكلٍ عام، ولكلّ دولةٍ منفردَةٍ بشكلٍ خاص، أبرزُها التحدياتُ التشريعيّةُ، والتنفيذيةُ، والإداريّةُ، والفنيّةُ، والتطبيقيّةُ، وفقدانُ السيطرةِ على البياناتِ[١]، وضمان أنَّ ما يحدث في الحوسبةِ السحابيةِ لا يخرجْ عن القواعد والضوابِط القانونية القائمَة[٢]. إضافةً إلى مسائلَ أُخرى كالأمنِ في الحوسبةِ السحابيةِ، وحمايةِ البياناتِ، ومُعالجتِها، ونقلِها، وأمنِ التطبيقاتِ، ونِظام إدارة الهويَةِ... بحيث يتضمّنُ الجانبُ القانونيّ للحوسبَةِ السحابيةِ أبعاداً ثُلاثيةٍ رئيسيةٍ: البُعدُ الوظيفيّ والتِقنيّ، والبُعدُ القانونيّ، والبُعدُ التَعاقُدي... مما أثار انشغال هذه الدول والمُنظّمات الدولية الساهِرة على أمن المُجتمع الدوليّ وتطوّره – ومن بينها، الإتحادُ الدوليّ للإتصالاتITU – لإيجاد أُطُرٍ تقنيةٍ، وتشريعيةٍ، وإداريّةٍ حديثةٍ للحوسبةِ السحابيةِ، وصونِ خصوصيةِ بياناتِ الأفرادِ، والشركاتِ والدولِ، عبر مراجَعةِ واقِع الدولِ والقواعِدِ المرعيةِ الإجراءِ المُتعلّقةِ بالحوسبةِ السحابيةِ، ولإيجاد إطارٍ تطبيقيّ لها.

علي الصعيد الدولي، يتجهُ العالم في العصرِ الراهِن نحو خدماتِ الحوسبَةِ السحابيّةِ، بحيث قامَتْ العديدُ من الدولِ، لا سيما تلك المتقدّمة على غرار الولاياتِ المُتحدة الأميركية والدُولِ الأوروبيةِ والصين، بالمُبادرةِ بصياغة استراتيجياتٍ محليةٍ وسياسات وطنيةٍ تهدفُ إلى الإستفادةِ من خدماتِ الحوسبة السحابية، لا سيما تلك المتعلقة بتنظيمِ علاقاتِها مع الشركات الضخمة التي تتطلّب طبيعة أعمالها بُنية شبكيّة تحتيّة كبيرة ومراكز بيانات مستقلة (Local Data Center)، أضف إليها المؤسسات الصغيرة أو المتوسطة الحجم. أما في الدولِ العربيةِ، فتُشيرُ التقارير الدوليةُ إلى نموٍّ سنويّ مُطرَدٍ في إستخدامَ الحوسبةِ السحابيةِ[٣]. مما يطرحُ أهميةُ مُناقشةَ واقعِها في هذه الدولِ وما إذا كان هناك رُؤيةٌ عربيةٌ (إقليمية ومحلية) رسميةٌ

لإرساء بنيةٍ تحتيةٍ رقميةٍ للإندماجَ في البيئةِ الرقميةِ العالميةِ والتي تتسِمُ بالتغييرِ الدائِمِ والسريعِ، لا سيما أنّ هناك العديدَ من الهواجسِ التي تُرافقُ هذه الخدمَةَ في الدوَلِ العربيةِ، أبرزَها معاييرُ أمنِ المعلوماتِ (Information security)، لا بل أمان المعلوماتِ (Information Safety) ذات الطابع الحكوميّ، وانقطاع الإنترنتِ أو ضُعف خدماتِها في بعضِ مناطق هذه الدولِ، والمخاوفِ البيئيةِ، وفِئَة عقودِ الإذعان (adherence contracts) التي تفرضُها الشركاتُ مُوردةُ الخدماتِ على العُملاءِ المَحليّين، أو فرضُ حظَرٍ مُفاجِئٍ من الشركاتِ لبرمجيات الحوسبَةِ السحابيةِ كخدمة (SaaS)، أو المنصّة كخِدمة (PaaS)، أو البُنية التحتيّة كخِدمة (IaaS)، مما يُعيقُ، حركةَ البياناتِ والخدماتِ والتطبيقاتِ؛ الأمرُ الذي يُسبّب في تأخُّر المنطقَةِ العربيَّةِ في هذا المِضمار. إضافةً إلى العديدِ من الإشكالياتِ القانونيّةِ، والمَوضوعيّةِ، والإجرائيّةِ المُثارة[٤]، ومدى تعاوُن الدُولِ فيما بينها، وإشكالياتَ تقنيةٍ[٥] بالدرجةِ الأُولى، لا بل مدى تعاون الوِزارات المُختصّة محلياً، والتعاون بين القِطاعين العام والخاص، مُروراً بالتكلِفَةِ الماليةِ للدُول العربيةِ للإنخراط في عالم الحوسبة السحابية، ومدى بِناء قُدُراتٍ عربيةٍ مُختّصة، وتَخصص جامعيّ أكاديمي، ومدى توعيةِ الرأي العام ونشرِ ثقافة وطنية وإقليميّة للحوسبة السحابيةِ.

أما الموضوعُ الأهم فيتعلّقُ بالسيادةِ الوطنيةِ على قواعدَ البياناتِ[٦]، بحيث تبرُزُ تحدياتٍ تعاقديّةً وهواجسَ مُتعدّدةً، لا سيما لِناحيةِ مركزِ حُفظِ البياناتِ، والقانونِ الذي تخضعُ له، هل هو قانونِ الدولَةِ المُضيفَةِ بإسم السيادَةِ الوطنيّة أم قانون المَقرّ الرئيسيّ للشركَةِ، ومدى احتماليَةِ تنفيذِ أَمْرٍ قضائيّ بحقّ هذه الشركاتِ في حالِ صُدُورِه عن المحاكِمِ المحليّةِ.

لمُناقشَةِ كُلّ هذه المسائِل لا بُدّ من مراجعةَ الإطارِ التشريعيّ للحوسَبَةِ السحابيةِ في المَنطقةِ العربيةِ بشكلٍ عام، وعلى الصعيدِ المَحليّ **للدولَ العربيةِ الإثنتَي والعشرين** (الأردن، الإمارات العربية المتحدة، البحرين، الجزائر، السعودية، الكويت، تونس، جزر القمر، جيبوتي، سوريا، السودان، الصومال، العراق، عمان، فلسطين، قطر، لبنان، ليبيا، مصر، المغرب، موريتانيا، اليمن) عبر بحث العديدِ من النِقاطِ وأبرزها: إشكالية تعريف الحوسبةُ السحابيةِ، وحجمُها، وخصائِصُها، ومُميزاتُها، ومُكوناتُها، وأنواعُها ونَماذجُها، وسطَ مخاوف ومحاذير أبرزُها: ضُعفُ البُنى التحتيّةِ، أمانُ المعلوماتُ، واقعُ الشركاتُ المُتخصّصةِ، تَطبيقاتُ الحوسبةُ في بعضِ الدولِ وكِلفتُها، التَرتيباتُ والضوابِطُ اللازمَةُ، مدى التعاونِ مع الهيئاتِ الدوليةِ المُختصّةِ، والشركاتِ الضَخْمةِ المُتخصّصةِ. إضافةً إلى الإشكالياتِ القانونيّةِ والتِقنيّةِ والإدرايّةِ والسياسيّةِ والتَطبيقيّةِ (مخاطرها)[٧]، والمُمارساتِ الأَفْضَل في الحوسبَةِ السحابيةِ، (التجاربُ الغربيّة الأوروبيّة والأميركية)، والدور الفاعِلِ للاتحاد الدوّلي للاتصالات على الصعيدِ العربي؛ وطرحِ العديدِ من المُقترحاتِ، أبرزُها لناحيةِ البُعدِ التعاقُدّي للحوسبةِ

السحابيةِ و عقد اتفاقٍ عربيّ للملاذ الآمنِ (Arab Safe Harbor)، قبل التوصّل إلى الخاتِمَة حيث سَنعْرُض لبعض الإستنتاجاتِ والمُقترحاتِ مع نافذَةٍ على المُستقبلِ.

الفقرة الأولى: مفهوم الحوسبة السحابية والإشكاليات التطبيقية والتشريعية:

كَلَمْحةٍ تاريخيةٍ، يعودُ استعمالُ مُصطلحَ الحوسبةِ إلى الستيناتِ مع مقولَةِ جون مكارثي Jhon MAKARSI مِن أنّه: "قد يتمُّ تنظيمُ الحوسبةِ لكي تُصبحَ خِدمةً عامةً في يومٍ من الأيامِ"، وقُورِنتْ هذه الحوسبةُ بتوفير الطاقَةِ والمرافِق، مثل الغاز والكهرباء. ويثار النقاش باستمرار حول مفهومِ الحوسبةِ السحابيّة، ما إذا كانت مجموعةَ تقنياتٍ، أو مجموعةَ خدماتٍ[٨]، أو مجموعةَ أنشطَةٍ، أو مجموعَةَ تطبيقاتٍ، أو مجموعَةً من التكنولوجياتِ المُختلفَةِ والعُروضِ السوقية. **مما ساهمَ، في تعقيد تعريفِها، لا سيما أنّه، وكلّ ما تقاربَتْ وجهاتُ النظَرِ في تعريفِها، تَتطوّر خدماتُها وتتَغيّرُ وتتسِعُ مما يُفاقمُ من جديدٍ عدمَ توحيدِ تعريفِها.** وهكذا تعدّدَت تعريفاتُها بِتعدُّد الجِهاتِ التي قدّمَت هذا التعريفَ. **الأمرُ الذي يُعرقِلُ تحديدَ تعريفٍ واضِحٍ ومُحدّد لها، وهي نُقطةُ الإنطِلاق الأهمّ لِتحديد الإطارِ التَشريعيّ للحَوسَبَةِ السحابيّةِ.** نذكرُ على سبيلِ المِثالِ تعريف الإتحاد الدولي للإتصالات لِلحوسَبَةِ السحابيّةِ على أنّها: "نموذَجٌ لتمكين مُستخدميّ الخدمات من النَفاذِ الشامِلِ والمُريحِ وتحت الطلبِ إلى مَجموعةٍ مُشتركَةٍ من موارِدَ الحوسَبَةِ القابِلةِ للتغيير التي يُمكن توفيرها على وَجْهِ السُرعَةِ وإطلاقها بأَقلّ جُهْدٍ إداريّ أو تدخُّل من جانِب مُقدّمِ الخِدمَةِ"[٩].

نشير إلى أنه توجد ثلاثة أنواع أساسية من نماذج خدمات الحوسبة السحابية هي: البنية التحتية كخدمة (Infrastructure as a service – IAAS)، المنصة كخدمة (Platform As A Service – PAAS)، والبرمجيات كخدمة (Software As A Service –SAAS).

كما أن هناك ثلاثة نماذج للحوسبة السحابية (Cloud Computing Types): الحوسبة السحابية الخاصة (Private Clouds)، الحوسبة السحابية العامة (Public Clouds)، والحوسبة السحابية المشتركة (أو الهجينة أو المجتمعية) (Hybrid Clouds). أما عن مقدمي خدمات الحوسبة السحابية (Cloud Computing Vendors): فهم مزودي خدمات الحوسبة السحابية للأفراد والشركات وحتى الدول الراغبة في شراء أو استئجار هذه الخدمات، ضمن مسؤولية الحفاظ على استمرارية هذه الخدمات وصيانتها على مدار الأيام والساعات. أهم مقدمو هذه الخدمات: Amazon – Rackspace – Vmware – GoGrid – Salesforce – Google...

أما عن أهم الخدمات والتطبيقات السحابية فهي: خدمات البريد الالكتروني (Gmail – Yahoo – Hotmail)، وخدمات التخزين السحابي (Box – Google Drive –SkyDrive – Dropbox)، وخدمات الموسيقى السحابية (Google music – Amazon Cloud Player – iTunes/iCloud – Music Creator)، والتطبيقات السحابية (Pixlr –Photoshop Express – Google Docs Editor، Jaycut، Aviary)، وأنظمة التشغيل السحابية (Google Chrome OS – Jolicloud)...

فيما يتعلّق **بِحجمِ الحَوسبَةِ السحابيّةِ** فتُفيدُ العديدُ من الإحصائياتِ عن نُموّها بِشكلٍ مُطْرِد في السنواتِ الأُخيرةِ واستمرار نموها في السنواتِ المُقْبلَةِ[١٠]. أما عن **مُميّزاتِها**، فلِلحوسبة السحابيّة، وكغيرها من مُفرزاتِ العولَمَةِ الإلكترونيّةِ، العديد من المَحاسِنِ والمَنافِعِ على صعيدِ الإدارةِ والتَكْلفَةِ والشركةِ والبياناتِ، أبرزُها: سُهولةُ الوصولُ والولوجُ إلى البياناتِ وقاعِدةُ المعلوماتُ والتطبيقاتُ، وتَوفيرُ الوقتُ ومصاريفُ كِلفة التجهيزاتِ الماديّةِ، والإعفاءُ من التَكلفَةِ الماديّةِ لِلتجهيزاتِ والمَفروشاتِ، والمَساحةُ التخزينيّةُ المُخصّصةُ للأرشيفِ، والتحرُّرُ من ضغوط والتزاماتِ القوانينِ التجاريةِ (كالعلامةِ التجاريةِ والسِجل التجاري)، والتحرُّر من العملِ المَكْتبي، وضمانُ استمراريةُ الخدماتِ، و**التأمينُ والحمايةُ**. إضافةً إلى العديدِ من الفوائدِ الإقتصاديةِ والتجاريةِ لأنظمَةِ الحوسبةِ السحابيةِ، فهي منجمُ ذهبُ القرنِ الواحدِ والعشرين وتكنولوجيا ستؤدّي إلى "تغييرَ قواعِدِ اللعب". وقد إعتَرَفَت نيللي كروز Neelie KROES، نائبةُ رئيسِ المُفوّضيَةِ الأُوروبيّةِ، بأنَّ خدماتِ الحوسبَةُ السحابيةِ توفّرُ مزايا ضَخْمةً لِلمواطنين والشركاتِ التجاريةِ، وبأنَّها تُعزّزُ الإقتصادَ الأُوروبيّ عموماً[١١].

وإذا كانت الدراساتُ الأوروبيةُ[١٢] تُحذّرُ من "المخاطِرِ الأمنيةِ للحوسبةِ السحابيةِ"، وخصوصاً بعد تمكّن جِهاتٍ مُعيّنةٍ من الإطّلاعِ على معلوماتِ الشركاتِ والأشخاصِ وحتى الأفرادِ، بِشكلٍ مُباشرٍ أو غير مُباشِرٍ، وهو ما ينتهِكُ الخصوصيّةُ ويترتّبُ عليه العديدُ من العواقِبِ الأمنيةِ؛ ومن المعلومِ، أنَّ الإتحادَ الأوروبيّ مُحصنٌ بالعديدِ من الإرشاداتِ والتوصِياتِ والإتفاقاتِ الثُنائيّةِ، فالسؤال الذي يُطرَحُ هنا ماذا بالنسبة إلى واقعَ الدُولِ العربيةِ؟ حيث أن العديد من هذه الدول لا ترغب في بدء استخدام الحوسبة السحابية وذلك للأسباب التالي ذكرها.

البند الأول: التحديات التطبيقية والقضايا التشريعية للحوسبة السحابية في الدول العربية:

تَتردَّدُ العديدُ من الدُولِ باتخاذَ القَرارِ بالإنتقالِ إلى الحوسبَةِ السحابيةِ، لِلعديدَ من الأسبابِ التاليةِ:

- عدم إمكانيةُ الحُصولُ على كُلّ المُستجداتِ الحديثَةِ للتطبيقاتِ والبرامجِ وبِأسعار مقبُولةٍ، وتهْميشُ عددٌ من الدولِ أوالمناطقِ غير المتوفّر لديْها خِدمة الإنترنيت، والحاجَةُ إلى مساحَةٍ تخزينيّةٍ إلكترونيةٍ

تَتسِعُ رُويداً رويداً لِلكم الهائِلِ من الأرشيفِ المَحْفوظِ، والأهم أَمن البياناتِ الخاصة والحكومية، وسريّتها بالنسبة للأفرادِ وللشركاتِ وللدُوَلِ بحدّ ذاتها.

- غِيابُ الإدارةُ الضريبيُّة عن أيةِ عمليةِ بيعٍ أو تفرُّغٍ أو شِراء قاعِدةِ معلوماتٍ[١٣]، مما يُسبّبُ خسارةً لِواردات خزينةِ الدولةِ، لا سيما في الدُوَلِ التي تُعتبرُ الضرائِبُ مَوْرداً أساسياً لها.
- تردُّد صانعي السياسةِ المحليّةِ العربيةِ والقرارِ الوطنيّ والإداريّ والسياسيّ بالإنتقالِ إلى الحَوْسبةِ السحابيةِ والإستفادةِ من خدماتِها.
- التَشكيكُ في قُدراتِ الحمايَةِ والتأمينِ لمُقدّمي الخدماتِ عِبر الحوسبَةِ السحابيَةِ.
- عدم الثِقة بِمزوّدي الخدماتِ[١٤]، وبالتقنياتِ الجديدةِ، ومُستوى مُقدّمي خدماتِ التطبيقاتِ السحابيةِ.
- عدم الوعي بأهميّة الإنتقالِ الإفتراضيّ إلى السَحَابةِ من قِبل المَسْؤولين والمَعنيّين بإتخاذَ القرارِ.
- ضُعْفُ التقدُّم على صعيد إقامةِ شبكةٍ وطنيّةٍ عِريضةِ النِطاقِ، وعدم تَطبيق سياساتٍ تقييديّةٍ على مُحتوى الإنترنت، وعدم تطبيقُ نَهْج تمييزيّ إزاء الشركاتِ التكنولوجيّةِ الأجنبيّةِ، وعدم توافر إطارٍ مُناسِبٍ لوضعَ معاييرِ تكنولوجيا المعلوماتِ والإتصالاتِ.
- عدم توفّر السُرعَةِ الكافيَةِ للإنترنت في بعض البُلْدانِ أو إرتفاع أَسْعارها؛ وعدم توفّر بُنْية تحتيّة رقميّة في البُلدانِ العربيةِ (حيث أنّ انقطاعَ خدمَةُ الإنترنت يعني إنقطاعَ خِدمةِ الحوسبَةِ السحابيةِ، وبالتالي توقفَ الإنترنت لدى بعض الشركاتِ قد يؤدّي إلى خسارةَ الملايين بل المليارات من الدولارات في دقائِقَ معدُودَةٍ).
- عدم توفّر أمن المعلوماتِ في الحوسبةِ السحابيةِ (فجميعُ معلوماتِ الشركاتِ والخدماتِ المُستأجرَةِ موجودَةٌ خارج نِطاقِ الشرِكةِ)، وبما أنّ معلوماتُ بعض الشركاتِ الخاصةِ ذات طابِعٌ خاصٌ وسرّي جداً فلا يُمكن المغامرةُ ووضعُ هذه المعلومات في مراكِزَ بياناتٍ مُستأجرةٍ مهما بلغَتْ درجةُ تطميناتِ الشركاتِ المُزوّدَةِ لهذه الخدَماتِ حول العالمِ. أضِفْ إلى ذلك العديد من مشاكلَ أمنِ المعْلوماتِ في السحابةِ الإلكترونيَةِ، والتي قد يُسبّبها معاً كُلْ مِنْ مُزوّد الخِدمةِ أو العميلِ. إنّما يقعُ العبءُ الأساسيُّ، على مُزوّد الخِدمةِ في إرساءَ بُنيةٍ تحتيّةٍ مُتطوّرةٍ وأدواتٍ ومُستودعاتٍ ومراكزَ تخزينٍ آمِنَةٍ، لا سيما إذا ما كان التَخْزينُ مُقابل بدَلٍ مادّي؛ في حين لا يَتطلَّب الأمرُ لدى العميل أكثرَ من إتصالَ سريعٍ مع الإنترنيت.
- عدم توفّر الأمان المعلوماتيّ بالنسبة إلى بَعضِ المُؤسساتِ ذات الطابِع الحُكوميّ (وهو سبب رئيسي لتردّدُ العديدُ من الدولِ العربيةِ في استخدامَ الحوسبَةِ السحابيّةِ).

- المخاوفُ البيئيّةُ، حيث أنّ مراكزَ البياناتِ الكبيرةِ تَستهلكُ كمياتٍ ضَخمةً من الطاقَةِ.
- نقصٌ في المعلوماتِ الدِعائيةِ والتوعويةِ حول أهميّة إستخدام هذه التقنيةِ، أيْ عدم توعيَة الرأي العامِ العربي حول كيفيّة استغلال هذه الخدمات، أو إدراك مخاطِرها المحتملة التي تُحيطُ بأمْن البياناتِ، ومِقدار القِيمةِ الحقيقيّةِ لهذه البياناتِ التي يُشار إليها على أنّها "نفطٌ جديدٌ" من المَنظورِ التِجاريّ، وما إذا كانَ يَحُقّ للمُستهلكين حقوقٌ اقتصاديّةٌ مقابل المُتاجرةِ ببياناتِهم[١٥].

الجدول التالي يوضح الأسباب التي تم ذكرها:

التحديات التطبيقية للحوسبة السحابية في الدول العربية:	
إمكانية الحصول على كل المستجدات التطبيقية الحديثة	عدم الوعي الكافي بالحوسبة السحابية
غياب الإدارة الضريبية	ضعف التقدم
تردد صانعي القرار	عدم توفر السرعة الكافية للإنترنيت أو كلفتها العالية
التشكيك في قدرات الحماية والتأمين	عدم توفر البيئة الرقمية
عدم الثقة بمودي الخدمات	المخاوف البيئية
غياب المراكز لقاعدة البيانات الضخمة	نقص المعلومات الدعائية والتوعوية

البند الثاني: التحديات التشريعية والتنظيمية للدول العربية منفردة

في الواقع، تُثيرُ مَسألةُ الإطارِ التشريعيّ للحوسبَةِ السحابيَةِ الكثيرَ من الإشكالياتِ، في الدولِ العربيةِ بشكلٍ خاص[١٦]، حيث هُناك غيابٌ عربيّ لقوانينَ خاصةٍ لِحمايةِ قواعدِ المعلوماتِ والبياناتِ بشكلٍ عام. ففي الأساسِ، تُعتبر نادرةٌ هي الدول العربية التي اعتمدَت قانوناً خاصاً لِحمايةِ البياناتِ الشخصيّةِ. فليس هناك سوى نصوصٌ مُبعثرةٌ في ثنايا تشريعاتٍ مُتفرقةٍ. كما أنّ أغلبيةَ الدُولِ العربيةِ تفتقرُ إلى آلياتِ تطبيقِ القواعِدِ التفصيليّةِ الخاصةِ بِحماية هذه البياناتِ وتنفيذِها. أضف أنّه، باتت المبادئُ التقليديّةُ، المحليّةُ والسِياديّةُ، في وضْعٍ من التحدّي والتجاذُبِ المُستمِر ما بين إحترام الحُرياتِ العامةِ وما بين مُتطلّباتِ الأمْنِ والسلامَةِ العامَةِ؛ وباتَتْ الإشكاليةُ قائمةً حول تحديدِ مدى إحترامِ الحُريّاتِ والخُصوصيات الشخصيّة والحُؤولِ دون التعسُّف في التدقيق والتدخّل من قِبل السُلطاتِ العامَةِ وغيرها.

أما على صعيد القوانينِ العامَةِ، فقد تمّ تعديَل العديدُ من القوانينِ العربيةِ، لا سيما قانون العقوبات العامة وقانون أصول المحاكمات المدنية، لِتتضمَّنْ الحمايَةَ القانونيةَ للمعلوماتِ وللبياناتِ، والمُلكيّةِ الفِكرية، والمُصنّفَاتِ الرقميّة. كما صدرَت العديدُ من القوانينِ المعلوماتيّةِ العربيةِ، والمُعاملاتِ الإلكترونيّةِ، والتِجارة الإلكترونيّةِ وجرائم المعلوماتيّةِ، لِتجريمَ العديدِ من الأفعالِ المُرتكبةِ بواسطة تكنولوجيا المعلوماتِ والإتصالات

وفي الفضاءِ السيبرانيّ وسائر جرائم الإنترنيت والإتصالاتِ، والمُساواة بين الرُكنِ الرقميّ والرُكنِ المادّي. وتعتبر دول الخليج من أوائِلَ الدُولِ العربيّةِ التي بادرَت إلى تعبيدَ طريقِ الحوسبَةِ السحابِيَةِ. (وسيتم عرض الدول العربية بحسب الترتيب الأبجدي).

الجدول التالي يعطي ملخصاً عن الواقع التشريعي للحوسبة السحابية في الدول العربية:

ملخص للواقع التشريعي والتنظيمي للحوسبة السحابية في الدول العربية				
اسم الدولة	**التشريعات السيبرانية**	**قواعد سلوكية**	**استراتيجية وطنية لتحول نحو الحوسبة السحابية**	**تدريب وتوعية**
الأردن	قانونَ الإحصاءاتِ العامةِ، المُؤقتِ عام ٢٠٠٨؛ قانون جرائم أنظمة المعلومات، رقم ٢٠١٠/٣٠ قانون الإتصالات السلكية واللاسلكية رقم ٢١ /٢٠١١).	**لا يوجد**	اطلاق منصة الحوسبة السحابية عام ٢٠١٤؛ وثيقة السياسة العامة للحكومة وفي قطاعات الاتصالات وتكنولوجيا المعلومات؛ انشاء مركز تكنولوجيا المعلومات	نقص في التدريب والتوعية
الإمارات العربية المتحدة	قانون "مؤسسة الإمارات للاتصالات" (رقم1 لسنة١٩٩١) ؛ قانون تنظيم قطاع الاتصالات رقم ٢٠٠٣/٣؛ "قانون التوقيع الإلكتروني والتجارة"، عام ٢٠٠٢، ؛قانون اتحادي رقم ٢٠٠٦/١ في شأن المعاملات والتجارة الإلكترونية؛ قانون امارة دبي الخاص بالمعاملات والتجارة الالكترونية رقم 2/2002 بشأن المعاملات والتجارة الالكترونية؛ القانون الإتحادي المُتعلّق بـ"مكافحةِ جرائم تقنية المعلومات"، رقم ٢٠٠٦/٢ ؛ مرسوم بقانون اتحادي رقم ٥ /٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات؛ التعميم رقم ٢٠١٣/٦ بشأن سياسة ومعايير حكومة أبو ظبي لأمن المعلومات؛ قرار مجلس الوزراء الإماراتي رقم ٢٠١٣/٢١ المتعلق بلائحة أمن المعلومات في الجهات الإتحادية؛ قانون حماية البيانات الشخصية – رقم ١ /٢٠٠٧ – خاص بالمركز المالي الدولي لدبي DIFC؛ قانون حماية البيانات الشخصية – رقم ٢٠٠٦/١١؛ قانون إمارة دبي، لنشر وتبادل البيانات (قانون البيانات المفتوحة في ١٧ أكتوبر ٢٠١٥)؛ قانون إمارة دبي، المُتعلّق، بإنشاءِ وحمايةِ شبكةِ الإتصالاتِ الصادر عام ٢٠٠٢، وقانون رقم ٢٠٠٤/٥ حول الأمنِ المعلوماتيّ.؛ قرار المجلس التنفيذي رقم ٢٠١٢/١٣ بشأن أمن المعلومات في إمارة دبي.	**يوجد انما تتطلب تطوير**	استراتيجية وطنية وقواعد ادارية للتحول نحو الحوسبة السحابية	البدء بتدريب متخصص وتوعية عامة
البحرين	قانون الاتصالات والإنترنيت رقم ٤٨ لعام ٢٠٠٢؛ القانون رقم ٢٨ /٢٠٠٢ المتعلق بالمعاملات والتجارة الإلكترونية، والقانون رقم ٢٠١٤/٦٠ بشأن جرائم تقنية المعلومات؛ المرسوم رقم ٩ لعام ٢٠٠٢ لإعادة تنظيم الجهاز المركزي للمعلومات؛ والقرار رقم ٢٥ لعام ٢٠٠٥، لتشكيل لجنة عليا لتقنية المعلومات والإتصالات.	**لا يوجد**	عام ٢٠١٥ إطلاق مشروع لتسريع الأعمال عبر الحوسبة السحابية	نقص في التدريب والتوعية
الجزائر	قانون رقم ٢٠٠٩/٤، بعض مشاريع القوانين	لا يوجد	إعداد استراتيجية وطنية (٢٠١٤-٢٠٢٠) تتضمن الحوسبة السحابية والادارة الالكترونية	نقص في التدريب والتوعية
السعودية	نظامُ مكافحة جرائم المعلوماتية لعام ٢٠٠٧؛ قرار المجلس الوزراي رقم ٤٠ /٢٠٠٦، المتعلق بضوابط التعاملات الإلكترونية الحكومية؛ القرار رقم ٦٦٦٧ المتعلق بشروط مزاولة مهنة الإستشارات في مجال الإتصالات وتقنية المعلومات؛ مشروع قانون حول حماية البيانات.	لا يوجد	ارادة سياسية وادارية للتحوّل نحو الجوسبة اسحابية؛ تشكيل هيئة الاتصالات وتقنية المعلومات.	نقص في التدريب والتوعية
السودان	مبادئ دستورية لحماية السرية والخصوصية؛ قانون المعاملات الإلكترونية عام ٢٠٠٧؛ وقانون مكافحة جرائم المعلوماتية عام ٢٠٠٧ .	لا يوجد	مبادرات حكومية	برامج تدريبية متخصصة والبدء بحملات توعوية

الصومال	لا يوجد	لا يوجد	لا يوجد	لا يوجد
العراق	قانون حماية المستهلك رقم ١ /٢٠١٠؛ القانون رقم ٢٠١٢/٧٨، المتعلق بالتوقيع الإلكتروني والمعاملات الإلكترونية.	لا يوجد	استراتيجية وطنية وخطة عمل الحوكمة الإلكترونية (٢٠١٢-٢٠١٥)	نقص في التدريب والتوعية
الكويت	القانون رقم (٥) لسنة1999 لحماية المصنفات والحاسب الآلي من البرامج وقواعد البيانات؛ قانون رقم ٢٠١٤/٣٧ استحداث هيئة تنظيم الاتصالات وتقنية المعلومات؛ مشروع قانون للمعاملات الالكترونية	لا يوجد	مبادرات وطنية	نقص في التدريب والتوعية
المغرب	مبادئ دستورية لحماية السرية؛ قانون رقم ٢٠٠٩/٨ لحماية البيانات الشخصية؛ قانون رقم ٢٠٠٣/٧ لمكافحة جرائم المعلوماتية؛ قانون رقم ٥٣,٠٥ المتعلق بالتبادل الالكتروني للمعطيات الالكترونية؛ قانون حماية المستهلك على الانترنيت رقم ٢٠٠٨/٣١	لا يوجد	مبادرات حكومية	نقص في التدريب والتوعية
اليمن	القانون رقم ٤٠ لعام ٢٠٠٦ بشأن أنظمة الدفع العمليات المالية والمصرفية الإلكترونية؛ قرار مجلس الوزراء رقم ٢٠٠٢/٤ " لإنشاء مدينة تكنولوجيا الإتصالات والمعلومات؛ مشروع قانون لحماية المعلومات	لا يوجد	خدمات تقنية تعتمد على الحوسبة السحابية	نقص في التدريب والتوعية
تونس	قانون رقم ٢٠٠٤/٦٣ المتعلق بحماية البيانات الشخصية؛ قانون ١٩٩٨/٣٨ المتعلق بمجلة البريد؛ قانون عدد ٢٠٠٠/٨٣ المتعلق بالمبادلات والتجارة الإلكترونية؛ الأمر عدد ٢٠٠٠/٢٣٣١ المتعلّق بضبط التنظيم الإداري والمالي وطرق تيسير الوكالة الوطنية للمصادقة الإلكترونية؛ الأمر ٢٠٠١/١٩٦٧ المتعلق لضبط خدمات المصادقة الإلكترونية، الأمر رقم ٢٠٠١/١٩٦٨؛ قانون رقم ٢٠٠٤/٥ المتعلق بتنظيم مجال السلامة المعلوماتية؛ قانون رقم ٢٠٠٥/٥١ المتعلق بالتحويل الإلكتروني؛ القانون التوجيهي عدد ٢٠٠٧/١٣ المتعلق بإرساء الإقتصاد الرقمي؛ أمر ٢٠٠٧/١٢٧٤ قائمة الأنشطة المرتبطة بالإقتصاد الرقمي.	لا يوجد	استراتيجية وطنية للتحول نحو الحوسبة السحابية (٢٠١٥)	البدء في تدريب متخصص وحملات توعوية
جزر القمر	لا يوجد	لا يوجد	لا يوجد	لا يوجد
جيبوتي	قانون حماية المستهلك لعام ٢٠٠٨	لا يوجد	مبادرات وطنية	نقص في اتدريب والتوعية
سلطنة عمان	قانون المُعاملات الإلكترونيةِ (٢٠٠٨/٦٩)؛ قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢.	لا يوجد	ارادة حكومية	البدء في تدريب متخصص وحملات توعوية
سوريا	قانونَ التوقيع الإلكترونيّ وخدمات الشبكة، رقم ٢٠٠٩/٤؛ قانونَ تنظيم قطاع الإتصالاتِ، رقم ٢٠١٠/١٨؛قانون الإعلام بالمرسوم الإشتراعي، رقم ١٠٨، تاريخ ٨ آب/أغسطس ٢٠١١؛ المرسوم الإشتراعي، رقم ٢٠١٢/١٧ المُتعلّق بِتنظيمَ التواصِلِ على الشبَكَة ومكافحة جريمَةِ المعلوماتيّةِ.	لا يوجد	استراتيجية وطنية لتقانة المعلومات (٢٠٠٤) استراتيجية وطنية للحكومة الالكترونية (٢٠١٠-٢٠٠٩)	نقص في اتدريب والتوعية

فلسطين	قانون الإحصاءات العامة رقم ٤ /٢٠٠٠ بشأن الحق في الوصول الى معلومات الإحصاءات؛ قانون المعاملات الإلكترونية لعام ٢٠١٠. مرسوم رقم ٣٥ لعام ٢٠٠٤ لحق الوصول الى شبكة المعلومات العالمية. قرارات مجلس الوزراءِ في فلسطين لحقَّ النفاذِ إلى الشبَكَةِ العالميَةِ (الإنترنيت) والبريد الإلكتروني عبر مركز الحاسوب الحكومي؛ بشأن منع بيع وتسويق خدمات الإتصالات وتقنية المعلومات والبريد السريع؛ للمصادقة على السياسات العامة لإستخدام الحاسوب وشبكة الإنترنيت في المؤسسات العامة؛	لا يوجد	الاستراتيجية الوطنية للإتصالات وتكنولوجيا المعلومات مبادرة فلسطين الرقمية	نقص في اتدريب والتوعية
قطر	مبادئ دستورية لحماية الخصوصية؛ قانونُ الإتصالاتِ، في قطر رقم ٢٠٠٦/٣٤؛ قانون معاملات التِجارةِ الإلكترونية رقم ٢٠١٠/١٦ (في ٢٠١٠/٨/١٩)؛ قانون مركز قطر المالي - قانون رقم (٧) لسنة ٢٠٠٥ بإصدار قانون مركز قطر للمال؛ مشروع قانون حول خصوصية البيانات.	لا يوجد	انشاء السحابة الالكترونية الحكومية الاستراتيجية الوطنية للأمن السيبراني (٢٠١٤)	نقص في التدريب والتوعية ابحاث حول الحوسبة السحابية
لبنان	القانون رقم ١٤٠ بتاريخ ٢٧ تشرين الأول/أكتوبر ١٩٩٩ المتعلّق بصون الحق بسرية المكالمات الهاتفية؛ مشروع قانون حول المعاملات الالكترونية وجرائم المعلوماتية.	لا يوجد	اعداد خطة وطنية لحماية وأمن الفضاء السيبراني في لنان (٢٠١٢)؛ عام ٢٠١٥ اطلاق رؤية الإتصالات الرقمية لعام ٢٠٢٠	نقص في التدريب والتوعية
ليبيا	مشاريع قوانين حول المعاملات الالكترونية وجرائم المعلوماتية	لا يوجد	اطلاق مبادرة ليبيا الإلكترونية	لا يوجد
مصر	مبادئ دستورية؛ قانون تنظيم الإتصالات لعام ٢٠٠٣؛ قانون رقم ١٢٠ /٢٠٠٨ لإنشاء المحاكم الاقتصادية؛ مشاريع قوانين متخصصة.	لا يوجد	مبادرات ادارية وتوقيع مذكرات تفاهم دولية لتبادل الخبرات	البدء بدورات تدريبية وتوعوية
موريتانيا	مشروع قانون حول الاطار القانوني للمجتمع الموريتاني للمعلومات	لا يوجد	مبادرات حكومية	لا يوجد

١. **<u>الأردن</u>:**

على الصعيدِ الإداري، وفي حزيران/يونيو ٢٠١٤، أطلقَتْ وزارةُ الاتصالات وتكنولوجيا المعلومات في الأردن "منصةَ الحوسبةِ السحابيةِ الخاصةِ" التي تمَّ تنفيذُها بالتعاونِ مع شركة مايكروسوفت؛ الأمرُ الذي يدعَمُ إحتياجاتِ القِطاعِ العامِ وإحتياجاتِ الشركات الناشِئَة التي لا تَمتلكْ بُنيةً تحتيةً داعمةً لتطويرَ أفكارِها ومُنتجاتها من البرمجيات والخدَمات الإلكترونية. كما وقَّعتْ شركةُ الإتصالات الأردنية "أمنية" اتفاقيةً لِخدماتَ الحوسبَةِ السحابيةِ مع شركة مايكروسوفت لتوفيرَ خدماتِ الحوسبَةِ السحابيةِ لمشغل أمنية. وفي اكتوبر ٢٠١٥، أطلقَتْ "شركة الخدمات الفنية للكمبيوتر STS" منصتَها المُتخصّصة بِحلولَ الحوسبةِ السحابيةِ، مما يُحوّل خدماتِها ومُنتجاتِها لِتقدَّم عِبر "السحابةِ". كما أنّ هناك مبادراتٍ منذ عام ٢٠١٤

لِتطبيقَ تكنولوجيا حلولِ التعليمِ السحابيةِ في بَعض المدارسِ الأردنيةِ، والتي تُمكّن المُستخدمُ من الدخولِ إليها من المدرسةِ أو المنزلِ بإستخدامَ الهواتِفِ الذكيّةِ وأَجهزة الكومبيوتِر اللوحيّةِ.

على الصعيدِ التشريعيّ، أصدَرَ المشرّعُ الأردنيّ قانونَ الإحصاءاتِ العامةِ المُؤقتِ الصادرِ في الأردن عام ٢٠٠٨، والذي يتضمّنُ مواداً خاصةً بِسريّة البياناتِ الإحصائيةِ وحمايتها ومنع افشائِها (المواد ١١ و١٢ و١٦ و١٧ و ٥١). وفي عام ٢٠١٠، أصدَرَ "قانون جرائم أنظمة المعلومات" رقم ٣٠ (جريدة رسمية رقم ٥٠٥٦ – تاريخ ٢٠١٠/٩/١٦ – صفحة ٥٣٣٤) الذي قَسَّمَ جرائمَ المعلوماتيةِ إلى نوعَين، ومن ضِمنها الجرائِمِ الواقعَةِ بِاستخدامَ أنظمةِ المعلوماتِ كأَداة لإرتكاب بعض الجرائِمِ، وجرائم "التعدّي على الخصوصيةِ" ومن أبرَز صُورها: جريمَةُ إفشاءُ البياناتِ أو المعلوماتِ عن طريقَ الدُخولِ غير المَشروعِ لِنظامَ معلوماتيّ؛ جَريمةُ إفشاءُ بياناتٍ أو معلوماتٍ عن طريقَ إدخالِ أو نشر أو إستخدامَ برامِجِ إلكترونيّةٍ؛ وجريمَةُ التنصّتِ على المُراسلاتِ الإلكترونيّةِ.

وكان الأردن قد أصدر قانون الإتصالات السلكية واللاسلكية رقم ١٣ لسنة ١٩٩٥، والذي عدل بموجب قانون التعديل رقم ٢١ لسنة ٢٠١١ (الجريدة الرسمية رقم ٤٠٧٢ بتاريخ ١٩٩٥/١٠/٠١.) ويحتوي هذا القانون على أحكام المنافسة في قطاعي الاتصالات وتكنولوجيا المعلومات، المنصوص عليها في المواد ٦ و١٢ و٢٦ و٢٨ . كما ينص على أحكام لترخيص شبكات الاتصالات، وتجديد الرخص وتعديلها والغاؤها، ومراقبة المرخصين وحماية المستيفدين.

في العام ٢٠٠٣، تبنّت الحكومة الأردنية «وثيقة السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات» والتي ركزت على تحرير قطاع الاتصالات بالكامل. في ٢٠٠٧، أقرّت وثيقة سياسة جديدة ركزت على المنافسة في قطاع الاتصالات، وتبني نظام متكامل للترخيص، وإتاحة بعض الترددات الراديوية للاستخدام من خلال الترخيص العام المفتوح. وفي نهاية العام ٢٠١٢، أقرت الحكومة وثيقة السياسة العامة المعمول بها حالياً حيث ركزت على قضايا المنافسة الفعالة والاندماج[١٧].

كما أنشأت الأردن "مركز تكنولوجيا المعلومات الوطني، National Information Technology Center الذي يهدف الى تأدية دور المرجعية التنفيذية لتكنولوجيا المعلومات في المؤسسات الحكومية في المواضيع المتعلقة بتوظيف موارد تكنولوجيا المعلومات ووضع المعايير لها. كما أنشأت الأردن "المركز الوطني للأمن وإدارة الأزمات"، (الجريدة الرسمية عدد ٥٣٣٥، رقم 20 لسنة ٢٠١٥)، وتتمثل طبيعة عمله في الإغاثة في حالات الكوارث وادارة الازمات.

٢. الإمارات العربية المتحدة:

على الصعيدِ التنظميّ والإداريّ، شهدت الإماراتُ تحوّلاتٍ كبيرةً نحو اعتمادِ الحَوسبةِ السحابيةِ وتُعدّ حالياً من أكبرَ الأسواقِ الخليجيّةِ لها، حيث يُقدّرُ حَجمُ هذه السوقَ في الدولةِ بـ ٥ مليارات درهم خلال العام الحالي ٢٠١٥. وأشارَ خُبراءٌ في هذا المجالِ إلى أنَّ جميعَ المشاريعِ في القِطاعينِ العامِ والخاصِ في دولةِ الإماراتِ العربيةِ المُتحدةِ تشهَدُ تَحوّلاتٍ تقنيةً كبيرةً على صعيدِ إعتمادِ حُلولِ الحوسبَةِ السحابيةِ وتَسريعِ نَشْرِ التطبيقاتِ القائِمةِ على السحابَةِ والمُلائِمةِ لإحتياجاتِ الأعمالِ، والإستجابَةِ على نحوٍ أسرعْ لِلفرصَ التجاريةِ الجديدةِ بإستخدامَ الحلولِ السحابيةِ، ودمج خدماتِ السحابةِ العامةِ والتطبيقاتِ في الموقَعِ للحصولَ على بُنيةٍ تحتيّةٍ قويةٍ لتكنولوجيا المعلوماتِ، وتوظيف البُنيةِ التَحتيّةِ كخِدمةٍ والبرمجياتِ كخدمةٍ لِتعزيزَ الكفاءَةِ والإنتاجيةِ ونموذج الأعمالِ المُبتكِر، وتطوير نماذِج عائِداتٍ جديدةٍ للأسواقَ الثانويَةِ.

أما على الصعيدِ التشريعيّ، فلا يوجَدْ في الإماراتِ العربيةِ المُتحدَة أيّ تشريع خاص بِحماية البياناتِ، على الرغم من أنَّ الحقَّ في الخُصوصيةِ منصوصٌ عليه في الدُستورِ الإماراتيّ وفي مُختلف القوانينِ. إذ ينصُّ هذا الدستورُ على أنْ يتمتعَ الفردُ بـ "حريّة الإتصالِ بواسطة البريدِ، أو البرقِ، أو بأي وسيلة إتصال أخرى، وتكون سِريّةُ الإتصالاتِ مكفولةً وِفقاً للقانون. وبالإضافةِ إلى ذلك، ينصُّ قانونُ العقوباتِ الإماراتيّ (رقم ١٩٨٧/٣) على حقوق معينةٍ في شأن الخصوصيّةِ وحِماية البياناتِ الشخصيةِ (المواد ٣٢٧ الى ٣٣٠ في الباب الخامس المختص بالجرائم الماسة بالأسرة والمادة ٢٧٩ من قانون العقوبات الإماراتي التي تنص على جريمة الإعتداء على أي وسيلة من وسائل الإتصال السلكية واللاسلكية).

وكانت الإمارات قد أصدرت قانون "مؤسسة الإمارات للاتصالات" (رقم1 لسنة ١٩٩١) الذي يعتبر القانون الأول المنظم لشؤون الاتصالات السلكية واللاسلكية بالدولة، وقد أنشأ هذا القانون مؤسسة الإمارات للاتصالات وحدد أهدافها وأغراضها واختصاصاتها، وأولاها حصرية حق نقل الاتصالات السلكية واللاسلكية وتشغيل وصيانة وتطوير نظام الاتصالات العامة في الدولة، وكذلك بين الدولة والخارج، واشتمل القانون في الفصل السادس عشر منه على العقوبات التي توقع على مخالفة أحكامه (المواد ٤٥ و٤٦) .

ثم صدر قانون تنظيم قطاع الاتصالات رقم (٣) لسنة ٢٠٠٣ ليعدّل بعض أحكام قانون مؤسسة الإمارات، وبهدف تنظيم عمل شركات الاتصالات بالدولة، وقد أنشأ هيئة جديدة تسمى هيئة تنظيم قطاع الاتصالات بالدولة، وحددت المادة (١٢) مهام وصلاحيات واختصاصات الهيئة بأنها هي السلطة المختصة بالرقابة على قطاع الاتصالات وورد بالباب التاسع من هذا القانون مجموعة مواد تجرم بعض الأفعال وتفرض عقوبات على مخالفة ألأحكام والالتزامات التي يفرضها القانون (المواد ٧١ و٧٢) .

عام ٢٠٠٢ صدر قانون إمارة دبي رقم (2) بشأن "المعاملات والتجارة الالكترونية"[١٨]، بهدف تطوير وتعزيز التجارة الإلكترونية من خلال تسهيل المراسلات الالكترونية، ونقل المستندات الإلكترونية، وازالة عوائق تطبيق التجارة الالكترونية والمعاملات الالكترونية، والتقليل من فرص التزوير والاحتيال الالكترونيين، وتعزيز ثقة الجمهور في سلامة المعلومات وصحتها (م. ٣). ايضا بهدف تحديد متطلبات المعاملات الالكترونية (م. ٧)، وانشاء العقود الالكترونية وصحتها (المواد ١٣ لغاية ١٨)، وكيفية انشاء السجلات والتوقيعات الالكترونية المحمية (المواد ١٩ لغاية ٢٢)، وتحديد الأحكام المتصلة بالشهادات وخدمات التصديق (المواد ٢٣ لغاية ٢٦)، والاستخدام الحكومي للسجلات والتوقيعات الالكترونية وقبول الايداع والإصدار (م. ٢٧). كما يحدد القانون المذكور العقوبات المترتبة على ارتكاب اي فعل يشكل جريمة بموجب التشريعات النافذة باستخدام أي وسيلة الكترونية (المواد ٢٨ لغاية ٣٥).

في السياق ذاته، أصدرت الإمارات قانونا اتحادياً رقم ١ لعام ٢٠٠٦، في شأن "المعاملات والتجارة الإلكترونية"[١٩] بهدف حماية حقوق المتعاملين الكترونيا وتحديد التزماتهم (م. ٣)، وتحديد متطلبات المعاملات الإلكترونية من المراسلات الإلكترونية (م. ٤)، وحفظ السجلات الإلكترونية (م. ٥)، وقبول التعامل الإلكتروني (م. ٦)، والكتابة والتوقيع الإلكترونيين (المواد ٨ و ٩)، وقبول البينة الإلكترونية وحجيتها (م. ١٠). كما ينص القانون المذكور على إبرام العقود الالكترونية وصحتها (م. ١١)، والمعاملات الالكترونية المؤتمتة (م. ١٢) والإسناد (م. ١٣)، والإقرار بالإستلام (م. ١٤)، وزمان ومكان إرسال الرسائل واستلامها (م. ١٥)، والسجلات والتوقيعات الالكترونية المحمية (المواد ١٦ و١٧)، والاعتماد على التوقيعات وشهادات المصادقة الإلكترونية (م. ١٨)، وواجبات الموقع الكترونياً (م. ١٩). كما يتضمّن هذا القانون الاتحادي الأحكام المتصلة بشهادات المصادقة الإلكترونية وخدمات التصديق ومراقبها (المواد ٢٠ و ٢١)، والإعتراف بشهادات المصادقة الإلكترونية والتوقيعات الإلكترونية الأجنبية (م. ٢٣)، والاستخدام الحكومي للسجلات والتوقيعات الإلكترونية (م. ٢٤ و ٢٥)، وينص أخيراً على العقوبات المترتبة على مخالفة التشريعات النافذة باستخدام وسائل الكترونية (المواد ٢٦ لغاية ٣٣).

وهناك أيضاً القانون الإتحادي المُتعلّق بـ "مكافحةِ جرائم تقنية المعلومات" رقم ٢/٢٠٠٦[٢٠]، الذي كان يُعدّ من القوانين النموذجيّةِ في الدُولِ العربيةِ. يشمل هذا القانون أغلب جرائم المعلوماتية ومنها: التوصل بغير وجه حق إلى موقع أو نظام معلوماتي بدخول الموقع أو النظام، أو يتجاوز مدخل مصرح به، والتعدي على البيانات الشخصية، وإلغاء بيانات أو معلومات، أو حذفها، أو تدميرها، أو إفشاؤها، أو إتلافها، أو تغييرها، أو إعادة نشرها.

إلا أنّ اتحادُ الإمارات أصدرَ المرسوم الإتحادي لمكافحة جرائم تقنية المعلومات بقانون رقم 2012/٥[٢١]، والذي ألغى بموجبه قانون مكافحة جرائم تقنية المعلومات (رقم ٢ لعام ٢٠٠٦). ولكنه لم ينصْ على قواعِدَ إجرائية ومُفصّلة، وخاصة فيما يتعلق بالتحقيقاتِ الجزائيةِ[٢٢].

ويعتبر هذا القانون قانوناً حديثاً وعصرياً لِمكافحةَ جرائِمِ السيبرانيّةِ، لا سيما لناحية النص على تجريم دخول موقع الكتروني أو أي نظام معلومات الكتروني أو شبكة معلومات أو وسيلة معلومات، بدون تصريح أو بتجاوز حدود التصريح (م. ٢ و م. ١٤)، أو إعاقة الوصول إليهم (م. ٨)، أو إيقافهم أو تعطيلهم (م. ١٠)، أو للحصول على بيانات حكومية أو معلومات سرية مالية أو اقتصادية (م. ٤)، طبية أو صحية (م. ٧) أو تغيير تصميم موقع أو إتلافه (م. ٥)، أو تزوير سندات الكترونية حكومية (م. ٦)، أو التحايل على العنوان البروتوكولي للإنترنت (م. ٩)، أو ارتكاب جرائم الإحتيال الالكتروني (م. ١١)، والابتزاز الالكتروني (م. ١٦)، والقمار الالكتروني وجرائم ضد الآداب العامة (المواد ١٧ لغاية٢٠)، والاستيلاء على النقود الالكترونية (م. ١٢ وم. ١٣)، واعتراض اتصالات الغير (م. ١٥)، إو الإعتداء على البيانات الخاصة (م. ٢١ و ٢٢)، والاتجار بالبشر (م. ٢٣)، أو إثارة الفتنة أو العنصرية (م. ٢٤)، أو الاتجار بالأسلحة (م. ٢٥)، الاتجار بالمخدرات (م. ٣٦)، أو الاتجار بالتحف الأثرية والفنية (م. ٣٤)، أو الإرهاب الالكتروني (م. ٢٦)، وسائر الجرائم التي تنال من هيبة الدولة ومكانتها وأمن الدولة الداخلي أو الخارجي (م. ٢٨ لغاية ٣٢ والمواد ٣٨ و ٤٤)، أو الإساءة إلى المقدسات والشعائر الدينية (م. ٣٥)، وغسيل الأموال (م. ٣٧).

وفي عام ٢٠١٣، أصدرت الإمارات العربية المتحدة التعميم رقم ٦ بشأن سياسة ومعايير حكومة أبو ظبي لأمن المعلومات. كما أصدر مجلس الوزراء الإماراتي القرار رقم ٢٠١٣/٢١ المتعلق بلائحة أمن المعلومات في الجهات الإتحادية، وبهدف تعزيز مفهوم أمن المعلومات وتوفير إطار قانوني لضمان أمن الأصول المعلوماتية وتحديد معايير الإستخدام الأمثل لها، وتشجيع التطبيق الفعال للأمن الإلكتروني وإيجاد بيئة آمنة في الجهات الإتحادية لحفظ المعلومات وضمان سرية المعلومات والبنية الأساسية للشبكة.

على صعيد الأجهزة المختصة نُشيرُ إلى أنّ الإماراتِ العربيةَ قد أنشأَتْ "مركز التصديق الإلكتروني" الذي طوّرَ "مشروعَ الهيئةِ الرقميّة". وفي عام ٢٠١٠، أصدَرَت "هيئة تنظيم الإتصالاتِ الإماراتية" مرسوماً لِضبطِ الإتصالاتِ التسويقيّةِ غير المرغوبِ بها والحدّ منها.

وفي عام ٢٠٠٨، أنشأت الإمارات "مركز الإستجابة لطوارئ الحاسب الآلي" aeCERT[٢٣]، بهدف تحسين معايير وممارسات أمن المعلومات وحماية البنية الأساسية لتقنيات المعلومات من المخاطر والهجمات السيبرانية.

كما أقرّ مركز دبي المالي العالمي[٢٤](DIFC) قوانينَ خاصةً تتضمّنُ حمايةَ البياناتِ واللوائحِ الخاصةِ بهم، تنسجِمُ مع توجيه الإتحادِ الأوروبيّ الخاص بِحمايةِ البياناتِ EC/46/95[٢٥]، وإرشادات الأسكوا، ومنظمة التنمية والتعاون الإقتصادي الأوروبية (OECD). إلّا أنّ تطبيقَ هذه الأحكامُ القانونية يتم فقط على الأنشِطَةِ الخاصةِ بهذا المركزِ الماليَة والخدماتِ المصرفِيَةِ، أو على التحويلاتِ التي تتمّ من هذِا المركزِ إلى خارجها، ولغاياتٍ إحصائيّةٍ فحسب.

وقد جاءَتْ أحكام قانونَ إمارة دبي لِنشر وتبادُل البياناتِ (قانون البيانات المفتوحة في ١٧ أكتوبر ٢٠١٥)[٢٦]، لِتنصّ على العديدِ من الأحكامِ من حيث أصول تجميعِ البياناتِ وقانونيتِها وأمان مُعالجتها وتحديثها ضمن مُدّةٍ زمنيّةٍ مُحدّدة (م. ٨)، وموافقة صاحب البياناتِ الصريحةِ، وضروريةِ المُعالجةِ (م. ٩)، والمُوافقة الخطيّة الصريحة (م. ١٠)، وتأمين الحِمايَةِ المناسبة لدى نقل البياناتِ إلى الخارجِ (م. ١١ و ١٢)، إضافةً إلى حقَّ الإطلاعِ والتصحيحِ (م. ١٧)، ومسؤولياتِ وواجباتِ مُفوّض حِماية البياناتِ (م. ١٨). ويضَعُ القانونُ المذكورُ آلياتٍ واضحةً وجِهةً مُحدّدة بالإمارةِ مُختصّةً للإشراف على تصنيفَ البياناتِ، ووضع معاييرِ لقواعدَ المعلوماتِ فيها، ومُتابعةِ نشرِها وتبادلِها بين الجِهاتِ، وتسهيلِ الحصولِ عليها، وتوحيدِ آلياتِ تخزينِها، وتصنيفِها، وتوحيدِ البياناتِ ضِمن منصةٍ واحدةٍ لِجميعَ دوائِرِ إمارة دبي. أيضاً يعملُ القانونُ على زيادةَ القُدرةِ التنافسيّةِ لِمزوّدي البياناتِ، وتعزيزِ الشفافيةِ في تبادلَ البياناتِ، والتناغمِ بين الخدماتِ المُقدّمةِ وخُصوصيّة الجِهاتِ المحليّة، مما يهدفُ إلى خلقَ بيئةٍ تشريعيةٍ مُتكاملةٍ، وتطويرَ جيلٍ جديدٍ من الخدماتِ الذكيّةِ المُتكاملةِ، وإستكمال البِناءِ التشريعيّ لمدينةِ "دبي الذكية".

على خطٍّ مُوازٍ، لا بُدّ من ذكر قانون إمارة دبي المُتعلّق بـ "إنشاءَ وحمايةِ شبكةِ الإتصالاتِ" الصادر عام ٢٠٠٢[٢٧]، وفي ٢٧ يناير من عام ٢٠١٢ صدر قرار المجلس التنفيذي رقم ١٣ بشأن أمن المعلومات في إمارة دبي[٢٨]. وفي عام ٢٠١٤ أنشأت دبي "مركزا للأمن الإلكتروني ومكافحة جرائم المعلوماتية[٢٩]".

٣. البحرين:

في نوفمبر ٢٠١٥، تمّ إطلاقُ أوّلَ مشروعٍ لِتسريعَ الأعمالِ عِبر الحوسبَةِ السحابيَةِ لِدولَ مجْلسِ التعاونِ الخليجيّ من مركزِهِ في البحرين بالتعاونِ مع شركة Amazon Web ، وذلك بِهدف مُواكبة التِقنياتِ والأولوياتِ الاقتصاديةِ، وكبديل حديثٍ للنفطِ يَستحقُّ العنايةَ لِتحقيقَ اقتصاد مُستدام في المنطقَةِ، مما ينعكِسُ على المؤسساتِ البحرينيةِ للتوجّه نحو إعتماد التقنيةِ الرقميّةِ وتحسينِ القُدراتِ الوطنيةِ وتحسين التعليمِ.

على الصعيد التشريعي، أصدرت البحرين سلسلة من القوانين المتعلقة بالفضاء السيبراني، أبرزها: قانون الاتصالات والإنترنيت رقم ٤٨ لعام ٢٠٠٢، الذي يجرم أي تحوير أو اعتراض أو الإفصاح عن الإتصالات ومضمونها (المادة ٧٥ منه). وأنشأ القانون "هيئة تنظيم الإتصالات" وجعل من صلاحياتها حماية البيانات الخاصة وخصوصية الخدمات". كما أنشأ "بدالة إنترنيت البحرين http://www.bix.bh، بهدف ضبط تراخيص مزودي خدمات الإنترنيت. انما لم يرد في القانون البحريني أحكاماً متعلقة بحركة المعلومات، ومحو البيانات المعالجة والمخزنة المتعلقة بالمشتركين من قبل مزودي خدمات عند الانتهاء من خدمات الارسال الالكترونية.

أيضا أصدرت القانون رقم ٢٨ /٢٠٠٢ المتعلق بالمعاملات والتجارة الإلكترونية، والقانون رقم ٢٠١٤/٦٠ بشأن جرائم تقنية المعلومات. كما أصدرت البحرين المرسوم رقم ٩ لعام ٢٠٠٢ لإعادة تنظيم الجهاز المركزي للمعلومات، والقرار رقم ٢٥ لعام ٢٠٠٥ لتشكيل لجنة عليا لتقنية المعلومات والإتصالات.

٤. **الجزائر**:

منذ عام ٢٠١٤، تُعدّ وزارةُ البريد وتكنولوجيا الإعلامِ والاتصالات في الجزائر إستراتيجية تمتدُّ إلى غاية ٢٠٢٠ وتشمُلُ مساحَة البلدِ بأكملِه، تتضمّنُ الحوسبَةَ السحابيةَ، والإدارةَ الإلكترونية لِلنهوض بِقطاع التكنولوجيات وبِهدف عصرنة الإقتصادِ الجزائري، وإعداد تشريع ونُظُم ملائمين لِلحفاظ على سِرية البيانات وسلامتِها، ولِضمان سريّةٍ تامةٍ في تبادل المُراسلاتِ الإلكترونيةِ.

على الصعيد التشريعي، لا بد من الإشارة إلى القانون رقم ٠٩-٠٤ المؤرخ في ١٤ شعبان عام ١٤٣٠ الموافق ٠٥ اوغسطس سنة ٢٠٠٩ الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

نشير إلى أنّ الجزائر تعد "مشروع قانون التصديق والتوقيع الإلكترونيين"، الذي يضمن حماية البيانات الشخصية وتسهيل المبادلات عبر الأنترنت؛ ومشروع قانون آخر يتعلق بالمعاملات الالكترونية.

٥. السعودية:

تطبيقياً، برَزَتْ فِكرةُ الحوسبة السحابية بِشكلٍ موسّع في نِطاق الأعمالِ والإستثماراتِ العالميةِ في السعودية، وشَهِدَ قِطاعُ تقنيةَ المعلوماتِ مُنافسةً بين كبرى الشركات المُتخصّصة في الإتصالات والتقنية بِطرح خدماتِ الحوسبةِ السحابيةِ الخاصة. كما امتدَّ نِطاقُ الحوسبَةِ السحابيّة نحو القطاعِ الحُكوميّ، الذي يتجِهُ لِمفهومَ آخر جديدٍ وهو (G-cloud) أو السحابةُ الإلكترونيّةُ الحكوميّة، والذي يرمي لِتحوّلَ الجِهاتِ الحكوميّة من وِزاراتٍ ومؤسساتٍ عامةٍ إلى فِكرة الحوسبةِ السحابيةِ، والسَحاباتِ الافتراضيةِ حيث تُحْفَظُ عليها كافةَ البياناتِ. وكأيّ مفهوم جديدٍ قُوبِلت فِكرةُ الحوسبةَ السحابيةَ في السعودية بالتخوّفِ وأحياناً بالرَفْضِ من جِهاتٍ عِدّة خاصة وحكومية، نَظَراً إلى مَحاذيرَ مُتعلّقةٍ بِأمن المعلوماتِ ومَخاوف تسرُّب البياناتِ من السحابةِ.

كما تمّ تشكيلُ "هيئةَ الإتصالات وتقنية المعلومات" في مجلس الشورى السعودي لمُناقشةَ ضوابطِ وتقديمَ خدماتِ الحوسبةِ السحابيةِ في المملكةِ، ولِعرض تجارب الدولِ المُتقدّمةِ في مجال خدماتِ الحَوسبةِ السحابيةِ وأبرزِ الضوابِط والآلياتِ لِتقديم هذه الخدماتِ، سواءً على مستوى التشغيلِ أو السياساتِ المُنظّمة لِتقديم الخِدمةِ أو الصِيغِ القانونيةِ لها. وحذّرتْ هذه اللُجنةُ من خُطورةَ توجّهِ الأفرادِ والجِهات الحكوميّة والشركاتِ السعوديةِ إلى الشركاتِ الأجنبيةِ فيما يتعلّقُ بالحصولِ على الخدماتِ الخاصةِ بالحوسبةِ السحابيةِ، مما يؤدّي إلى محاذيرَ تتعلّق بالأمنِ الوطنيّ، وارتفاعَ الطَلَبِ على سِعاتِ الإتصالِ الدوليّ، وحِماية البياناتِ، وتسرُّبِ الأموالِ والاستثماراتِ للخارِجِ.

على الصعيدِ التشريعيّ، لا يوجَد في المملكةِ العربيةِ السعوديةِ أيّ تشريع خاص بِحماية البياناتِ على الرغم مِن أنَّ الحقَّ في الخُصوصيةِ مُقررٌ في عددٍ من القوانين. هناك قانونُ الإدارة الأساسيّ، الذي ينصُّ على مبدأ أساسيّ مُؤدّاه أنَّ جميعَ المُراسلاتِ والإتصالاتِ بين الأطرافِ ينبغي أن تَكونَ سريةً تماماً ويُلزمُ عدمُ إفشائِها. وتتولّى المحاكِمُ القضائيةُ في المملكةِ تحديدَ الإنتهاكاتِ لِسرية البيانات، استناداً إلى مبادِئ الشريعةِ الإسلاميةِ، مُتمتّعةً بِسلطةَ تقديريةٍ واسعةٍ في تقديرَ وسيلةِ هذه الإنتهاكاتِ. كما أنَّ الإتجاهَ المُعتمدَ في المَملكةِ هو الحصولُ على مُوافقةَ صاحِبِ البياناتِ قبل أي تصديرٍ لِبياناتِه الشخصيّةِ. نُشير، إلى أنّ هناك مشروعَ قانونٌ يتمُّ بحثُه في مجلس الشورى، في المملكةِ العربيةِ السعوديةِ، حول حماية البيانات. كما أنشأت المملكة "مركز الإستجابة لطوارئ الحاسب الآلي" SA-CERT[٣٠].

في السياقِ عَيْنِه، يُعاقبُ "نظامُ مكافحة جرائم المعلوماتية" في المملكةِ الصادر في عام ٢٠٠٧ (بموجب المرسوم الملكي رقم م/١٧ وتاريخ ١٤٢٨/٣/٨هـ)، أيَّ شخصٍ يتصرّفُ بِطريقةٍ غير قانونيةٍ للوصول إلى كومبيوتر أو شخصٍ آخر لغرض حذْفِ أو تدمير، أو تغيير أو إعادة توزيع المعلومات بغرامةٍ لا تزيد على

٣٠٠٠٠٠٠ ريال سعودي و/أو السجن لِمُدّة لا تزيد على أربع سنوات؛ وأي شخص، يصلُ إلى معلوماتِ الشخصِ الآخرِ البنكيةِ أو الإئتمانية، أو لأي معلومات بالأوراقِ الماليةِ التي يَمْلُكها ذلك الشخصُ يُجرّم بِغرامة لا تزيد عن ٢٠٠٠٠٠٠ ريال سعودي و/أو بالسجنِ لمدّة لا تزيد عن ثلاث سنوات.

في السياق عينه، أصدر المجلس الوزراي القرار رقم ٤٠ تاريخ ٢٠٠٦/٣/٢٧، المتعلق بضوابط التعاملات الإلكترونية الحكومية؛ والقرار رقم ٦٦٦٧ تاريخ ١٤٢٦/٧/١ هـ، المتعلق بشروط مزاولة مهنة الإستشارات في مجال الإتصالات وتقنية المعلومات.

٦. **السودان**:

تَعتبرُ السودان أنّ تفعيلَ الحوسبَةِ السحابيةِ وتبنيّ تِقنياتِها من ضِمن استراتيجياتِها لِتخطيطَ التنميةِ المُستدامةِ، بعد تنامي الوعي بِأهمية تقنيةِ المعلوماتِ لدى مسؤوليّ الدولةِ؛ وتعتبرُ أنَّ إمكانيةَ إستخدامُ الحوسبَةِ السحابيةِ يُساهمُ في تحقيقَ الإستراتيجيةِ العامةِ للدولة من خلال توحيدِ أدواتِ وبرامِجِ الحكومةِ الإلكترونيةِ و"التطبيقاتِ النموذجية"، لا سيما أنَّ إنشاءَ قاعدةِ بياناتٍ تُتيحُ لِمستخدميها ومُتخذّي القرارِ حُزمةً مُتكاملةً من المعلوماتِ الدقيقةِ والمُوثَّقةِ بالصورِ تدعمُ مَشروعاتِ التنميةِ المُستدامةِ. إضافةً، إلى خِدمَةِ MobileMapping، حيث يعملُ نِظامُها من خلال عمليات ثلاث: جمعُ البياناتُ، وتخزينُها في مركزٍ خاصٍ، وتهيئة الجِهة التي تستخدم النظام للعملِ به.

على الصعيد التشريعي، ينص دستور السودان في المادة ٢٩ على حرية الاتصال والمراسلة وسريتها وعلى خصوصية كل إنسان. وأصدرت السودان قانون المعاملات الإلكترونية عام ٢٠٠٧ وقانون مكافحة جرائم االمعلوماتية عام ٢٠٠٧، وهو ينص في المادة السادسة على جريمة التنصت أو التقاط أو اعتراض الرسائل دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة ويعاقبها بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً. وتنص المادة السابعة منه على جريمة دخول المواقع عن طريق شبكة الانترنيت عمداً بقصد الحصول على بيانات أو معلومات أمنية تمس الأمن القومي للبلاد أو الاقتصاد الوطني ويعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معاً. أما إذا كان الدخول بهدف إلغاء بيانات أو معلومات تمس الأمن القومي للبلاد أو الاقتصاد الوطني أو حذفها أو تدميرها أو تغييرها فيعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً.

وفي ١ كانون الثاني/يناير ٢٠١٠، أنشأ السودان "المركز السوداني لأمن المعلومات للإستجابة لحوادث أمن المعلومات" Sudan Cert[٣١] بهدف تقديم المشورة الفنية للمواطنين وللشركات ومساعدة الضابطة العدلية، وحماية البنية الأساسية للاتصالات والمعلومات بالبلاد. وقد قام بإنجازات ملموسة كتحليل الدودة المعلوماتية الخطيرة Duku والتصدي لها. كما تمّ إطلاق حكومة السودان الإلكترونية[٣٢].

وفي 2013 تمّ البدء في تنفيذ مشروع "تدريب المدرّب" في الاستخدام الآمن للانترنت إضافة إلى العديد من النشاطات التوعوية.

٧. الصومال:

بالرغم من أنّ الدستور الصومالي ينص في المادة ٢٢ منه على "حرية المراسلة وسريتها وكذلك كل وسائل الاتصال، وبالرغم من أنّ قطاع الاتصالات السلكية واللاسلكية يعتبر من أفضل القطاعات في الصومال، إلا أنّ هناك فراغ تشريعي فيما يتعلق بالمعاملات الالكترونية، وتنظيم تكنولوجيا المعلومات والإتصالات، والجرائم الإلكترونية.

٨. العراق:

الإتجاه عَينه في العراق، حيث لا يُوجَد سوى مُبادراتٍ حول مبدأ وفِكرةِ إستخدامِ الحوسبةِ السحابيةِ وإستثمارِها، وقواعِدِ البياناتِ، والحِفاظِ على السريَةِ والخُصوصيَةِ، واعتمادِ تطبيقاتِها في التعليمِ العاليّ بشكلٍ خاص. عِلماً بأنَّ توظيفَ تِقنيةُ الحوسبَةِ السحابيَةِ قد يكون أحدَ الحُلولِ لِلعديدَ من المشاكِلِ التقنيّةِ التي يُعاني مِنها قِطاعُ تقنية الإتصالاتِ والمعلوماتِ في العراق.

أما على الصعيد التشريعي، فهناك قانون العلامات والبيانات التجارية رقم ٢١ لعام ١٩٧٥، والذي تعدّل بموجب قانون ٢٠١٠، تاريخ ٢٠١٠/١/٤. إضافة إلى قانون حماية المستهلك رقم ١ تاريخ ٢٠١٠/١/٤.

وفي عام ٢٠١٢، أصدر العراق القانون رقم ٧٨ المتعلق بالتوقيع الإلكتروني والمعاملات الإلكترونية[٣٣]، الذي اعترف بالسندات الالكترونية ونظم الأحكام القانونية المتعلقة بها. كما وضعت جمهورية العراق الإستراتيجية الوطنية وخطة عمل الحوكمة الإلكترونية العراقية ٢٠١٥-٢٠١٢.

٩. الكويت:

يُمكِن تلخيصُ الواقِعِ في الكويت بِمبادراتٍ وطنيةٍ تسْعى إلى تفعيل تطبيقاتِ الأَرشفةِ الإلكترونيَةِ والحوسبَةِ السحابيةِ مُواكبَة لِلثورةِ الرقميّةِ، وإلى تقديم حُلولٍ عمليةٍ واستراتيجياتٍ فعالَةٍ لإدارة المُحتَوى، والمنافِذِ الإلكترونيّةِ، ونُظُم التخزينِ، والأَرشفَةِ، ومُناقشَة التحديّاتِ التكنولوجيةِ والإدارية، التي تُواجهُ المُؤسساتِ الحكومية والخاصة في التحوّلِ إلى استبدال البيئةِ الورقيّةِ بالبيئةِ الإلكترونيةِ. إضافةً إلى "شبكة الكويت للمعلوماتِ"[٣٤]، التي تربُط حوالي ٥٦ جِهةٍ حكوميةٍ في شبكةٍ آليةٍ واحدةٍ تُتيحُ لها نقل وتبادُل المعلوماتِ والوثائقِ الإلكترونيّة؛ ويُعوّل على تقنياتِ الحوسبةِ السحابيةِ في تفعيل دورِ هذه الشبكةِ محلياً لِتحقيق نقلةٍ نوعيةٍ للتكنولوجيا في الكويت، ولِحفظ البياناتِ والمعلوماتِ في السحابةِ الرقميّةِ. كما تمَّ إطلاقُ خدمةَ "مايكروسوفت أوفس ٣٦٥" لِتقديم مجموعةِ تطبيقات وخدمات في مجال تِقنياتِ الحاسوب.

أضِفْ أنّ الجِهازَ المركزيّ لتكنولوجيا المعلومات[٣٥]، ومنذ نشأته في عام ٢٠٠٦، يُساهمُ في إنجاز العديدِ من المشاريعِ المُرتبطةِ بالبُنيةِ التحتيّةِ المعلوماتيّةِ اللازمَةِ ولِتطوير منظُومةِ الحكومَةِ الإلكترونيةِ. وهناك مشروع قانون كويتي حول الجرائم السيبرنية.

على الصعيد التشريعي، فقد أصدر الكويت القانون بالمرسوم رقم (٥) لسنة1999 م يتعلق بحماية الملكية الفكرية متضمنًا حماية المصنفات والحاسب الآلي من البرامج وقواعد البيانات (م١).

كما تعد الكويت مشروع قانون خاص بالمعاملات الإلكتروني ينص في بعض مواده (٣٥ لغاية ٤٠) على عدم الجواز للجهات الحكومية أو الهيئات أو المؤسسات العامة، أو الشركات، أو الجهات غير الحكومية أو العاملين بها الإطلاع دون وجه حق أو إفشاء أو نشر أي بيانات أو معلومات شخصية مسجلة في سجلات أو أنظمة معلوماتها الإلكترونية، بإستثناء بعض الحالات ولإعتبارات تتعلق بالأمن القومي للبلاد، وغيرها العديد من الأحكام.

وفي عام ٢٠١٤، تم استحداث هيئة تنظيم الاتصالات وتقنية المعلومات بموجب قانون رقم ٢٠١٤/٣٧، في الكويت CITRA[٣٦]، كما أن الكويت في صدد إنشاء "مركز الاستجابة لطوارئ المعلوماتية" يتبع للجهاز المركزي لتكنولوجيا المعلومات بهدف الحد من المخاطر أو الثغرات الأمنية الإلكترونية وإتخاذ الإجراءات الوقائية ونشر المعلومات الخاصة بأي تهديد إلكتروني حالي أو محتمل، وتنسيق جهود الاستجابة لحالات الطوارئ أو المخاطر الإلكترونية بما في ذلك الخطوات العملية والتقنية والإجرائية.

١٠. المغرب

نص الدستور المغربي الجديد الصادر بتنفيذه الظهير الشريف رقم ١,١١,٩١ الصادر في ٢٧ من شعبان ١٤٣٢ الموافق لـ ٢٩ يوليو ٢٠١١ في المادة ٢٤ على أنه "لا تنتهك سرية الاتصالات الشخصية كيفما كان شكلها، ولا يمكن الترخيص بالإطلاع على مضمونها أو نشرها كلا أو بعضاً، أو باستعمالها ضد أي كان، إلا بأمر قضائي ووفق الشروط والكيفيات التي ينص عليها القانون". وقد ورد هذا المبدأ في القانون رقم ٠٣-٠٣ المتعلق بمكافحة الإرهاب قبل اعتماده في الدستور الجديد، حيث تنص الفقرة الأولى من المادة ١٠٨ من قانون المسطرة الجنائية (ق.م.ج) على أنه "يمنع التقاط المكالمات الهاتفية أو الاتصالات المنجزة بوسائل الاتصال عن بعد وتسجيلها أو أخذ نسخ منها أو حجزها".

أدخل القانون رقم ٠٨-٠٩ لعام ٢٠٠٩ المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[٣٧] للمشهد القانوني المغربي للمرة الأولى مجموعة من المقتضيات القانونية التي تتلاءم مع القانون الدولي، وخصوصاً التوجيه الأوروبي المشترك رقم ٤٦/٩٥ المتعلق بحماية المعطيات ذات الطابع الشخصي. يطبق القانون رقم ٠٩-٠٨ على معالجة المعطيات ذات الطابع الشخصي سواء كانت تتعلق بشخص ذاتي محدد الهوية أو قابل لتحديد هويته. مثلا: الاسم والعنوان والبريد الإلكتروني والصورة ورقم الهوية وبصمات الأصابع كلها معطيات ذات طابع شخصي. وتشمل المعالجة التي تهم حماية المعطيات ذات الطابع الشخصي، كل عملية أو مجموع العمليات التي تنصب على المعطيات ذات الطابع الشخصي سواء كانت بواسطة وسائل آلية أو غيرها. ويهم ذلك بالخصوص، الجمع والتسجيل والتنظيم والمحافظة والتكييف أو التعديل والاستخراج والتصفح والاستعمال والإخبار بالإرسال أو أي شكل آخر من أشكال الإتاحة والتقريب أو الترابط وكذلك الإغلاق والمسح أو التدمير. وفضلا عن ذلك، نذكر أن عملية واحدة من هذه العمليات تكفي لكي تصبح معالجة المعطيات ذات الطابع الشخصي قائمة وتخضع لمقتضيات القانون رقم ٠٩-٠٨، فجمع المعلومات دون الإخبار بها أو نشرها يكفي لكي يميز عملية المعالجة.

وبالإضافة إلى ذلك، تجدر الإشارة إلى أن هذا القانون يسري ليس فقط على الشركات والأشخاص القائمين فوق التراب المغربي ولكن كذلك على كل الشركات الأجنبية التي تقيم علاقات أعمال مع نظيراتها المغربية أو التي تتبادل المعطيات مع فروعها أو الشركات الأم المغربية، وذلك باستعمال وسائل تقع على التراب الوطني. غير أن مجال تطبيق هذا القانون يستثني المعطيات المتعلقة بممارسة الأنشطة الشخصية

أو الأسرية، والمعطيات المحصل عليها من مصلحة الدفاع الوطني والأمن الداخلي والخارجي للدولة، وكذلك المحصل عليها في إطار معالجة تمت تطبيقاً لتشريع معين.

وقد جرم هذا القانون، ضمن الباب السابع منه مجموعة من الأفعال، ومنها: القيام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة، أو إنجاز معالجة لأغراض أخرى غير تلك المصرح بها أو المرخص لها، أو إخضاع المعطيات المذكورة لمعالجة لاحقة متعارضة مع الأغراض المصرح بها أو المرخص لها؛ أيضاً يعتبر نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين ٤٣ و٤٤ من هذا القانون.

كما أوكل هذا القانون إلى اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي المعتمدة لدى رئيس الحكومة، مهمة التكفل بتفعيل أحكام هذا القانون والنصوص المتخذة لتطبيقه والسهر على التقيد به، وذلك وفقا للمادة ٢٧ من هذا القانون. كما تمسك هذه اللجنة، وفقا للمادة ٤٥، السجل الوطني لحماية المعطيات الشخصية.

كما أصدر المغرب القانون رقم ٠٧-٠٣ المتمم لمجموعة القانون الجنائي المتعلقة بجرائم الإخلال بسير نظم المعالجة الآلية للمعطيات. ويحصر هذا القانون الأفعال المجرمة فيما يلي:

- الدخول الاحتيالي إلى مجموع أو جزء من نظم المعالجة الآلية للمعطيات؛
- البقاء في نظام المعالجة الآلية للمعطيات بعد الدخول فيه عن طريق الخطأ؛
- حذف أو تغيير المعطيات المدرجة في نظام المعالجة الأوتوماتيكية للمعلومات أو تسبب في اضطراب اشتغالها؛
- العرقلة المتعمدة لسير نظام المعالجة أو إحداث خلل بهذا الأخير؛
- إدخال دون الترخيص بذلك لمعطيات أو إتلافها أو حذفها أو تغييرها؛
- التزوير أو التزييف في وثائق معلوماتية واستعمالها في إلحاق الأذى بالغير؛
- منح تجهيزات أو أدوات أو برمجيات معدة لارتكاب الجرائم أعلاه.

حدد في هذا الإطار القانون رقم ٥٣-٠٥ المتعلق بالتبادل الالكتروني للمعطيات الإلكترونية، الذي يتضمّن ٤٣ مادة تتمحور حول المواضيع التالية:

النظام المطبق على المعطيات القانونية التي يتم تبادلها بطريقة الكترونية وعلى المعادلة بين الوثائق المحررة على الورق وتلك المعدة على دعامة إلكترونية، وعلى التوقيع الإلكتروني، كما حدد الإطار القانوني

المطبق على العمليات المنجزة من قبل مقدمي خدمات المصادقة الالكترونية وكذا القواعد الواجب التقيد بها من قبل مقدمي الخدمة المذكورين ومن قبل الحاصلين على الشهادات الالكترونية المسلمة. ومن أجل حماية المعاملات الإلكترونية ولحجية الوثائق الإلكترونية والتوقيع الإلكتروني قد جرّم هذا القانون، وخاصة بمقتضى الباب الثالث المتعلق بالعقوبات والتدابير الوقائية ومعاينة المخالفات، مجموعة من صور جريمة المعلوماتية باعتبارها تشكل مساساً بالثقة التي تتمتع بها المحررات والوثائق الإلكترونية، وأغلب العقوبات المقررة للأفعال المنصوص عليها هي عقوبات جنحية.

كما صدر القانون رقم ٣١-٠٨ القاضي بتحديد تدابير لحماية المستهلك ليعزز الترسانة القانونية المغربية في مجال حماية المستهلك بما في ذلك حماية المستهلك على الإنترنت. ويضمن هذا القانون للمستهلكين إعلاماً جيداً وحمايةً مناسبةً من الشروط التعسفية وبعض الممارسات التجارية. وتضمّن أحكاماً تكميلية متعلقة بالضمان التعاقدي والخدمة بعد البيع والاستدانة.

وفي السياق عينه، ونظراً للدور الهام لحركة المستهلكين في الإعلام والتبصير والحماية القانونية لحقوق المستهلكين، فقد منح القانون جمعيات المستهلكين ذات المنفعة العامة الحق في المرافعة أمام المحاكم لتمثيل المصالح العامة للمستهلكين.

١١. **اليمن:**

في بحثٍ واقعيّ، أطلقَتْ اليمن خِدمةً تلفزيونيّةً تعتمدُ على الحوسبةِ السحابيةِ أُطلقَ عليها إسم Play Station. وعلى الصعيد التشريعي، تعدّ اليمن مشروع قانون لعام ٢٠٠٩ بشأن المعلومات[٣٨]، بهدف تحديد مبادئ الحق في الحصول على المعلومات، وشروطه وإجراءته، وتكلفة الحصول على المعلومات، والاستثناءات على حق الحصول على المعلومات في حدود ما يجيزه القانون، ولمن يمنحه القانون، وإدارة المعلومات، ومهام الهيئة المختصة بالإشراف والتوجيه ورسم وإقرار السياسات والخطط في مجال المعلومات ومتابعة تنفيذها، ودور هذه الهيئة في وضع أسس ومعايير معالجة البيانات والمعلومات؛ بالإضافة إلى تبادل المعلومات بين كل أجهزة الدولة ووحدات القطا ع العام والمختلط والخاص والشركات الأجنبية العاملة داخل البلد. إنما غاب عن مشروع القانون هذا موضوع نقل البيانات الخاصة وتحويلها إلى خارج البلاد، ويُرجى إضافته قبل اقراره بشكل نهائي.

كما أصدرت اليمن، قانون رقم ٤٠ لعام ٢٠٠٦ بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، الذي ينص على شروط قابلية السند الإلكتروني للتحويل وإجراءات الدفع، والتحويل الإلكتروني للأموال، وإجراءات توثيق السجل والتوقيع الإلكترونيين.

في عام ١٩٩٥ أنشأ اليمن، بموجب القرار الجمهوري رقم ١٩٩٥/١٥٥ "المركز الوطني للمعلومات"، لمواكبة تطورات مجتمع المعلومات. وفي عام ٢٠٠٢ أنشأت، وبموجب قرار مجلس الوزراء رقم ٢٠٠٢/٤، "مدينة تكنولوجيا الإتصالات والمعلومات" بهدف الإعداد لتحقيق الحكومة الإلكترونية، ولتكوين مجتمع تقني متكامل يعنى بتقنيات الاتصالات والمعلومات. وتجدر الإشارة إلى عدم وجود قوانين واضحة تتحدث عن الخصوصية في اليمن وبالأخص الخصوصية الرقمية.

١٢. **تونس:**

تَمَّ إطلاق أوّلَ موقع للحوسبةَ السحابيةِ لِلمؤسّسات في تونس في ابريل ٢٠١٥، بِهدفَ مُساعدةِ المؤسساتِ الحكوميّةِ أو الخاصَةِ في الوصولِ إلى طلباتِ التطبيقاتِ المهنيّةِ، وذلك بِهدفَ جعلِ الحوسبةِ السحابيةِ مُتاحةً لِمختلفَ المؤسساتِ، وتحسين خدمة شبكةً الإنترنيت، ومُعدّل التَحميلِ، والتَغطيةِ والخدماتِ.

على الصعيدِ التشريعيّ، تجدر الملاحظة أنه تم منذ عام ١٩٩٨ تحديد الخدمات المتعلقة بمجال تكنولوجيا المعلومات والاتصال بصفة عامة، والخدمات البريدية بصفة خاصة، وضمان حسن استعمالها واستغلالها من خلال إصدار القانون عدد ١٩٩٨/٣٨ في مجلة البريد، وذلك بهدف ضبط شروط تعاطي النشاط البريدي وضمان حق العموم في الخدمات البريدية الأساسية، مع تأمين سرية المراسلات طبقا للتشريع الجاري به العمل. وقد تم التفكير في كيفية حماية المعطيات والخدمات الالكترونية والنظم المعلوماتية من خلال إصدار القانون ١٩ لسنة ١٩٩٨ المتعلق بتنقيح وإتمام بعض أحكام من المجلة الجنائية.

من جهة أخرى، تمّ إصدار القانون عدد ٨٣ لسنة ٢٠٠٠ المتعلق بالمبادلات والتجارة الإلكترونية، حيث يضبط القواعد العامة المنظمة للمبادلات والتجارة الإلكترونية، والتي تخضع فيما لا يتعارض وأحكام هذا القانون إلى التشريع والتراتيب الجاري العمل بها. وقد أقر هذا النص ما يلي "يجرى على العقود الإلكترونية نظام العقود الكتابية من حيث التعبير عن الإرادة ومفعولها القانوني وصحتها وقابليتها للتنفيذ فيما لا يتعارض وأحكام هذا القانون". وقد أحدث بموجب هذا القانون "الوكالة الوطنية للمصادقة الإلكترونية".

كما أصدرَتْ تونس، سلسلةً من القوانين، والمراسيمِ والقراراتِ، التي تُشكّلُ الإطارَ التشريعيَّ لأوجه استخدامِ الإنترنت والحقوقِ المُتصلة بها، أبرزُها القانون رقم ٢٠٠١/١، المتعلّق بمجلة الإتصالات والتي تهدف إلى تنظيمَ مجالِ الاتصالاتِ، وتوفيرَ الخدماتِ الأساسيةِ للاتصالاتِ والبثّ المرئيّ والمسْموع، وتمتُّع الأفراد بِخدماتِ الاتصالاتِ. وأنشأَتْ، وبموجب القانون عينه رقم ٢٠٠١/١ "الهيئةَ الوطنيةَ للاتصالاتِ" ذات الصلاحياتٍ في إبداءِ الرأي حول سُبل تحديدِ تعريفاتِ الشبكاتِ والخدماتِ، والتصرُّف في المُخططاتِ الوطنيةِ المُتعلّقةِ بِالترقيمِ والعنونةِ، ومُراقبة احترام الالتزاماتِ الناتِجةِ عن الأحكامِ التشريعيّةِ والتراتبيّةِ، والنظّرِ في النِزاعاتِ المُتعلّقةِ بإقامةَ وتشغيلِ واستغلال الشبكاتِ.

ثم وفي العامِ ٢٠٠٤، اعتمَدَت القانون رقم ٢٠٠٤/٦٣ المُتعلّق بِحماية المُعطياتِ الشخصيةِ، الذي أَقرَّ حقَّ كُلّ فرد، في حِمايةِ المُعطياتِ الشخصيَةِ المُتعلّقةِ بحياتِه الخاصةِ بإعتبارها من الحقوقِ الأساسيةِ المَضمونةِ بالدستورِ ولا يمكن أن تقع معالَجتها إلّا في إطارَ الشفافيةِ والأمانَةِ واحترام كرامةِ الإنسانِ.

في السياقِ عينِه، صدرَ القانونُ التونسيّ رقم ٢٠٠٤/٥، المتعلق بتنظيمَ مجالِ السلامةِ المعلوماتيةِ وضبطِ القواعِدِ العامَةِ لحمايةَ النُظُم المعلوماتيّةِ والشبكاتِ، والذي أحدث "الوِكالةَ الوطنيةَ للسلامةِ المعلوماتيةِ" ANSI، والتي تضطلع بمراقبة عامة على النظم المعلوماتية والشبكات بالنظر إلى مختلف الهياكل العمومية، ومُولياً إيّاها العديدَ من الصلاحياتِ أبرزُها: تنفيذُ استراتيجيةٌ وطنيةٌ للسلامَة المعلوماتيةِ من خلال وضعِ المقاييسِ اللازمَةِ، وإعدادَ أدلَّةٍ فنيةٍ، وإعتمادَ حلولٍ وطنيةٍ معلوماتيّةٍ، وتنفيذِ التدقيقِ الدوريّ لكُل المرافِقِ العامَةِ والخاصَةِ، وضمانَ اليقظَةِ التكنولوجيّةِ. وفي عام ٢٠٠٧، أنشأت الوكالة المذكورة "مركز الإستجابة لطوارئ الحاسب الآلي tunCERT[٣٩]. كما نُشير إلى أنّه صدَرَتْ العديدُ من القوانين اللاحقةِ (قانون رقم ٢٠٠٤/١٢٤٩ و٢٠٠٤/١٢٥٠)، بِهدف وضعِ القانونِ رقم ٢٠٠٤/٥ قيد التطبيقِ.

من ناحية أخرى، صدر القانون التوجيهي عدد ٣١ لسنة ٢٠٠٧ المتعلق بإرساء الاقتصاد الرقمي الذي يعتبر من ضمن الأولويات الوطنية بالنظر إلى مساهمته في دفع القدرة التنافسية للاقتصاد الوطني وانعكاساته الإيجابية على مختلف الأنشطة. ويُقصد بالإقتصاد الرقمي في هذا القانون، الإقتصاد الذي يتكون من الأنشطة ذات القيمة المضافة العالية التي تعتمد تكنولوجيات المعلومات والاتصال. كما يجري الإعداد لمشروع إحداث "الوكالة الفنية للاتصالات" لتأمين الربط القانوني لحركة الإنترنيت، ومشروع قانون يتعلق بمكافحة الجرائم المتصلة بتكنولوجيات المعلومات والاتصال.

١٣. جزر القمر:

من مراجعة بحثية لم يتوفّر لدينا أيّ تشريعات خاصة بالأمن السيبراني أو قواعد تنظيميّة أو تشريعيّة أو إدرايّة لتنظيم تكنولوجيا المعلومات والاتصالات في جزر القمر. في أيار/مايو ٢٠٠٩ تم تأسيس الهيئة الوطنية لتنظيم تكنولوجيا المعلومات والاتصالات بموجب المرسوم رقم ٦٥ بهدف السهر على وضع سياسة وقوانين قيد التطبيق، ولخلق بيئة تنافسية مشروعة بين الموردين، ولحماية مصالح الدولة والمستهلكين[٤٠].

ويذكر أنه في يونيو ٢٠١٥ م تمّ إطلاق مشروع انطلاق التلفزيون الرقمي الأرضي في جزر القمر كمبادرة لمواكبة تطورات تكنولوجيا المعلومات والإتصالات.

١٤. جيبوتي:

كمُبادرةٍ أوليّة، أطلقَتْ جيبوتي مشروعَ استخدامِ قُدراتِ الحوسبةِ السحابيةِ في قطاعَي التربيةِ والاتصالاتِ بالتعاونِ مع شركة (Ericsson)، مُساهمةً في تقديمَ خدماتٍ تعليميّةٍ عاليةِ الجُودةِ.

على الصعيد التشريعي، أصدرت جيبوتي "قانون الحماية ومكافحة الغش وحماية المستهلك"، رقم ٢٨ عام ٢٠٠٨، الذي ينص في المادة ٤٢ البند ١ على «حماية موافقة المستهلك» بشأن الدعاية الزائفة والمضللة التي تضلل المستهلكين.

كما تسعى جيبوتي لتشكل مركزاً إقليميا في قطاع الاتصالات وتجسيد الرؤية التنموية، فقطاع الاتصالات يعد من القطاعات الواعدة التي يمكن من خلالها النهوض بالاقتصاد الجيبوتي. وتتعاون جيبوتي مع كل من الاتحاد الدولي للإتصالات لتعزيز قدرات البنية التحتية لتكنولوجيا المعلومات والاتصالات[٤١]، ومع البحرين ومصر في مجال تبادل الخبرات وتنمية القدرات البشرية.

١٥. سلطنة عمان

بادرَتْ سلطنةُ عمان إلى إرساءَ ترسانَةٍ تشريعيّةٍ مُتعلّقةٍ بالفضاءِ السيبرانيّ، ومُسودّة قانونٍ[٤٢] حول حِماية البياناتِ والذي يأتي مُكمّلاً لِمنظومةَ القوانين العمانيّة ذات الصلةِ. كما اعتمدَتْ قانون بشأن المُعاملات الإلكترونيةِ (٢٠٠٨/٦٩)، الذي يتضمّنُ أحكاماً تتعلّقُ بِحمايةِ البياناتِ مُتفقاً مع قوانينَ الأُمم المُتحدةِ النموذجيّة الخاصةِ بالتِجارةِ الإلكترونيةِ والتوقيعاتِ الإلكترونيةِ. بحيث تنصُّ المادة ٤٣ من الفصل السابع المُدْرج تحت عنوان: "حماية البيانات الخاصة" على أنّه لا يجوز جمعُ البياناتِ، أو مُعالجتُها، أو إستخدامُها،

لأيّ غَرَض دون المُوافقة الصريحةِ لِلشخص صاحب البياناتِ. ويُؤكّدُ القانونُ على سريّةَ البياناتِ الشخصيّةِ (المادة ٤٤)، وإلزاميّةِ إخطارِ صاحِبِ البياناتِ وقَبْل المُعالجةِ بالإجراءات التي يَتْبعُها لِحمايةَ البياناتِ الشخصيّةِ (المادة ٤٥)، وحقّ صاحِب شهادَةِ التصديقِ الإلكترونيّ في النفاذِ إلى بياناتِه الشخصيّةِ وتعديلِها (م. ٤٦)، وحقّ الإعتراضِ على مُعالجةَ البياناتِ (م. ٤٧)، وعدم المعالجة فيما إذا كانت ستُسبّبُ ضرراً للأشخاصَ (م. ٤٨)، والشروطِ الواجِب توفُّرها لدى نقلِ هذه البياناتِ إلى الخارِجِ (م. ٤٩).

كما أصدرَتْ "هيئة تنظيم الإتصالاتِ في سلطنة عمان القرار رقم ٢٠٠٩/١٣، الذي أقرّ اللائحةَ التنفيذيّةَ الخاصةِ بحِماية سريّة خصوصيّة البياناتِ المُستخدمةِ، مما يسمحُ بإلزام مُقدّمي خدماتِ الاتصالاتِ السِلْكيّةِ واللاسلكيّة بِضوابطَ خاصةٍ لِحمايةَ البياناتِ رُغم عدم وجودِ نصٍّ صريحٍ مُتخصّص بِحمايةِ البياناتِ.

كما نُشيرُ إلى "قانون مكافحة جرائم تقنية المعلومات"، الذي صدَرَ بموجب المرسوم السلطاني رقم ٢٠١١/١٢ (الجريدة الرسمية عدد ٩٢٩ – تاريخ ٦ فبراير ٢٠١١)، يتناولُ في الفصلِ الثاني مِنه "التعدّي على سلامة وسرية وتوافر البياناتِ والمعلوماتِ الإلكترونيةِ والنُظُمِ المعلوماتيّة"، والمُتضّمن ثماني مواد. يجرم هذا الفصل من القانون دخول موقع الكتروني أو أي نظام معلومات الكتروني أو شبكة معلومات أو وسيلة معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو تغيير تصميم موقع أو اتلافه، أو تحريفه (م. ٣ و م. ٧ و م. ٩)، لا سيما الملف الصحي (م. ٥)، أو الحصول على بيانات حكومية أو معلومات سرية مالية أو اقتصادية (م. ٦)، أو تزوير سندات الكترونية حكومية (م. ٦)، أو اعتراض خط سير البيانات (م. ٨).

كما يجرم هذا القانون إساءة استخدام وسائل تقنية المعلومات (م. ١١)، والتزوير والاحتيال أو الابتزاز المعلوماتي (م. ١٢ و م.١٨)، وارتكاب جرائم المحتوى لا سيما تلك المخلة بالآداب العامة (المواد ١٤ و ١٥ و ١٧)، أو الاعتداء على الحياة الخاصة (م. ١٦)، أو المساس بالقيم الدينية والنظام العام (م. ١٩)، والإرهاب الالكتروني (م. ٢٠)، أو تبييض الأموال (م. ٢١)، أو الاتجار بالبشر (م. ٢٢)، أو الاتجار بالأعضاء البشرية (٢٣)، أو الاتجار بالأسلحة (م. ٢٤)، أو الاتجار بالمخدرات والمؤثرات العقلية (م. ٢٥)، أو الاعتداء على الملكية الفكرية أو الصناعية (م. ٢٦)، أو الاتجار بالتحف والآثار الفنية (م. ٢٧)، أو التعدي على البطاقات المالية (م. ٢٨).

وفي عام ٢٠١٠، أنشأت سلطنة عمان "المركز الوطني للسلامة المعلوماتية OCERT[٤٣]. وتستضيف السلطنة "المركز الإقليمي للأمن السيبراني للمنطقة العربية، التابع للإتحاد الدولي للاتصالات، ويهدف هذا المركز إلى تقديم الخدمات والمبادرات للمنطقة العربية لتحسين قدرات الأمن الإلكتروني عن طريق التنسيق وتعزيز التعاون الإقليمي.

١٦. **سوريا:**

قامت الجمهورية العربية السورية منذ عام ٢٠٠٤ بوضع استراتيجية وطنية لتقانة المعلومات والإتصالات. وفي عام ٢٠٠٩، اعتمدَتْ سوريا قانونَ التوقيعِ الإلكترونيّ وخدمات الشبكة، رقم ٢٠٠٩/٤، والذي أحدثَ "الهيئةَ الوطنية لِخدماتِ الشبكةِ[٤٤]"، والتي بدورها أحدثت "مركز أمن المعلومات" بهدف إصدار نشرات دورية عن التنبيهات الأمنية، وأدلة عن الثغرات الأمنية، وتقديم خدمات في أمن المعلومات للمؤسسات، والدعم الفني للجهات الحكومية لمنع إختراق موقعها الإلكتروني أو نشر بيانات ومعلومات خاصة بها دون تصريح. كما أن سوريا في صدد إنشاء "مركز الاستجابة لطوارئ الحاسب الآلي" syCERT من ضمن هذا المركز.

ثم أصدرَتْ، قانونَ تنظيمِ قطاع الإتصالاتِ رقم ٢٠١٠/١٨، الذي يُؤكّد في المادة ٥٠ منه على مبدأ احترامِ الخُصوصيّةِ؛ وأَنشأَ القانون "الهيئةَ الناظِمةَ لِقطاع الإتصالاتِ[٤٥]"، ونص على إحداث ضابطة عدلية مختصّة بالمخالفات والجرائم المتعلقة بخدمات الإتصالات. وفي عام ٢٠١١، صدر قانون الإعلام بالمرسوم التشريعي رقم ١٠٨، تاريخ ٨ آب/أغسطس ٢٠١١، يتضمن هذا القانون ١٠٦ مواد توزعت على ٨ فصول هي التعاريف, المبادئ الاساسية, الحقوق والواجبات, المجلس الوطني للاعلام, حق الرد والتصحيح, الترخيص والاعتماد وإجراءاته, العقوبات واصول المحاكمات, وغيرها بهدف تنظيم وسائل التواصل على الشبكة. كما صدرَ المرسوم التشريعي رقم ٢٠١٢/١٧ المُتعلّق بِتنظيمَ التواصِلِ على الشبَكَة ومكافحة جريمَةِ المعلوماتيّةِ، وهو ينظّم مسؤوليات مزودي خدمات الشبكات وواجباتهم والتعريف عن مزود خدمات الاتصال على الشبكة، وينص على إحداث ضابطة عدلية مختصة. وصدر عن وزارة الإتصالات والتقانة القرار رقم ٢٩٠ لعام ٢٠١٢ لتنيسق التعليمات التوضيحية والتنفيذية لهذا القانون.

وفي عام ٢٠٠٩–٢٠١٠ وضعت وزارة الاتصالات والتقانة استراتيجية مفصلة للحكومة الالكترونية، تضمنت الإشارة إلى قضايا أمن النظم المعلوماتية الحكومية وسبل حمايتها[٤٦]. وفي عام ٢٠١٤ أصدرت

وزارة الاتصالات والتقانة وثيقة "السياسة الوطنية لأمن المعلومات" التي حدّدت مجالات ومتطلبات العمل في هذا الشأن[٤٧]. ويمكن الإشارة هنا الى اعتماد هذه الوزراة مجموعة من المعايير الخاصة بتكنولوجيا المعلومات، منها ما يتعلق بحماية تقانة المعلومات والاتصالات[٤٨].

على الصعيدِ الإداريّ، هناك إدراكٌ لأهميةَ الحوسبَة السحابيةِ في كِلا القِطاعيَن العامِ والخاصِ، لا سيما تِجاه التفاوتِ الكبيرِ بين المُؤسساتِ الحُكوميّةَ في توصيفَ البرمجياتِ اللازِمةِ لِلعمل.

١٧. فلسطين:

بادَرَتْ فلسطين إلى التأكيد على أهمية اعتماد الحوسبَة السحابيَة مُواكبةً لِتوجّه العصر ونظراً إلى مزاياها المُتعدّدة في تطوير المُجتمع المحليّ في سائِر مشارِبِه، لا سيما لناحية تبادُل المعلومات وتعزيز خدمات الإتصالات ومؤسسات التعليمِ وقطاع الأعمال.

على الصعيد الحكومي الرسمي أنشأت وزارة الاتصالات وتكنولوجيا المعلومات حديثاً مركز البيانات الوطني National Data Center حيث انتقلت الوزارة من تقديم الخدمات من خلال البيئة التقليدية وهي كل خدمة على خادم منفصل إلى البيئة الافتراضية بمعنى تقديم الخدمات من خلال التكنولوجيا الافتراضية وتوفير سعات كبيرة جداً لحفظ البيانات الحكومية والنسخ الاحتياطي التلقائي. حيث أن الوزارة بصدد استخدام تقنية الحوسبة السحابية الخاصة "Private Cloud Computing" والتي تخدم الحكومة الفلسطينية، حيث أنه من خلال استخدام هذه التقنية نقوم بتقديم الخدمات الحكومية سواء كانت رئيسية أو احتياطية لباقي المؤسسات دون الحاجة لوجود مراكز لحفظ البيانات في المؤسسات.

أما على صعيد القطاع الخاص هناك بعض الشركات الخاصة والتي تعمل في مجال تكنولوجيا المعلومات والاتصالات تستخدم الحوسبة السحابية الخاصة private clouds والتي تشمل (SAS,PAS, IAS) ومنها من يعمل كمزود خدمة لشركات عالمية.

كما أصدرت دولة فلسطين سلسلة قوانين وقرارات أبرزها:

- قرار رقم ٢٠ لعام ٢٠٠١، الذي أنشأ الهيئة الوطنية لمسميات الإنترنت
- قرار مجلسِ الوزراءِ في فلسطين رقم ٣٥ لعام ٢٠٠٤، الذي يتناول حقّ النفاذ إلى الشبَكَة العالميَة للمعلومات (الإنترنت) والبريد الإلكتروني عبر مركز الحاسوب الحكومي.
- قرار مجلس الوزراء رقم ٣ لعام ٢٠٠٤ بشأن منع بيع وتسويق خدمات الاتصالات وتقنية المعلومات والبريد السريع.

- قرار مجلس الوزراء رقم ٢٦ لعام ٢٠٠٥، بالمصادقة على السياسات العامة لاستخدام الحاسوب وشبكة الإنترنت في المؤسسات العامة.
- قرار مجلس الوزراء رقم ٧٤ لسنة ٢٠٠٥ بشأن الإستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات (في هذا الصدد قامت الوزارة باعتماد الخطة الاستراتيجية لقطاع الاتصالات للأعوام ٢٠١٧-٢٠٢٢ وكذلك اعتماد الخطة الاستراتيجية الوطنية للحكومة الالكترونية).
- قرار مجلس الوزراء رقم ٦٥ لعام ٢٠٠٥ للمصادقة على اعتماد مبادرة فلسطين الإلكترونية.
- قرار اعتماد إطار التبادل البيني "زنار" قرار رقم (١٤/٤١/١١/م.و/س.ف) بتاريخ ٢٠١٣/٠٢/١٩ بشأن اعتماد إطار التبادل البيني (زنار) في جميع الوزارات والمؤسسات الفلسطينية كوثيقة مرجعية لإطار التبادل البيني.
- اعتماد وثيقة سياسة أمن المعلومات بقرار رقم (١٣/١٢٧/٠٨/م.و/س.ف)
- قرار إنشاء فريق فلسطين للاستجابة لطوارئ الحاسوب (أمن المعلومات) قرار رقم (١٤/٤٦/٠٨/م.و/س.ف) بتاريخ ٢٠١٣/٠٣/١٢.
- قرار تشكيل الفريق المركزي الدائم للحكومة الالكترونية بقرار رقم (١٧/٤٥/٠٨/م.و/ر.ح).
- قرار تشكيل اللجنة الوزارية العليا بقرار رقم (١٦/٢٤/٢٢/م.و/ر.ح).

بالإضافة الى ذلك يوجد العديد من القوانين قيد الاعداد أبرزها:

- قانون المعاملات الالكترونية في عام ٢٠٠٩ صدر قرار مجلس الوزراء رقم (١٣/٢٢/٠١/م.و/س.ف) لإنشاء لجنة وزارية لمناقشة مشروع قانون المعاملات الالكترونية من قبل مجلس الوزراء بتاريخ ٢٠١٦/٥/١٧ بموجب القرار رقم (١٧/١٠٣/٠٢/م.و/ر.ح) وتم إحالته لرئيس دولة فلسطين لإصداره.
- قانون الجرائم الالكترونية تم عرضه على مجلس الوزراء للقراءة الثانية من أجل اعتماده قبل المصاقة عليه من قبل رئيس الدولة
- قانون حماية البيانات والمعلومات الشخصية، صدر بتاريخ ٢٠١٦/٤/١٢ قرار مجلس الوزراء رقم (١٧/٩٨/٠٩/م.و/ر.ح) لعام ٢٠١٦ بتشكيل لجنة لإعداد مشروع قانون حماية البيانات والمعلومات الشخصية.

١٨. قطر:

منذ عام ٢٠١١، شكّلت الحوسبةُ السحابيةُ في قطر، تحت مظلة وزارة المواصلات والاتصالات (ictQATAR) وبدأت بتقديم خدماتها للجهات الحكومية المختلفة وهي تعملُ على بناءَ سحابةٍ حكوميةٍ خاصةٍ لإضفاءَ الكفاءَةِ والرِيادةِ على مؤسساتِ الحكومَةِ، وخفضَ تكلفةِ الإستثمارِ، وعلى تهيئةِ المُناخِ للحوسبةِ السحابيةِ من خِلال وضعِ السياساتِ اللازمةِ مثل قانون خصوصيةِ وحمايةِ البياناتِ. وفضلاً عن ذلك، تتعاونُ قطر مع مُقدّمي الخدماتِ السحابيةِ المُبتكرةِ لتلبيةَ احتياجاتِ المؤسساتِ الصغيرةِ والمُتوسطة.

على الصعيدِ التشريعيّ، هناك العديدُ من القوانين والمُبادرات السارِيةِ المفعول، والتي تهدُف إلى بناءَ إطارٍ تشريعيّ وتنظيميّ للحوسبةِ السحابيةِ في قطر. بحيث يَتبنّى الدستورُ القطريّ لعام ٢٠٠٣ المادة ٣٧ من مبادئ الإرشاد الأوروبي لعام ١٩٩٥، والتي تنصُّ على حُرمة خصوصيةِ الإنسانِ، فلا يجوز تعرُّضُ أيّ شخصٍ لأيّ تدخُّل في خُصوصياتِه إلّا وِفقاً لأحكامَ القانونِ، وبالكَيفيةِ المنصوصِ عليها فيه.

كما أصدرت قطر القانون رقم ١٤ لعام ٢٠١٤ المتعلق بمكافحة الجرائم الإلكترونية٤٩، وهو ينص على تجريم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية (المواد ٢و ٣ ٢ ٤)، وجرائم المحتوى (٩-٥)، والتزوير والاحتيال الإلكتروني (١١-١٠)، وجرائم بطاقة التعامل الإلكتروني (١٢-١٢)، والتعدي على حقوق الملكية الفكرية (١٣-١٣). ويحدد هذا القانون التزامات مزودي الخدمة (م. ٢١) والتزامات أجهزة الدولة (م. ٢٢).

كما يتميز هذا القانون بنصه على إجراءات التحقيق الواجب اتباعها والأدلة (المواد ١٤-٢٠)، وعلى إجراءات التعاون الدولي لناحية القواعد العامة (م. ٢٣-٢٩) والمساعدة القانونية المتبادلة (م. ٣٠-٣٨) وتسليم المجرمين (م.٣٩-٤٣).

كما صدرَ قانونُ الإتصالاتِ في قطر رقم ٢٠٠٦/٣٤، الذي يوجِب على مُقدّمي خدماتِ الاتصالاتِ باستخدامَ شبكاتِ الاتصالاتِ السِلْكيّةِ واللاسلكيّةِ والأنظمةِ المُتعلّقة بها الحِفاظَ على خُصوصيّة العُمَلاء وتحمُّل مسؤولية حِماية البياناتِ وضبطِ الاتصالاتِ التسويقيّةِ. إضافة إلى "قانون معاملات التِجارةِ الإلكترونية" رقم ٢٠١٠/١٦ (في ٢٠١٠/٨/١٩)، الذي أضافَ بعض الأحكام التي تتعلّقُ بحماية البياناتِ الخاصَةِ.

وهناك قانون مركز قطر المالي[٥٠] Qatar Financial Centre، الذي يتضمن حمايةَ البياناتِ واللوائحِ الخاصةِ بهم[٥١]، إلّا أنّ تطبيقَ أحكامه القانونيةُ تُطبّقُ فقط على الأنشِطَةِ الخاصةِ بالمركزِ والخدماتِ المصرفِيَةِ أو على التحوِيلاتِ المالية (على غرار مركز دبي المالي المذكور أعلاه).

كما أنّ هناك مشروعَ "قانون الخصوصية وحماية البيانات الشخصية" في قطر وهو قيْد التصدِيق، وقد تمَّ تعديله كي يتضمَّنْ إلزاميةَ المحافظةِ على سرية البياناتِ الشخصيةِ الخاصةِ بالأفرادِ والشركاتِ، كما أنّه سيفرُض غراماتٍ ماليةً مُرتفعةً على كشفَ أيّة معلومةٍ ماليةٍ أو غير مالية للعُملاء من دون أخذِ مُوافقتِهم؛ مما يُساعدُ في ضمانَ أمنِ، وحِمايةِ البياناتِ التي يتمُّ استضافتِها من قِبل المورّدين المحليّين.

على صعيد "أجهِزة إنفاذِ القانون" ، فقد أنشأَتْ قطر العديدَ من الجِهاتِ التي تتعاونُ فيما بينها وتتولّى تحقيقَ الأمنِ والسريةِ عبر الإنترنت، أهمها: "الفريقُ القطَري للإستجابةَ لطوارِئ الحاسباتِ[٥٢] Q-CERT، الذي يلعَبُ دوراً وِقائياً في تحديدَ التهديداتِ الرئيسيةِ للحيّز الرقمي والتنبيه لها وحلّها قبْل أنْ تُسبّب في وقوع ضررٍ للأشخاصِ أو للأفراد أو للجهاتِ. كما أنَّ هناك "مركزَ مكافحة الجريمة الإلكترونية" في وزارة الداخليةِ القطريةِ، بِهدف كَشْف هذه الجرائِم وتنفيذِ القوانين واللوائِحِ التي تصدُرها الحكومةُ ضد المُنتهكين.

في شهر يونيو ٢٠١٤، وضعَتْ قطر "سياسةَ تأمينِ الحوسبةِ السحابيةِ للمؤسساتِ الحكومية" بهدَفِ تقديمِ نظرةٍ عامةٍ على ما تنطوي عليه هذه الحوسبة من تحدياتٍ تتعلّقُ بالأمنِ والخُصوصيّة، ومُناقشةِ التهديداتِ والمَخاطرِ التكنولوجية ووسائِل الحِماية للبيئاتِ السحابيةِ، أيضاً بهدف توفير الرؤيةِ والأفكارِ اللازِمَةِ لمُساعدةَ صُنّاع القرار في قِطاعَ تكنولوجيا المعلومات والاتصالات على اتخاذ قراراتٍ مدروسَةٍ وتطبيقيّة.

كما وضَعَتْ" إرشاداتِ المُمارساتِ الأفضل في الحوسبةِ السحابية"، التي تتضمَّن إجراءَ تقييمِ الجُهوزيّةِ لِمُتطلّباتِ هذه الخدماتِ، وإنشاءَ استراتيجيةٍ وطنيَةٍ، ومُناقشةَ نِقاطِ النَجاحِ والإخفاقاتِ، وتقييم ماهيةِ البياناتِ التي يجب الإحتفاظ بها وتلك التي لا أن يُمكِن أنْ تُحْتَفَظَ، وتَحقيقَ ضماناتِ الأداءِ، وتوافرَ البياناتِ من مزوّدي الخِدمةِ، وغيرها العديدِ من الإشاراداتِ التوعويةِ.

في شهر مايو ٢٠١٤م اعتمدت دولة قطر "الاستراتيجية الوطنية للأمن السيبراني" والتي تعزز مفهوم الأمن السيبراني على مستوى الدولة وتركز على خمسة أهداف هامة (حماية البنية التحتية للمعلومات الحيوية الوطنية ، الاستجابة للحوادث والهجمات الالكترونية وحلها والتعافي منها ، وضع الاطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الالكتروني ، تعزيز ثقافة الأمن السيبراني ، تطوير وصقل المهارات

الوطنية) ، وكذلك تشجع المشاريع والمبادرات الخاصة في مجال أمن المعلومات المعنية للتقنيات الجديدة مثل الحوسبة السحابية وتطبيقات الهاتف النقال الجديدة وتنفيذ تكنولوجيا الشبكة الذكية في قطاعات البنى المعلوماتية الهامة.

ويُركّز"معهد قطر لبحوث الحاسب الآلي"، على ثلاثة مَحاور بَحثيّة: البُنى التحتيّة لِلجيل القادِم من الحوسبَة السحابية، وخوارزميات موزّعة لِتغطية كمٍّ هائِل من البيانات؛ وخدمات الحوسبة السحابية وتطبيقاتِها. ويعمَل على تحسينَ بروتوكولات العرْض اللاسلكية لإستخدامها مع البِيئات السحابية، وإستخدام الحَوسبَة السحابية في خَلْق الجيل القادِم من الخدمات الإعلاميَة، وهندسة مراكز البياناتِ\ وتصميمها لِتلائم البيئات الصَحْراوية، وأَنشطة التَشغيل المُدارة سَحَابياً، وفهم التأثير البِيئي لِلحوسبَة في بِيئة مراكِز البيانات.

١٩. **لبنان**:

على الصعيدِ التشريعيّ، إعتمدَ مشروعُ قانون ECOMLEB (الذي أعدتّه وزارة الإقتصادِ والتِجارةِ اللبنانيةِ) مُصطلَحٌ واسعُ النِطاقِ وهو "البيانات الخاصة" مُستوحياً نصوصِه من القانونِ الفرنسيّ رقم ٢٠٠٤. كما أعدَّت الوزارة مشروعَ قانونٍ جديدٍ حول "المُعاملات الإلكترونيةِ والبياناتِ ذات الطابعِ الشخصيّ" مُقتبسٌ أيضاً عن القوانينِ الفرنسيةِ والإرشاداتِ الأوروبيةِ ومُتوافقاً مع سائِر الإتجاهاتِ الدُوليةِ الحديثةِ في هذا المِضمارِ. وقد سبق للبنان أن أقر القانون رقم ١٤٠ بتاريخ ٢٧ تشرين الأول/أكتوبر ١٩٩٩ المتعلّق بصون الحق بسرية المكالمات الهاتفية.

وفي السياقِ عينه، يتعاونُ لبنان مع الإتحادِ الدولي للاتصالاتِ ITU من خلال:

- المشاركةُ في اجتماعَ لُجنة الدِراساتِ ١٧، لِقطاعَ تقيّيس الإتصالاتِ، التي تُنسّق العملَ المُتعلّق بالأمنِ السيبرانيّ في جميع مجموعاتِ الدِراسةِ ITU–T
- اقتراحُ المُساهمات في لِجنة الدراسات ١٧، التي تعمَلُ حالياً على الأمنِ السيبرانيّ وإدارة الأمنِ وهندسَة الأمن والأُطر ومُكافحة البريد المُزعج وإدارة الهُويّة وحِماية المعلومات الشخصية وأمن التطبيقاتِ والحوسبةِ السحابيةِ.
- المُتابعة والمُساهمة في1 / 1_Q22، في مجموعةَ دراسة ١ (ITU–D) بعنوان " أفضل الممارسات لتطوير ثقافة الأمن السيبيراني "

بدورها قامَتْ "الهيئة المُنظّمة للاتصالات" عام ٢٠١٢ بإعداد خُطّة وطنية لِحماية وأمن الفَضاء السيبرانيّ في لبنان، ودِراسة مُفصّلة لِلتدابير والإجراءات اللازِمة لِتأمين الحماية لِشبكات الاتصالات الوطنيّة من القرصنَة؛ وفي تموز/يوليو ٢٠١٥ أطلَقَتْ وزارةُ الاتصالات اللبنانيّة "رؤية الإتصالات الرقميّة لعام ٢٠٢٠"[٥٣].

كما أنّ هناك العديد من الأسئلة التي تَنتظرُ الإجابة في لبنان في الوقتِ الراهِن، أبرزُها يتعلّقُ بالسيادةِ على البياناتِ؟ ومكان تخزينِها؟ ومَنْ سوفَ يمتلكُ هذه السحابَة الحكومية؟ وأيّ قانون سيُطبّق عليها؟ ومدى تعهُّد مُقدّمي خدمات الحوسبة السحابية بِعدم نقل قاعدِة البيانات إلى الخارجِ؟ لا سيما البيانات المُتعلّقة بالأمن الوطنيّ والسِيادة اللبنانيّة؟ وهل سيعْتمدون سحابَةً واحِدةً أمْ عِدّة سحاباتٍ؟ هذه أُمورٌ لم تُحْسَم بعد لكن تَمّ تشكيل لِجان حُكوميّة لِنقاش هذه الخطواتِ.

عملياً، تُوفّر شركةُ مايكروسوفت في لبنان حلولَ السحابَة العامَة والخاصة إستجابَةً لِمتطلّباتِ عُملائِها، وبِغضّ النظرِ عن إستعداد الوِزارات اللبنانيّة لاعتماد الحوسبة السحابية، والأَهم أَنْ يكون هناك وعيٌّ من قبل الجِهات الحُكومية حول أهميّتِها وكيفيّة إستخدامِها. لكن يبقى الأساسُ وهو أنْ يكون هناك قانونٌ لِلمعاملاتِ الإلكترونيّة وجرائمَ المعلوماتية في لبنان. كما أنَّ هناك عدداً من الشركات تُقدّم خدماٍ إستضافة سحابات في لبنان وتعملُ مع الشركات المتوسطة والصغيرة التي لا تملُكْ قُدراتٍ تشغيلية وتُفضّل أنْ تكون جميع الخدمات التكنولوجية مُؤمنةً عِبر سحابةٍ عامةٍ. نُشير إلى أنّه، وبشكل عام، هناك قاعدة بيانات تَحتاجُ إلى خُصوصيةٍ أعلى ويجب أنْ تبقى داخل البلِد، مثل موضوع السريةِ المصرفيةِ التي تُلزمُ البنوكَ بأن تُبقي معلوماتِها داخل لبنان.

كما يعاني لبنان من غياب التشريعات المتخصصة والقواعد الإجرائية الخاصة، وعدم وجود محاكم متخصصة، وعدم وجود مركز للإستجابة لطوارئ الحاسوب (إنما هناك مساع لإنشاءه)، وعدم وجود قواعد سلوكية، وعدم كفاية الحملات التوعوية والدورات التدريبية للقضاة والضابطة العدلية وللرأي العام.

٢٠. ليبيا:

بادرَتْ ليبيا حديثاً وفي شهر نوفمبر ٢٠١٥ إلى إطلاقَ أوّل "وِكالة أنباء ليبية "إل سي إن إيه" تعتمدُ على الحوسَبَةِ السحابيةِ" ويتمُّ تحميلُها على خِدمةٍ سحابيةٍ تقعُ خوادمُه خارِج البِلادِ. وفي سبتمبر الماضي، تمَّ إطلاقُ "المنظومةَ الإلكترونيةَ الجديدةَ الخاصة بالطلبَةِ الليبيين" التي تعتمد على تقنياتِ الحوسبَةِ السحابيَةِ. بدورِها أطلقَتْ وزارةُ الاتصالات والمعلوماتيةِ "مبادرةَ ليبيا الإلكترونيّة"[٥٤]، لإرساءَ البُنيةِ التحتيّةِ لليبيا الإلكترونيةِ، مُتضمّنةً الخدماتِ الإلكترونيّةِ: الشبكاتُ، النُظُم، البياناتُ المُشتركةُ، والأمنُ وسائر

قواعِد هذه الُبنية. ومن ضِمن الإستراتيجياتِ أيضاً بِناء وتطويرِ مركزِ معلومات مركزيّ خاص لِتقديمَ الخدماتِ التقنيةِ المُشتركَةِ والإستفادةِ من تقنياتِ الحوسبَةِ السحابيَةِ، ووضْع القوانين والأنظمة والسياسات والحوكمة الإلكترونية لضمانَ الشفافية ودعم النُظُم الإلكترونية.

على الصعيد التشريعي، لم يقم المشرع الليبي بإصدار أي قانون خاص بالمعاملات الالكترونية أو الاتصالات والتكنولوجيا أو جرائم المعلوماتية، وإنما اقتصرت معالجته لموضوع المعاملات الالكترونية على إصدار مادة وحيدة في ثنايا قانون المصارف عالجت بحياء موضوع الاعتداد بالأدلة الالكترونية في إثبات نوع واحد من المعاملات وهي المعاملات المصرفية. وحالياً تعد بعض الجهات مشروعي قانون لتنظيم المعاملات الإلكترونية، ولمكافحة جرائم المعلوماتية[٥٥].

٢١. مصر:

يورد الدستور المصري الجديد بعض المبادئ القانونية فيما يخص استخدام المعلوماتية، فينص في مادته رقم ٣١ على أنّ أمن الفضاء المعلوماتي جزء أساسي من منظومة الأمن الاقتصادي والأمن القومي. كما تنص المادة ٥٧ منه على حرمة الحياة الخاصة وعدم المساس بالمراسلات البريدية والبرقية الإلكترونية والمحادثات الهاتفية. وتلتزم مصر بحماية المواطنين في استخدام وسائل الاتصال العامة بأشكالها كافة.

تُولي "وزارة الاتصالات وتكنولوجيا المعلومات"، في مصر الحوسبَةَ السحابيةَ ومراكزَ البياناتِ والحلولِ المُتكاملَةِ وويب ٢,٠ أهميةً بارِزةً، بِهدف تشجيع ودعمِ تنميَةِ الحوسبَةِ السحابيةِ واستخداماتِها، وكذلك التقنياتِ ذات الصِلةِ في الحُكومةِ. وقد تمَّ توقيعُ، العديدَ من مُذكراتِ التفاهُمِ مع مُختلف الجِهاتِ الأجنبيةِ، (المانيا وماليزيا وسنغافورة...) من أجلِ تبادُل الخُبراتِ لِضمانَ جاهزيَةِ الكوادِرِ المَصريةِ لِلحاقَ بهذه الصناعَةِ الجديدةِ.

كما عُقِدَتْ وُرَشُ عَمَلٍ مُتعدّدة منذ عام ٢٠١٢، وتم اجراء دورات تدريبية للقضاة وللضابطة العدلية، وتمَّ تنظيمُ "يومَ التكنولوجيا حول الحوسبةِ السحابيةِ" وعُطلةَ "نِهاية الأسبوع حول الحوسبةِ السحابيةِ" بهدف نشْر الوَعي بأهميتها وتقديم التوجُّهاتِ العالمية وأفضل المُمارساتِ.

أمّا على الصعيدِ التشريعيّ، فلا بُدّ من الإشارةِ إلى القانونِ رقم ١٠ لعام ٢٠٠٣ (قانون تنظيم الإتصالات)٥٦، الذي ينظِّمُ لوائحَ، وخدماتِ شبكاتِ الإتصالاتِ بما يُضفي الصفةَ القانونيّةَ على الدورِ الحيويّ الذي يُؤدّيه مُزوّدي خِدماتِ الإنترنيت.

كما بادرت وزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية في أغسطس ٢٠١١ بتشكيل لجنة من الخبراء من ذوي التخصصات المختلفة، القانونية والتقنية، من أجل صياغة مجموعة من مشروعات القوانين الجديدة ذات الصلة أبرزها:

- مشروع قانون "حرية المعلومات" الذي يعالج من ضمن ما يعالجه مسألة تنظيم إتاحة البيانات والمعلومات وحماية البيانات الشخصية وتجريم استغلالها في غير الغرض الذي أعطيت من أجله. وعليه، فقد سعى مشروع قانون حرية المعلومات إلى وضع حدود وضوابط قانونية لحالات الإفصاح عن البيانات والمعلومات، مع التأكيد على الحق في الخصوصية والحريات العامة.
- مشروع قانون "أمن الفضاء المعلوماتي"، الذي يهدف إلى حماية الفضاء المعلوماتي بجميع مشتملاته من أي تعد خارجى.

على الصعيدِ القضائي، تمَّ إنشاءُ المحاكمَ الإقتصاديَة بموجب القانون رقم ١٢٠ لعام ٢٠٠٨، مهمتُها الفَصلُ في القضايا الجنائيَةِ المُتعلّقة بالأنشطَةِ الإقتصاديةِ والإستثماريةِ والقضايا المُرتبطة بِتكنولوجيا الاتصالاتِ والمعلوماتِ. وأُجْرِيَت تدريباتٍ متعددةً لِلقضاةَ ووكلاء النيابةِ العامَةِ بالتعاونِ مع المُنظماتِ الدوليةِ والشركاتِ المُتعدّدةِ الجنسيةِ المُتخصّصةِ في تكنولوجيا المَعلوماتِ والاتصالاتِ. كما تمَّ إنشاءُ "إدارةً مُتخصّصةً لِمكافحَةَ جرائِمِ الحاسِباتِ والشبكاتِ في وِزارةِ الداخليةِ المَصريةِ" بمُقْتضى قرارٍ وِزاريّ رقم ٣٢٧ عام ٢٠٠٥، وتسمّى "إدارة مباحث مكافحة جرائم الحاسبات الإنترنيت".

وفي عام ٢٠١٠، أنشأت مصر "مركز للإستعداد لطوارئ الحاسبات والشبكات" EGCERT٥٧، وهناك "إدارة عليا في الجهاز القومي لتنظيم الإتصالات"٥٨ والتي تقدّم الخبرة الفنية في فحص الأدلة في الجرائم السيبرانية. ويهدف هذا الجهاز الى تحقيق وثبات ناجحة فى قطاع الاتصالات، مما يسهم فى دعم الإمكانيات ورفع شأن قطاع الاتصالات. كما يهدف إلى كونه حكم ذو ثقل فى القطاع يحفظ التوازن بين الدولة وصناعة الاتصالات والمستخدم.

٢٢. موريتانيا:

أطلَقَتْ"هواوي" جيلاً جديداً من حلولَ الحوسبَةِ السحابيَةِ والتخزين في جيتكس في عامِ ٢٠١٥ في موريتانيا. أما على الصعيد التشريعي، فلم يقم المشرع الموريتاني بإصدار أي قانون خاص بالمعاملات الالكترونية أو الاتصالات والتكنولوجيا أو جرائم المعلوماتية، إنما هناك مشروع "قانون الإطار القانوني للمجتمع الموريتاني للمعلومات" قيد الإعداد، وينص على حماية البيانات وإنشاء سلطة لضمان هذه الحماية وعدم نقل البيانات إلى الخارج إلا في بعض الحالات الإستثنائية. كما تبحث موريتانيا إدخال نظام التسديد الإلكتروني في التعاملات المالية للمصارف.

وابتداء من العام ٢٠١٤، يمكن القول أنّ حكومة موريتانيا بدأت تهتم بـ "الأمن السبراني" وتعزيز قدراتها في هذا المجال سعياً منها إلى حماية النظم والبيانات المعلوماتية للمؤسسات الحكومية والخاصة والفردية.

الجدول التالي يوضح الدول التي تمتلك مراكز وطنية للاستجابة للطوارئ المعلوماتية في المنطقة العربية:

اسم الدولة	اسم CERTs او اي هيئة أخرى	الموقع الالكتروني	سنة التأسيس
الأردن	الإعداد لإنشاء "مركز الاستجابة لطوارئ الحاسب الآلي مركز تكنولوجيا المعلومات الوطني المركز الوطني لأمن وإدارة الأزمات (٢٠١٥)	--------	-------
الإمارات العربية المتحدة	مركز الإستجابة لطوارئ الحاسب الآلي aeCERT	www.aecert.ae	2008
البحرين	إنشاء "هيئة تنظيم الاتصالات انشاء "بدالة انترنيت البحرين" تنظيم الجهاز المركزي للمعلومات لجنة عليا لتقنية المعلومات	www.bix.bh	
الجزائر	لا يوجد	--------	-----
السعودية	مركز الإستجابة لطوارئ الحاسب الآلي saCERT	www.cert.gov.sa	
السودان	مركز الإستجابة لطوارئ الحاسب الآلي sudanCERT	www.cert.sd	2010
الصومال	لا يوجد	--------	-----
العراق	لا يوجد	--------	-----
الكويت	الإعداد لإنشاء "مركز الاستجابة لطوارئ الحاسب الآلي"؛ هيئة تنظيم الاتصالات وتقنية المعلومات CITRA شبكة الكويت للمعلومات	https://www.cait.gov.kw/National-Projects/Kuwait-Information-Network.aspx	قيد الانشاء
المغرب	لجنة الرقابة الوطنية لحماية البيانات الشخصية	www.cndp.ma	-----
اليمن	المركز الوطني للمعلومات (١٩٩٥)	http://www.yemen-ic.info	-----
	مركز الاستجابة لطوارئ الحاسب الآلي tuCERT	www.tuncert.ansi.tn	2007

تونس			
جزر القمر	الهيئة الوطنية لتنظيم تكنولوجيا المعلومات والاتصالات	http://www.anrtic.km/	2009
جيبوتي	لا يوجد	-------	-----
سلطنة عمان	مركز الاستجابة لطوارئ الحاسب الآلي oCERT انشاء هيئة تنظيم الاتصالات	www.cert.gov.om	2010
سوريا	لإعداد لإنشاء "مركز الاستجابة لطوارئ الحاسب الآلي"؛	------	قيد الانشاء
فلسطين	لا يوجد	-------	-----
قطر	مركز الاستجابة لطوارئ الحاسب الآلي Q-CERT	www.qcert.org	2005
لبنان	الهيئة الوطنية لتنظيم الاتصالات TRA	http://www.tra.gov.lb/	
ليبيا	لا يوجد	-------	-----
مصر	مركز للإستعداد لطوارئ الحاسبات والشبكات EG-CERT الادارة العليا في الجهاز القومي لتنظيم الاتصالات	www.egcert.eg http://www.ntra.gov.eg/arabic/main.asp	2010
موريتانيا	لا يوجد	-------	-----

الفقرة الثانية: الممارسات الأفضل للإطار التشريعي للحوسبة السحابية: دراسة مقارنة

لقد أطلقت المُبادراتُ التشريعيّةُ في العديدِ من الدُول والمُنظمات الدولية والإقليمية لِتوفير الحمايَة القانونيةِ لِقواعدَ البياناتِ وعدم نَقلِها، أبْرزها، الأمم المتحدة والإتحاد الدولي للإتصالات ومنظمة حماية الملكية الفكرية WIPO والمجلس الأوروبي.

البند الأول: الأمم المتحدة والاتحاد الدولي للاتصالات والحوسبة السحابية:

تعكفُ لجنةُ الدراساتِ ١٧ التابعة لِقطاع تقييسِ الاتصالاتِ في الاتحادِ الدولي للاتصالاتِ على دراسة الأمنِ في الحوسبةِ السحابيةِ منذ أبريل ٢٠١٠، وتقومُ بِوضع مَبادئ توجيهيةٍ وإشتراطات في عدد من المجالاتِ من بَينها إدارة الهُويّة[٥٩].

وفي عام ٢٠١٣، أصدَرَ الاتحادُ تقريراً حول "اتجاهات الإصلاح في الإتصالاتِ ٢٠١٣ الجوانب العابرة للحدود الوطنية في تنظيم المجتمع المربوط شبكياً"، الذي تضمن فَصْل تحت عنوان "الحيز السحابي: حماية البيانات والخصوصية لمن يعود الحيز السحابي على أي حال؟" والذي يُناقشُ خدماتِ الحوسبةِ السحابيةِ ومنافعَها الإقتصاديةِ والإجتماعيةِ، والقواعِدَ التنظيميّةِ الحالية المُطبّقة عليها من حيث حِماية الخُصوصيّة والبياناتِ. ويُوصي بِوضع سياسات ولوائح متسقة ومتماسكة على الصعيدين المحلي والدولي لزيادة الإقبال على الخدمات السحابية العالمية بما يُوازنُ بين الإحتياجاتِ والفُرصِ التجاريةِ والواقعِ التكنولوجيّ والتَوقّعاتِ المَعقولةِ من جانب المُواطنين فيما يتعلّقُ بالخصوصيةِ في نِظام إيكولوجيّ رقميّ ودوليّ.

وبِشكلٍ عام، يبذُلُ الاتحادُ الدوليّ للاتصالاتِ جُهوداً حثيثةً في تَوفير الأمنِ السيبرانيّ، فقد أصدرَ "دليلَ الأمنِ السيبرانيّ لِلُبلدان النامية" عام ٢٠٠٧، إضافةً إلى العديدِ من البرامِجِ وخُطط العملِ بِهدف توفيرِ المعاييرِ اللازِمةِ في تقديمَ خدماتِ الحوسبةِ السحابيةِ، وتعزيز استخدامِ أفضلِ المُمارساتِ لِتوفير الضمانِ الأمنيّ لها. فقد تمَّ تشكيلُ، العديد من المُنظمات المُعنيّةِ، أبرزُها تحالف الأمن السحابي"، (Cloud Security Alliance SCA) الذي يعكُفُ على وضع بروتوكولٍ لأَمْن الحوسبةِ السحابيةِ لنشر أَفضلِ المُمارساتِ في الصِناعةِ وتحقيق الشفافيةِ لمُستعمليّ الحوسبةِ السحابيةِ.

وهنا تجدرُ الإشارةُ إلى المشروعِ الذي أطلقَه "الاتحاد الدولي للاتصالات" ITU بالتعاونِ مع المنظمة العربية للثقافة والتربية والعلوم ALECSO[٦٠]تحت مظلة الشبكة العربية لمشغلي الاتصالات (ARGENET) حول استخدام تكنولوجيا الحوسبةِ السحابيةِ في المؤسساتِ التعليميةِ العربيةِ بهدف الإطلاعِ على مدى إعتمادِ هذه الحوسبةِ في المؤسساتِ التعليميةِ والبحثيةِ في الدول العربية، ونِسبة إستخدام الحوسبةِ السحابيةِ فيها، ولِنشر الوعي بِمزايا وفوائدها ، خاصة لخِدمة التعليمِ والمُتعلّمين ودعم استخداماتها في قطاع التعليمِ والبحثِ العِلمي في العالمِ العربيّ.

تبرز أهمية هذا المشروع نظراً إلى ما تعانيه مؤسساتِ التعليمِ العالي في الدول العربية من غياب خُطط تطويرٍ رقميةٍ واضِحةِ المعالِم، عِلماً أنّ قِطاعَ التعليمِ يُعتبرُ من أكثر القِطاعاتِ المُستفيدةِ من خدماتِ الحوسبةِ السحابيةِ، من هنا تبرُزُ أهميّة تطوير البُنيةِ الرقميّةِ في التعليمِ والمُؤسساتِ التربويةِ، لا سيما التعليمِ العالي في الدُولِ العربيةِ، وتزويدِ الأستاذ الجامعيّ والمدرّس بأدواتِ الإبداعِ والإبتكارِ، وحصول الطالبِ على عدَد ضخمٍ من الموارِدِ المُتمثّلةِ في برامجَ ومصادرَ المعلوماتيّةِ، والوصول إلى بعض المكتباتِ الأجنبيةِ والمحليةِ وسائِرِ البرامجِ بِتكلفةٍ زهيدةٍ أو حتى مجانية، وتبادُل الأبحاثِ والدِراسات.

كما لحظَتْ مبادئُ الجمعية العامة، للأُمم المُتحدة بعض المبادِئ[٦١] التي تلتزِمُ الدولُ المعنيةُ بإيرادَها في قوانينها، أبرزُها: مبدأُ المَشروعيةُ والنزاهةُ في جمع البياناتِ الشخصيةِ[٦٢].

وبدورها أوصتْ، مُنظّمة التعاون الإقتصاديّ والتنميةِ OECD الدولَ الأعضاء الإلتزامَ بدليلَ حمايةِ الخصوصيةِ للأشخاص الطبيعيّين المُعالجة يدويّاً أو آلياً وفي القطاعين العامِ والخاصِ، وقد تضمَّنَ الدليلُ بعض المبادئ الأساسيّة[٦٣]. كما تنص المادة ٢٤ من إرشادات الإسكوا على مبدأ عدم نقل البيانات ذات الطابع الشخص إلى دول أجنبية إلا إذا أمن هذا البلد مستوى معين من الحماية القانونية. وتنص المادة ٢٥ منه على الإستثناءات، ومنها موافقة الشخص صاحب البيانات أو أن يكون النقل ضرورياً لأسباب معينة[٦٤].

<u>البند الثاني: دور رائد للإتحاد الأوروبي:</u>

لقد شكّلَ الإرشادُ الأوروبيّ لعام ١٩٩٥ (EC/46/95) تاريخ ١٩٩٥/١٠/٢٤، والمُتعلّق بِحماية الأشخاصِ الطبيعيين إزاءَ معالجة البياناتِ ذات الطابعِ الشخصيّ والتداول الحُرّ بِها، النواةَ الأوروبيةَ الأولى الراميةَ إلى حمايةِ البياناتِ الشخصيةِ، والمتوافقةِ مع السياسةِ الأوروبيةِ الراميةِ إلى حماية حقوقِ الإنسانِ، وقد اقتصَرَ تطبيقُ هذا الإرشاد على نِطاقَ الإتحاد الأوروبيّ.

وتنص المادة ٢٥ من الإرشادِ على منعَ تبادُل البيانات مع دُول خارج الإتحادِ الأوروبيّ[٦٥] لا تؤمّن حماية مُوازيَة للحمايَة التي تُؤمّنها الدُول الأوروبيّة[٦٦]. وتُعتبرُ "اللجنة الأوروبية" هي المرجَع الصالح لإعتبار ما إذا كانت الدولة الثانية تُؤمّن الحمايةَ ذاتها. ولغايَةِ تاريخِه، تُعدُّ الدولُ التي تؤمّن الحمايةَ عينها من خارج الإتحاد الأوروبي، قليلةَ العددِ، وهي كندا والأرجنتين وأوروغواي ونيوزيلاند وسويسرا وآندور وجرساي واسرائيل وجزر غيرنسي وجزيرة آيل أوف مان.

في السِياقِ عَيْنه، تمَّ عقدُ اتفاق الملاذ الآمن" Safe Harbor Agreement ("أو اتفاقُ المِيناء الآمن")[٦٧] مع الولاياتِ المُتحدةِ الأميركيةِ عام ٢٠٠٠[٦٨]، والذي يُلزمُ الشركاتِ الأميركيةَ بالعديدِ من المبادِئ التي تمنعُ الإعتداءَ على البياناتِ الشخصيةِ، وأبرزها: مُوجِبُ الإعلام وتَحديدُ الغايةُ من جمعَ المعلومات وإستخدامها أو نقلِها للغير؛ حقُّ قُبول نقل المعلوماتِ للغير، أو الرفضُ والتزام الغير بمبادئ الملاذِ الآمنِ؛ حقُّ الوصولُ إلى المعلوماتِ المُستقاةِ وتِصحيحِها، إضافَةً إلى أمنِ المعلوماتِ ، وصحَّة البياناتِ، وإيجاد آلياتِ للإعتراضَ والتطبيقِ والنظرِ في شَكاوى المُتضرّرين وتقرير العُطْلِ والضرَرِ.

ولا بُدّ من ذِكر "اتفاق الولايات المتحدة الأميركيّة مع الإتحادِ الأوروبيّ"، اتفاق واشنطن لعام ٢٠٠٤[٦٩]، الذي يفرضُ على الإتحادِ التأكُّدَ من التزامَ الناقليين الجويين بِتقديمَ كل المعلوماتِ المَطلوبَةِ لسلامَة الطيرانِ. حيث ألزمَ هذا الإتفاقُ أميركا بِضماناتٍ لتأمين الحمايةِ عينها المحدّدة من قبل الإتحادِ الأُوروبيّ. وفي عام ٢٠١٢، وقع الفريقان إتفاقاً آخر Safe Harbor (الملاذ الآمن او الرصيف الآمن)[٧٠]، يتضمّنُ نقلَ بياناتِ المُسافرين وتحليلَها، وحصرَ أهدافِه في مكافحةَ الإرهابِ، والإتجارِ بالمُخدراتِ، والإتجارِ بالرقيقِ، وسائِر الجناياتِ، والإحتفاظِ بهذه البيانات لمدّة عشرة سنوات، ضِمن إطارِ تعاونٍ قانونيّ وتنظيميّ وأمنيّ. علماً بأن هذا الإتفاقَ لا يُقدّم الأمانَ سِوى إلى الشركاتِ الكُبرى.

إنما وعلى الصعيدِ القضائيّ، وفي ٦ اكتوبر ٢٠١٥، قضَتْ المحكمةُ العُليا للإتحاد الأوروبيّ بِبُطلان "اتفاق الملاذ الآمن"[٧١] لتبادلَ البياناتِ مع أميركا بعد قضيةِ "فيسبوك"، مُعتبرةً أنّه لا يمكن للشركةِ المذكورةِ أنْ تُسلّم وبِبساطة بياناتِ المُستخدمين إلى السلطاتِ الأميركيةِ. وعلّلت المحكمةُ البُطلان بأنَّ شركةَ فيسبوك وعدداً من شركاتِ التكنولوجيا الأُخرى، وهي غوغل وأمازون، قد إسْتغلَّتْ هذا الاتفاقَ وأقدمَت على نقلَ بياناتِ المُستخدمين، وبِكمياتٍ ضخمةٍ، لأجهزتِها في الولاياتِ المتحدةِ الأميركيةِ، حيث سيتُمّ الإحتفاظُ بها هناك. وبالطبعِ، سينعكسُ هكذا الحكمُ على جميعَ الشركاتِ الأميركيةِ، التي تتعامَلُ مع بياناتٍ أوروبيَةٍ، بما في ذلك تويتر ومايكروسوفت وياهو وغوغل.

أما بالنسبةِ إلى المُستهلكين في منطقةِ الإتحادِ الأوروبيّ والمُتعاقدين مع مُزوّدي خدمات السحابة وغير الخاضعين "للملاذ الآمن"، فعليهم أنْ يخضعوا إلى تشريعاتِ الإتحادِ الأوروبيّ حول تصديرِ البياناتِ الشخصيةِ. وقد أنشأَتْ مؤسسة أمازون، على سبيل المِثال، موقعاً أوروبياً للحوسبَة السحابيةِ يُوفّرُ الثقةَ للمُستهلكين في أنَّ البياناتِ لن تُنقل عِبر الحدودِ بالشكلِ الذي يُعدّ انتهاكاً للتوجيه الأوروبيّ. وهنا لا بدّ من ذكر التَوصية الأوروبية[٧٢] تاريخ ٢٤ اكتوبر ١٩٩٥ حول حِمايةِ الأشخاصِ فيما يتعلق بمعالجةِ البياناتِ ذات الطابعِ الشخصيِ، وحريّة نقلِ المُعطياتِ بما فيها البياناتِ الطُبيّة والوِراثية.

عام ٢٠١٠، أصدرَتْ المفوضية الأوروبيةُ "نماذجَ بنودٍ" للإقتداءَ بها لدى تصديرِ بعض البياناتِ خارج الإتحادِ الأوروبيّ نشر يوم ٥ فبراير ٢٠١٠)(2010/87/UE [٧٣].

في السِياقِ عينه، صدَرَ الإرشادُ الأوروبيّ عام ٢٠٠٢[٧٤] مُستهدِفاً شركاتِ تقديمِ شبكاتِ الإتصالاتِ العامة والخاصة، والذي بموجبه ينبغي أنْ يكونَ النفاذُ فيها إلى البياناتِ الشخصيةِ بِتفويض شخصيّ للأغراضَ المُصرّح بها قانوناً، أو أنَّه ينبغي أنْ يكون تخزينُ البياناتِ الشخصيةِ أو نقلها محمياً ضِدّ الإتلافِ

العرَضيّ أو غير القانوني أو الضَياع أو التغيير العرَضي، وضد التخزين أو المُعالجة، أو النَفاذ، أو الإفشاءِ غير المُصرح به أو غير القانونيّ.

كما تجدرُ الإشارةُ، إلى "المعاهدةِ الأوروبيةِ معاهدة بودابست لمكافحة الجرائم السيبرانية، لعام ٢٠٠١ [٧٥] التي تنصُّ على التزامَ الدولةِ، حيث إرتُكِبَت الجريمةُ السيبرانيةُ، بالإحتفاظِ بالبياناتِ الخاصةِ بِحركة الاتصالاتِ والكَشفِ عنها إلى الدولةِ التي تطلُبُ هذه البياناتِ.

ولا بُدّ من ذكرالإطارِ التنظميّ لِعمل المجلسِ الأوروبيّ تاريخ ٢٧ نوفمبر ٢٠٠٨، حول حمايةِ البياناتِ الشخصيةِ[٧٦] في مجال التعاونِ القضائيّ والأمنيّ فيما يتعلق بالبياناتِ الخاصةِ بالشؤونِ الأمنيةِ والعسكريةِ المُتبادلةِ بين دول الإتحادِ.

بِدورهم، توجَّهَ قادةُ القِطاعاتِ الصناعيةِ والتجاريةِ في أوروبا إلى المفوضية الأوروبيّة لإيجاد الإطارِ التشريعيّ المُلائِم لِخدمات الحوسبةِ السحابيةِ[٧٧].

وفي عام ٢٠٠٩، أصدَرَتْ المُفوضيّة الأوروبية مُدوّنةَ سلوكٍ بشأن الكفاءةِ في استهلاك قواعد البياناتِ للطاقة، ووضعت مجموعةً من التدابيرِ الطوعِيةِ، منها تحقيق الكفاءةِ في تصميمَ وتشغيلَ قواعد البياناتِ[٧٨]. وفي ٢٥ يناير ٢٠١٢، نشرَتْ المفوضيةُ الأوروبيةُ التعديلاتِ المُقترح إدخالها على "التوجيه الأوروبيّ لحماية البياناتِ"[٧٩]، في محاولة لتنسيق الإطارِ التشريعيّ وسائر القوانين المحليةِ المُتعلقة بحماية البياناتِ ضمن دول الإتحاد. وتتضمن التعديلاتِ المُقترحةِ ما يلي:

- تمكين السلطاتِ التنظيميةِ الوطنيةِ من إتخاذِ إجراءاتٍ ضد الشركاتِ العامِلةِ في الدولِ الأعضاءِ الأخرى في ظُروف مُعيّنة، مع الحق في فرضَ غراماتٍ تصل إلى ٢ مليون يورو أو في بعض الحالات ٢ في المائةِ من حجمَ الأعمالِ السنويّ للشركَةِ.
- توسيعُ تعريفُ البياناتِ الشخصيةِ، بحيث يُغطّي أي معلوماتٍ متصلةٍ بصاحب البياناتِ، وتَشترطُ القواعدُ التنظيميةُ الحصولَ على موافقةَ صريحةٍ من الفردِ بالسماحِ بحجب البياناتِ.
- تطبيقُ القواعدُ التنظيميةُ فيما يتجاوز الإتحاد الأوروبي، بحيث تشمُلْ كل الدول الأوروبية (بما فيها تلك غير المنضمة الى الاتحاد الأوروبي) التي تمتلِكُ بياناتٍ شخصية ذات صِلة بمواطني الإتحاد الأوروبيّ.
- يُشترط أنْ تقومَ الهيئاتُ المعنيّة بالإبلاغِ بدون أي تأخير غير مبرر عن أي خرقٍ للبياناتِ وأن يتمّ ذلك في غضون ٢٤ ساعة من وقوع الخَرقِ.

- يُشترط أن تقومَ الشركاتُ المُتحكّمة في البياناتِ بتقييم مدى حِماية البياناتِ وتعيين مسؤولين عن حماية البياناتِ وإبلاغ الأطرافِ الأُخرى بأيّة خروقات.
- يكون للأفراد حقٌّ جديدٌ هو "الحق في النسيان" في ظُروف مُعيّنة ولا يكونوا مُطالبين بعد الآن بِدفع مُقابلٍ للنفاذ إلى بياناتِهم.
- تخضعُ عملياتِ النقلِ الدولي للبياناتِ لإطارَ تنظيميّ أكثر تفصيلاً ينصُّ على ضماناتٍ يجب تطبيقُها وعلى أَنْ تقومَ السلطاتِ بإجراء فُحوص مُسبقة وزيادة تقييد قُدرة الشركاتِ المُتحكمةِ في البيانات على إبطال هذه الضماناتِ.

وفي مايو ٢٠١٢، نشرَ البرلمانُ الأوروبيّ دراسةً، حدّدَت الطُرق التي ينبغي أنْ يتبنّاها واضعو السياساتِ لتيسيرَ الحوسبةِ السحابيةِ[٨٠]. وتشملُ هذه الطرقُ التعاملَ مع الثغراتِ المُتصّلة بالتشريعاتِ؛ وتحْسين الشروطِ والأحكامِ لجميع المُستعملين؛ ومعالجةَ المخاوف والشواغلِ المُتصلة بالأمنِ لدى أصحاب المصلحةِ؛ وتشجيعَ الأخذِ بالحوسبةِ السحابيةِ في القطاعِ العامِ[٨١]؛ وتشجيعَ التوسّع في البحثِ والتطويرِ في مجالاتِ الحوسبةِ السحابيةِ.

<u>البند الثالث: التشريعات المحلية الغربية:</u>

تنصُّ "المدونة النموذجية " للجمعية الكنديّةِ للمعايير على حِماية البياناتِ الشخصيةِ والوثائق الإلكترونيّة[٨٢]. كما استحدثت المحاكِمَ الكنديّة قانوناً عاماً عن الأضرارِ المُترتّبة على انتهاكَ الخصوصيةِ، وبالحقيقة فالقوانينُ الكنديّةُ لا تُقيّد النقلَ الدوليّ للبياناتِ الشخصيةِ ولكن أيّ عملية نقل تبقى ضِمن مسؤوليةِ الطرفِ الذي يُفشي البياناتِ.

كما يُجيز القانونُ البريطاني لعام[٨٣] ١٩٩٨ المُتعلّق، بِحماية البياناتِ، نقلَها إلى الخارجِ في حال تأكّدَت المؤسساتُ بنفسها من الحمايةِ المُلائمةِ لِهذه المعلوماتِ من قِبل البلدِ التي يتم نقلها إليه.

أيضاً، هناك القانونُ الأميركيّ باتريوت آكت Patriot Act [٨٤] (الذي أعقب هجمات ١١ سبتمبر ٢٠٠١)، والذي يسمحُ بِتقاسمَ البياناتِ الشخصيةِ الخاصةِ بأيّ فردٍ مُشتبه في ضلوعه في أَنشطة إرهابيةٍ أو في غسيل أموالٍ. وقد نشرَتْ اللجنة الوطنية للمعلوماتية والحريات في فرنساCNIL توجيهاً بشأن المُعالجة القانونية للبيانات الشخصية[٨٥] يفرضُ على الشركاتِ المُتحكّمةِ في البياناتِ شروطَ الإبلاغِ والتعاونِ والمُحافظةِ على أمن البياناتِ الشخصيةِ[٨٦]، ويفرضُ عليها في ظُروف مُعيّنة حصولَ الهيئةِ على مُوافقة مُسْبقةٍبِشأن مُعالجة البياناتِ[٨٧]. كما يفرضُ القانونُ الأميركيّ على كُل الشركاتِ مُقدّمي خدمات التخزينِ السحابي والتي تَتخِذُ من أميركا مقراً لها إتاحةَ البياناتِ المُخزّنة على خوادمها إلى سلطاتِ الأمنِ الأميركيّةِ.

التشريع الفرنسي: بدوره أصدرَ المُشرّع الفرنسيّ "قانون المعلوماتية والحريات" La loi informatique et Libertés رقم ٧٨/١٧[٨٨] في ٦ كانون الثاني ١٩٧٨ للمعالجةِ الإلكترونيةِ للبياناتِ الإسميةِ، وخضعَ لبِضعة تعديلاتٍ[٨٩] آخرها بموجب القانون ٢٠٠٤/٨٠١ [٩٠] ، الذي إعتمدَ بموجبه الإرشادَ الأوروبيّ لعام ١٩٩٥ المُتعلّق بِحماية البياناتِ ذات الطابِع الشخصيّ. وفي عام ١٩٨١ اعتُمِدَ هذا القانون كنموذج لإتفاقية المجلس الأوروبي[٩١].

يُعرّفُ هذا القانونُ البياناتِ الشخصيّة بأنّها معلومةٌ إسميةٌ تتعلّقُ بِشخص طبيعيّ مُحدّدة هُويّته أو من المُمكِن تحديد هُويّته بِطريقة مُباشرةٍ أو غير مُباشرة. يَستثني هذا التعريفُ بياناتٍ أخرى يُمكن أنْ تُساعدَ في الغايَةِ عينها. ونُشير إلى أنَّ تعديلَ عام ٢٠٠٤[٩٢] اعتمَدَ عِبارةً أكثرَ شُمولية وهي "البيانات ذا الطابع الشخصي" ، فيحدّدُ المُشرّع الفرنسيّ بهذا الإتساعِ صُوراً حديثةً أكثر إتساعاً للبياناتِ الشخصيةِ التي يتوجَّب حمايتها. إلّا أنَّ الإجتهادّ الفرنسي حدّدَ من صِلاحية القضاءِ الفرنسيّ في التطبيقِ فيما يتعلّقُ بتنازع الصلاحياتِ إذا كان الضررُ الذي وقعَ على الأرضِ الفرنسيّةِ ليس لا إحتمالياً ولا افتراضياً[٩٣]. نُشير هنا إلى التناقُضِ الحاصِل في الإجتهادِ الفرنسي حول حِماية البياناتِ الشخصيةِ، فبعضُ الأحكام قد صدر مُؤيّداً لهذه الحمايةِ[٩٤] والبعض الآخر يعارض هذه الحماية[٩٥].

ومِن أبرز التعديلاتِ، التي أُدخلِت على قانون العقوباتِ الفرنسيّ لعام ١٩٩٢ جاءَتْ في القانونِ رقم ٢٠١٢/٤١٠، تاريخ ٢٧ مارس ٢٠١٢، والقانون رقم ٩١٢ لعام ٢٠١٥، والصادر بتاريخ ٢٤ يوليو ٢٠١٥ (المادة ٤ منه)[٩٦] الذي أضافَ فقراتٍ جديدةً إلى الموادِ ١/٣٢٣ و٢/٣٢٣ و٣/٣٢٣ تتعلّقُ بارتكاب جريمةِ المعلوماتيّةِ على مُعطياتٍ ذات طابعٍ شخصيّ[٩٧].

كما أنَّ القانونَ الفرنسيّ لعام ١٩٩٨ يحمي قواعدَ البياناتِ لِمدّة خمس عشرة سنة ويُحظّر أي إعادة استعمالِ سواء لِجُزء من قاعدة البياناتِ أو للقاعدة بأكملها عن طريق توزيعِ نسخ أو الإيجار أو النقلِ على الإنترنت. ويُحظِّرُ النقلَ الكُليّ أو الجُزئيّ من مُحتوى قاعدةِ البيانات بأيّ شَكْلٍ متى كان الحصولُ أو النقلُ دائماً أو مُؤقتاً على دعامة بأيّ وسيلةٍ أو تحت أيّ شكْلٍ كان. أيضاً لا بُدّ من ذكر المرسومِ الفرنسيّ EDVIGE رقم ٢٠٠٨/٦٣٢[٩٨]، والذي يهدُف إلى تجميع معلوماتِ الأشخاصِ الطبيعيّين والمَعنويّين وتحليلِها.

البند الرابع: معايير قانونية، وقواعد تنظيمية واقتراحات حقوقية:

على الصعيدِ الميدانيّ، لا تزال الشركاتُ الأجنبيّةُ الكُبرى هي المُسيطرة على السوقِ العربيّ في مجال الحوسبة السحابية، فشركاتٌ كمايكروسوفت وأمازون وغوغل وغيرهم، تُعدُّ من أهمّ الشركاتِ المُوفّرة والمُزوّدة لخدمة البنية التحتية كخدمة الـIAAS ، وتكادُ تخلو السوقُ العربيةُ من أيّ منافسةٍ على مستوى هذه الشركاتِ. من هنا تبرُزُ محاذيرُ الإحتكارَ والمنافسَةَ غير المَشروعةِ من قبل هذه الشركات المُتخصّصة لعدم توافر المعاييرِ المُنظِّمة لِلصناعةِ أو نتيجة لِمعيار قائمٍ بِحكم الأَمرِ الواقِعِ. ويُعد القطاعُ العام مَصدَراً ثالثاً لمعايير الأمنِ في الحوسبَةِ السحابيةِ، بحيث بدأَتْ السُلطاتُ العامةُ في بعض البلدانِ تَتبنّى حلولَ الحوسبَةِ السحابيةِ التي يُوفّرُها القِطاعُ الخاصُ.

١. من هي هذه الشركات العالمية من وجهة نظر قانونية؟

إنْ صحّ وصف النِظام الإقتصادي العالمي الراهن بِأنَّه عصرُ العولمةِ، فمِن الأصح وَصْفه بِأنَّه عصرُ الشركاتِ المُتعدّدة الجِنسية بإعتبارَها العمودِ الفِقريّ لِهذه العولمةِ. وفي الواقع، تُعتبرُ هذه الشركاتُ مشروعاً يتكَّون من مجموعةَ وحداتٍ فرعيةٍ ترتبِطُ بالمركزِ الأصليّ في البَلَدِ الأُم بِعلاقاتٍ قانونيةٍ تخضَعُ لاستراتيجيةَ إقتصاديةٍ عامةٍ (من تَوجيه، وتخطيط، وتنظيم، وإشراف ومُراقبة...). وتتولّى الإستثمارَ في مناطقَ جُغرافيةٍ مُتعدّدةٍ. وتمتلكُ هذه الشركاتُ رصيداً من "رأس المال غير المادي" في شكلِ المعرفَةِ الفنيّةِ، وبراءات الإختراع، والعلاقاتِ التجاريةِ، والسُمعَةِ الطيّبة محلياً وعالمياً، فضلاً عن الأَدواتِ والفُنونِ التسويقيّةِ.

في الواقِع، وعلى الرُغم مِن أنّ هذه الشركات لا تتمتع بالشخصيةِ القانونيةِ الدوليةِ على غِرار الدولِ والمُنظماتِ الدوليةِ، فهي تَضطلعُ بِدور كبيرٍ في العلاقاتِ الدوليةِ كجَماعات ضَغْطٍ دوليّة سياسياً ونِقابياً ودينياً وماليا وإقتصادياً. كما تتمتّعُ بإمكاناتٍ ماليةٍ وتتجاوزُ نشاطاتُها حدودَ الدولةِ الواحدةِ وميزانِيَتها.

من جِهةٍ أُخرى، نُشيرُ إلى أنّ الحفاظَ على البياناتِ لا يُعتبر أحدَ أوجه الحقّ في الخُصوصيةِ فحسب[٩٩]، بل أحد حقوق المُواطِن الأساسيةِ في الحِفاظِ عليها من الاعتداءاتِ من الغيرِ وحتى من تدخُّل الدولةِ التعسُّفي أو من الشركاتِ الأجنبيةِ التي تخفي خلفَ خدماتِها العديدَ من البواطِنِ الأمنيةِ في انتهاكَ هذه الحقّ. إضافةً، إلى ما نشهدُه اليوم من قاعِدة معلوماتٍ إرهابيةٍ [١٠٠]Data espionage، وغيرها من الهجماتِ السَيْبرانيةِ ذات الإرتداداتِ الكارثيَةِ، كالحربِ السيبرانيّةِ والإرهابِ السيبرانيّ، وبحيث يضَع صنّاعُ القرارِ في الدُولِ العُظْمى مسائلَ الدفاعِ السيبراني والأمنِ السيبراني في رأسِ سُلمَّ الأولويَّات العسكرية ويَعتبرُونَها أولويَّةً في سياساتِهم الوطنيَّة والدفاعيَّة.

٢. البعد التعاقدي للإطار التشريعي للحوسبة السحابية: مقترحات ومعايير

من أبرز التحدياتِ، التي تُثيرُها التوجهاتُ التِقنيةُ الحديثةُ للحوسبة السحابيةِ هي التحديات التعاقدية والإداريّة في الدولِ العربيةِ، التي تتجلّى في "عمل العقود أو الاتفاقات" وتضمنُ أمانَ الخِدمةِ وتأمينها وحمايةَ المعلوماتِ، وِسط غِيابِ الخِبرةِ والتجارِبِ لدى القانونيين العرب وغِياب نماذج عُقود يُقتدى بها.

من هنا، يتضمَّنُ البُعدُ التعاقديّ للحوسبةِ السحابيةِ فِئَةَ العقدِ وبُنوده والآلياتِ المعنية لإدارة المسائِلِ والمَفاعيلِ القانونيةِ والأمنيةِ الخاصَةِ بتلك الخدماتِ التي تُؤمّنها خدماتُ هذه الحوسبةِ. ففي الواقِع، فإن فريقي مَشاكِل الأمنِ في الحوسبةِ السحابيةِ يتكون من كلاً من العميلِ ومُوفّر الخِدمةِ الذي يُلقى على عاتقه التزامَ توفُّر بُنيةٍ تحتيةٍ سليمةٍ ومُستودعاتِ تخزينٍ آمِنةٍ، لا سيما إذا كانَت خدماتُه غير مجانيّة.

الجدول التالي يبين تحديات البعد التعاقدي في عقود الحوسبة السحابية:

تحديات البعد التعاقدي في عقود الحوسبة السحابية
• غياب نماذج القوانين • غياب نماذج العقود • غياب الخبرة أو التجربة العربية • غياب الحماية الدستورية والقانونية للبيانات الشخصية • غياب القوانين العربية تجرم وتعاقب أعمال الشركات المتعددة الجنسية • فقط قواعد سلوكية مناقبية دولية أو أوروبية ذات التزامات معنوية

تعتبُر **مرحلَةُ ما قبل إبرام العقد** من المراحِلِ المُهمّة في التَفاوض وتحديد الشروط ومضمون عقود الإشتراك في الخِدمَة، مُروراً بالعقد ذات المُحتوى التقني، وعقود الجِهات ذات العلاقَة بِمواقع الإنترنت، أو عقود المُستخدِمين بما فيها عقود طلَب الخدمات وعقود الخدمات المدفوعة والمجانية، من أجل ضمان التعويضات اللازمة في حال الإخلال بِبنود العقد من قِبل أحد الطرفَيْن، ومُتابعة دفْع استحقاق مُزوّدي الخِدمة أو انقطاع خِدمة الإنترنت لِأسباب بيئية أو إدارية أو سرقة أو فك شِفْرَة كلمات السِرّ، أو مفاتيح التعامل مع الخِدمة.

الجدول التالي يبين ما هي التحديات لمرحلة ما قبل لإبرام العقد:

مرحلة ما قبل إبرام العقد
• التفاوض • تحديد الشروط القانونية والتقنية (العامة والتفصيلية والهامشية) • المسؤولية المدنية الجزائية المترتبة على الاخلال بالعقد ومقدار العطل والضرر

كما تعدُ مرحلةَ إبرام العقدِ من أهم المراحِلِ وأدقّها وما فيها من الإشكاليات الأوليةِ[١٠١] التي تُثيرُها خدماتُ الحوسبةِ السحابية وتطبيقاتُها، لا سيما لناحية المسؤولية المُترتّبة في حال إنهاء العقد وواجب مُقدّم الخِدمة بإعادة البياناتِ إلى العَميل (أكانت الدولة أم الأفراد)، وليس حجزُها وتهديد العميل بها أو تسليمُه نسخة مُصوّرة وليس الأصليّة.

الجدول التالي يوضح تحديات مرحلة إبرام العقد:

مرحلة إبرام العقد
• نوع العقد (عقد الاذعان / أو عقد الغرر) • عقد غير قابل للتفاوض أو للتعديل • تنازع القوانين وتحديد القانون الواجب التطبيق

لذلك لا بدّ للعميلِ من بَذْل الجُهودِ والعِنايَةِ المَطلوبَة لدى توقيع العقد مع مُقدّمي الخِدمة، ففي أغلَب الحالات تفرضُ فِئة "عقد الإذعان أو الغرر" [١٠٢](Contrat d'adhésion)، وهو نوعٌ من العقودِ غير خاضِع لِلتفاوض أو لِتعديلَ بنودِه، يَفرضُه الطرفُ القويّ على الفريقِ الأَضْعف (حالةُ الشركاتُ الصغيرة لدى توقيعها عقد مع شركة غوغل، على سبيل المثال لا الحصر. فالتدقيق مطلوب في ظِلّ غِياب شِبه تامّ لِلقوانين الخاصةِ بالحوسبة السحابيةِ[١٠٣]؛ وفي ظِلّ تنازُع القوانين التي ستُطبّق على أيّ نِزاع أو دعوى قضائيّة (تنازُعٌ إيجابيّ أو سلبيّ). ففي فرنسا، يُطبّقُ القانونُ الفرنسي على هكذا دعاوى فقط في حال كان المسؤولُ عن مُعالجة البيانات مُقيماً في فرنسا، أو في حال تمَّت مُعالجَةُ البيانات على الأرض الفرنسيّة.

مقترحات ومعايير وآفاق	
١. **أمن المعلومات** • كلمة مرور قوية • عدم مشاركة جميع البيانات والملفات والمجلدات • مكافحة البرامج الخبيثة • حفظ نسخ احتياطية باستمرار	٢. **بذل العميل للعناية المطلوبة** لعدم: • اختراق الجهاز الافتراضي • اختراق البرمجيات الخبيثة • الإدارة الأمنية للحوسبة السحابية • تحديات إدارة مراكز البيانات الضخمة
٣. **بنود العقد** • امكانية الوصول الى المعلومات • الإجراءات المتبعة لحفظ البيانات ومعالجتها ونقلها • ملكية العميل لقاعدة البيانات	

- مدة العقد ونهايته
- انعكاسات القوة القاهرة
- ضمان دفع الخدمات المقدمة
- استلامه النسخة الاصلية لدى انتهاء العقد
- اتلاف كل النسخ الاحتياطية

- **<u>أمن البيانات:</u>** تبرُز إشكالياتٌ أخرى، منها ما أدركَه مقدمو الخدمات من أنّه صحيح أنَّ بعض المُستخدمين لا يهتمّون بما يجري في حقيقة خلفياتِ المواقِعِ الإلكترونيةِ، إلّا أنَّ البعضَ منهم (وهم بأغلبيتهم الخبراء المحترفون أو ذوي الحشرية) قد يكون لديهم دوافِع عدة للإطّلاع واستشكاف ما يجري خلفَ المواقِع الإلكترونيةِ، وإذا كانت بعض الشركات والمواقع تجهدُ في تطويرَ خدماتِها تلبيةً لِرغبات زبائنِها ولِلحفاظ عليهم ولِتبيان قُدرتها التنافسيّة بين أقرانها، إلّا أنَّ بعض هُواة التقنياتِ يرغبونَ دائماً في الإطّلاعِ على ما يستجدُّ في عالِمِ الحوسبةِ الإلكترونيةِ ولو بِطريقة غير شرعيةٍ أو غير مباحةٍ (القرصنة الإلكترونية). وتُشير الدراساتُ إلى تفاوتٍ حادٍّ في مدى الإستعدادِ للأخذ بالحوسبةِ السحابيةِ بين البلدانِ المُتقدّمةِ (تعتبر اليابان في المقدمة) والبلدانِ الناميةِ[١٠٤]. أما عن أسباب هذا التفاوت فهي متعددة: هناك العديدَ من الهواجسِ، والمحاذير والمخاوف التي تُرافقُ هذه الخدمَةَ في الدوَلِ العربيةِ، أبرزَها معاييرُ أمنِ المعلوماتِ وضُعفُ البُنى التحتيّةِ، وفِئَة عقودِ الإذعان وتَطبيقاتُ الحوسبةُ في بعضِ هذه الدولِ، وكِلفتُها والتَرتيباتُ والضوابِطُ اللازمَةُ، ومدى التعاونِ مع الهيئاتِ الدوليةِ المُختصّةِ والشركاتِ الضَخْمةِ المُتخصّصةِوإنقطاع الإنترنيتِ، وضُعف خدماتِها، والمخاوفِ البيئيةِ.

في المقابِل، يتوجَّب على المستخدمِ إستخدامَ الخِدمة بِشكلٍ آمِن من خلال إدراج كلمة مرور قويّة لتوثيق الحِساب السحابيّ، وعدم مُشاركة جميع البياناتِ والملفاتِ والمُجلَّداتِ وسائِر الروابطِ مع الآخرين، وتثبيت برنامِج مُكافحةِ البرامجِ الخبيثةِ، والتنبُّه إلى أخذ نسخ إحتياطيةٍ خاصةٍ به بِشكلٍ مُستمر لِكل قواعد بياناته.

من هنا يتوجّبُ على العميلِ التنبُّهَ، إلى تضمينَ العقدِ بنود تغطي النِقاط الرئيسيةِ التالية: إختراقُ الجهاز الإفتراضي كأي جهاز حقيقي ، وإختراقُ البرمجيات بالبرامِجِ الخبيثَةِ والفيروسات، والإدارة الأمنيّة لِطبقاتِ الحوسبةِ السحابيةِ (كمراكز البياناتِ، والشبكةِ، والأجهزة، ونظام التشغيلِ، والبرمجيات الوسيطة، والتطبيقات، المُستخدم...)؛ وتحدياتُ إدارة مراكز البياناتِ الضَخْمةِ ومراكز الخدمات، والمرونة والدقة والإستخدام الأمثل للموارد، وقابلية التوسع بالحجم Scalability، والفاعلية والكفاءة

والإعتمادية Reliabilty (أيّ اطمئنان العميل إلى الخدمة وعدم مفاجئته بإنقطاعها). كما يجدرُ السهرَ على أنْ يتضمّن العقدُ بنوداً توضِّح إمكانية الوصولِ إلى المعلوماتِ والإجراءاتِ المُتّبعةِ لحفظ البياناتِ ومعالجتِها ونقلِها. والأهمّ بند واضح وصريح يُؤكّد مُلكيّةَ العميلِ لِقاعدة البياناتِ، ومُدّة العقدِ، وانعكاسات القوّة القاهِرة، وضَمان دفْع الخدمات المُقدمة، ونِهايته، وتسليمِه النسخة الأصليّة وإتْلاف كُلّ النَسَخ الإحتياطية الأُخرى.

- **<u>واجب الحماية</u>:** أمنياً، تُعاني الشركاتُ وحتى الدول من أجل حِماية معلوماتِها من الاختراقاتِ الأمنيةِ والهَجَماتِ التي أصبحَتْ أكثر تعقيداً وصعوبةً في الاكتشافِ. ممّا يتطلّبُ إرساءَ قواعد تنظيم، لسد الفَجواتِ التأمينيةِ ولتوفير خدماتٍ تأمينيةٍ تقنيةٍ تُناسِبُ حَجمَ هذه القواعِدِ البيانيّةِ، لا بل حِماية لوجيستيّة للأبنية المحليّة التي تحتوي على مراكزَ هذه البياناتِ. كما يفرضُ على المستخدِم أنْ يتأكدَ من سُمعة الشركةِ مُورّدة الخِدمة، ومَقرَّها القانونيّ، وفُروعها المحليّة والأجنبيّة، ووضعِها القانونيّ (أقلّه لعدم تعرّضها للإفلاس)، وموقِع خوادمها حول العالم، أقلّه تلك الموجودةِ في أميركا والمُلزِمة بإتاحة كل بياناتِها إلى السُلطاتِ الأميركيةِ. كما يتوجَّبُ على المُستخدِم أنْ يتأكَّد من توفُّر جودَة الدعمِ الفنيّ، وسُهولة الإستخدامِ والإسترجاعِ، وتوفير مستوى عالٍ من أمن المعلوماتِ، والأهم التأكُّد من قِراءة شُروط الإستخدام المُدْرجة في بنود العقدِ، لا سيما تلك المُذيّلة في هامِش الصفحاتِ لأنَّها هي من تحتوي على استثناءاتٍ أساسيةٍ ودقيقةٍ.

من هنا، يتوجّب على مُزوّدي الخِدمة عبر الحوسبة السحابِية التميُّز بالقُدرةِ العاليَةِ على إحتواءَ البياناتِ واستعادتِها في الحالاتِ التي يحدُث بِها عطْلٌ بالخَوادِمِ. نُشير إلى أنَّ غالبيةَ الشركاتِ مُزوّدة الخِدمةِ تُؤمّنُ حمايةً للبياناتِ من خِلال تشفيرِها وترميزِها، ولا يُمْكِن إزالة التَرميز إلّا باستخدام كلمة السِر الخاص بالمُستخْدم. وهنا تُطْرَح أهميةُ "حِماية البيانات"، والواجِب المُلقى على عاتِقَ العميلِ في التأكُّدِ من جُودة إتصالِه بالإنترنت، وعدم إختراق حِسابه، والتأكُّد من الهُويّة الحقيقيّةِ لِلمستخْدم، وحُسن تخزين البياناتِ، بينما يُرتّب على مُزوّدي الخِدمة توفيرَ أَدوات مُعالجة البياناتِ والأدواتِ البرمجيّةِ لِتطويرَ أي كود برمجيّ لِمساعدة الُمستخدم على عدم تَسرُّب أي بياناتٍ وحُفظ حقوقه وخصوصياته.

<u>٣. بين السيادة الوطنية وأمن الحوسبة السحابية وتحديات الأمن العابر للحدود:</u>

في السِياق عَيْنه، لا بُدّ من الإشارةِ إلى ما تفرضُه الجرائمُ العابِرة للحدود والإرهاب[١٠٥] من أهميّة تعاون الدُول في تبادُل المعلوماتِ والبياناتِ الشخصيّةِ للأشخاص المُشتبَه بِهم[١٠٦] أو المُلاحَقين أو المحكُوم

عليهم في جرائِمَ مُنظّمةٍ عابِرةٍ للحدود الدَولية وجرائِمَ إرهابيّة[١٠٧]. مما يُهدّدُ الأمنُ والسِلمُ الدوليَّين ويفرضُ "الأمنَ العابِرَ للحدود" كأولويةٍ في سياسةَ منعِ الجريمةِ أو الوِقايةِ منها[١٠٨]. من هنا تأتي أهميّة تبادُل المعلوماتِ في التدقيقِ في جوازاتِ السفرِ، والتأشيراتِ، وسِجل المُسافِر، وسائر تفاصيل الرِحلة، وشرِكة الطيران، أو اسم وكالة السفر، وقيمة التذكَرة وكيفيّة الدفع، ووُجهة السفرِ، والإقامة والفُندق[١٠٩]. مما سمحَ بإمكانية، توسيع نِطاق النَفاذِ إلى المعلوماتِ الشخصيّةِ وتقاسمها.

السيادة الوطنية وتحديات الأمن العابر للحدود
• أهمية تبادل المعلومات • السيادة على قاعدة البيانات • المعلومات الحساسة: معلومات أمنية ومالية ومصرفية • القانون الواجب التطبيق • انتهاك سيادة الدولة • حقوق الملكية الفكرية • أمن وخصوصية المعلومات • غياب ضمانات عدم انتهاك الحقوق والقوانين والسيادة

هنا تبرزُ العديدُ من التساؤلاتِ المُتعلّقة بالسيادة الوطنيّة، فقاعدةُ البياناتُ ليست بمستوى واحد من الحِماية فهناك معلوماتٌ حسَّاسةٌ تتعلَّقُ بالأمن الوطنيّ[١١٠]، والأمن الاقتصاديّ (كالسرية المصرفية)، وأبْرزُ هذه التحديّات: السيادَةُ على قاعِدة البيانات، والقانونُ المُزمِع تطبيقه، ومكان تواجُد المعلومات والبيانات[١١١]. مما يُثيرُ المخاوفَ من الإختراقاتِ الأمنيةِ والتجسّسِ الإلكترونيّ وما يُمكن أنْ ينجم عنها من إنتهاكَ لسيادة الدولةِ والعديدِ من الخسائِرِ المعنويّةِ والماديةِ.

ففي غالبية الدولِ يخضعُ مركزُ قاعدةَ البياناتِ لقانون الدولةِ المُضيفَةِ وسيادتها، والسؤال هو في حال صدورِ قرارٍ قضائيّ عن القضاءِ المحليّ فهل ستُطبّقه الشركاتُ مُورّدة الخدماتِ؟ اللافت أنَّ البياناتِ ومتى ما تخزَّنَت وتمَّتْ مُعالجتَها فإنها تتحوّل من مُجرّد بياناتٍ إلى قاعِدة مُعطياتِ وقاعدة معلوماتٍ ذات قِيمة ماليةٍ وتجاريةٍ. في السِياق عينه، نُشيرُ إلى أنّ تخزينَ بياناتِ المُستخدم لدى مزوّد الخِدمة يُثير المخاوفَ من الوصولِ إليها، وإختراقها من قِبل أطرافٍ أو جِهاتٍ مُعيّنة، ومن عدم حِمايةِ حُقوقِ المُلكيّة الفِكريّة، وأمن وخُصوصيّة المعلوماتِ، ومن إحتماليّة إطّلاعِ الغير على معلوماتِهم وبياناتِهم، ووِسط غِياب ضماناتِ عدَم إنتهاكِ هذه الحقوقِ.

- **<u>إدارة البيانات الضخمة</u>:** يُمكن إضافةُ العديدَ من الإشكالياتِ الأُخرى المُمكِن إثارتها في هذا السياقِ، لا سيما لناحية تِقنياتِ التشفيرِ في السحاب وآلياتِ التشفيرِ وحدود ونقاط ضُعْف هذه التقنياتِ وتعدّد المُستخدمين وإمكانية فُقدان التحكُّمِ في البياناتِ. ويُثار التساؤلُ حول الجِهة المُختصةِ في تقييم أخطاءِ تطبيقاتِ الحوسبةِ السحابيةِ، لا سيما قاعِدة البياناتِ الضخمة، التي تضخّمت وتعقّدَت

لِدرجةٍ بات من الصعبِ معالجتُها باستخدام تطبيقاتِ معالجة البياناتِ المحليةِ أو البياناتِ التقليديةِ المُعتمدة على قاعِدة بياناتٍ واحدةٍ. نذكرُ على سبيلِ المِثال لا الحصر، أنَّ هذه الشركاتِ الضخمةِ تستحوِذُ على كَنْز مَهولٍ من البياناتِ الخاصةِ والذِكرياتِ الشخصيةِ، على غِرار برنامج غوغل فوتوز، حيث تتِمُّ مُعالجةُ هذه البياناتِ بِواسطته فقط ويُخزّن الآفَ الأطنانِ من الصوَرِ على نِظامَ الحوسبةِ السحابيةِ.

إدارة البيانات الضخمة	
• قاعدة بيانات شخصية ضخمة وذكريات شخصية • تقنيات التشفير في السحاب • حدود ونقاط ضعف التقنيات السحابية • تعدد المستخدمين	• فقدان التحكم في البيانات • توعية الزبائن • تقييم المخاطر ونظم التحقيق وضبط الاجراءات • الاستجابة الى الحوادث الأمنية والطوارئ التقنية

وكما ذكرَتْ "مؤسسةُ العلومِ الوطنيةِ الأميركية" أنَّ انتشارَ الحوسبة السحابية في البيئاتِ الطبيعيةِ والإجتماعيةِ تنتجُ عنه بياناتٌ غير متجانسة لم يسبُقْ لها مثيل من حيث حجمِها ومدى تعقُّيدها. فيبرزُ التحدّي في تنبُّه العميلِ إلى كيفية إدارةِ هذه البياناتِ، ومُعالجتها، وموثوقيّةِ المعلوماتِ المُخزّنة، وتقييم المخاطرِ، ونُظُم التحقيقِ وضَبط الإجراءاتِ، والإستجابة إلى الحوادثِ الأمنيةِ والطوارئ التقنيةِ.

- **<u>حماية المستهلك:</u>** من ضِمن المشاكِل التي تطرأُ على هذا الصعيدِ مشكلات ماهية حقوق المستخدمين والمُتعاملين في بيئةِ الإنترنتِ، وبالتحديدِ "حماية المستهلك" في الفضاءِ السيبرانيّ، أكان فرداً أم مؤسسةً، لا سيما في ظلِّ شِبه غِياب للقوانين العربيةِ المُلائمةِ، ولِطبيعة عقودِ الإذعانِ، وللإعلاناتِ الخادعةِ[١١٢]، وللفارق بين المُستهلِكِ المحترف أو عديم الخِبرة في التِجارةِ الإلكترونيةِ أو سائر المُعاملاتِ الإلكترونيةِ[١١٣]. من هنا يترتَّب على العالِمِ الحقوقّي في العالمِ مُراعاةَ المُتطلباتِ القانونيةِ والإداريةِ الحديثةِ الخاصةِ بِخِدمة الحوسبةِ، لا سيما تحت وطأةِ تهديداتٍ قانونيةٍ بِسبب طبيعةِ خدماتِ الحوسبةِ السحابيةِ مُقارنةً مع الخدماتِ التقليديّةِ.

حماية المستهلك
• حقوق المستخدمين • طبيعة عقود الاذعان • الاعلانات الخادعة • مراعاة المتطلبات القانونية والادارية والتقنية الحديثة • تجارة البيانات الشخصية

ووفقاً لتقرير يُصدره الإتحاد الدولي للإتصالاتِ، بعنوان "إتجاهات الإصلاح في الإتصالات لعام ٢٠١٣"، يزداد التحدّي الذي يواجهُ صانعي السياساتِ في المُوازنةِ بين الحاجةِ التجاريةِ ورغبَةِ الأفرادِ في حريّة تدفُق المعلوماتِ مع توافر المعرفَةِ عن عِلْم والتحكُّم الفعّال من جانب الأفرادِ في معلوماتِهم الشخصيةِ[١١٤].

فقد غدت للبيانات الشخصية قيمة اقتصادية بحيث انتشرت مؤخراً ظاهرة "تجارة البيانات الشخصية" وانتهاكها من قبل شركات دعائية متخصصة في هذا المجال[١١٥]، باستغلال بيانات المستهلك أو الموظف أو العميل والوصول إلى لوائح الاصدقاء من أفراد العائلة والأصدقاء والزملاء والصور والأحداث ، وحركة البيانات ، والعناوين الرقمية IP، وسجلات البرامج المعلوماتية ، ومعلومات تحديد الموقع الجغرافي GPS، والتسجيلات الرقمية وغيرها، كل ذلك بهدف معالجتها وعرضها لاحقا وعبر مواقع الكترونية متخصصة لأغراض ترويجية كالتسويق الالكتروني وتجارية كالتجارة الإلكترونية من دون الحصول على موافقتهم[١١٦]. إن أهمية هذه البيانات بالنسبة للجهات المقدمة للخدمات تكمن باعتبارها مُلكية أساسية تدعم نماذج الاعمال الخاصة بها[١١٧] وتساعد على اتخاذ القرار وتعزز قدرتها على الابتكار وتحقيق التنافس وزيادة الانتاجية، وتعد هذه المعلومات الشخصية، من ضمن حقوق هذه الشركات المنقولة، وأحد أصولها، في حال بيعها كلياً او جزئياً.

٤. التنسيق الإقليمي والتعاون بين الدول في المنطقة العربية:

على الصعيد الدستوري، لا يوجد أي دستور عربي ينص على الحق في الوصول للمعلومات، أو ينظّم أي من مظاهر حماية خصوصية المعلومات، فلا يوجد في أي من الدساتير العربية ذكر للبيانات الشخصية أو مسائل المعالجة الالكترونية، أو تقييد إجراءت جمع البيانات وتخزينيها واستخدامها من قبل السلطات العامة.

التدابير الواجب اتخاذها بين الدول العربية
• تعاون عربي قانون وقضائي وأمني • تعاون عربي مؤسساتي واداري • رفعِ مستوى شفافيةِ سلوك الشركاتِ والتقاريرِ الماليةِ، • ضرورةُ إجراءُ التحقيقاتِ والمُقاضاةِ، • تعزيزُ مساءلةُ المسؤولين في الشركات ومحاسبتهم، • المُشاركةُ بين أجهزة إنفاذِ القانونِ والقِطاع الخاصِ. • المساهمة في سنّ قانون دولي يطبّق على الأفعالِ غير المشروعةِ التي تَرتكبُها الشركاتُ المتعددة الجنسية.

على الصعيد التشريعي، لا يوجد لغاية اليوم قانون دولي أو عربي يُجرّمُ ويُعاقبُ أعمالَ الشركاتِ المُتعدّدةِ الجِنسيةِ، بل فقط قوانين محليةٍ وقواعد سلوكيةٍ ذات قيمة معنوية وأدبيّة غير ملزمة. لذلك لا بدّ من أخذ الخُطواتِ التاليةِ: ضرورةُ التعاونُ العربيّ القانونيّ، مواصلةُ فرضُ تطبيقِ القوانينِ بحزمٍ بغيةَ رفعِ مستوى شفافيةِ سلوك الشركاتِ والتقاريرِ الماليةِ، ضرورةُ إجراءُ التحقيقاتِ والمُقاضاةِ، تعزيزُ مساءلةُ المسؤولين في الشركات ومحاسبتهم، المُشاركةُ بين أجهزة إنفاذِ القانونِ والقِطاع الخاصِ. والأهمّ من ذلك،

يُفترضُ سنّ قانون دولي، أي معاهدات دولية، لتطبّق على الأفعالِ غير المشروعةِ التي تَرتكبُها هذه الشركاتُ.

على الصعيدِ القضائيّ، مما لا شكَّ به أنَّ المحاكمَ العربيةَ المحليّةَ باتَت تُدرك في الوقتِ الراهِن أهميةَ خدماتِ إدارةِ حمايةِ البياناتِ والأخذَ بالدليلِ الرقمي، على الرُغم مما تواجهه من تحدياتٍ قانونيةٍ تتعلّق بمدى صُدقيّة الإثباتِ الإلكترونيّ ومدى صِحته. الأمر الذي يُرتّب على العميل أهميةَ الوعي لمدى ترتّب المسؤوليةِ على موفّرِ الخِدمة في حال التقاضي أو التحكيمِ أو الوساطَةِ. ومما لا شكَّ فيه أنّ القضاءَ المحليّ سيُواجه مسائلَ تقليديةً ذات إثبات إلكترونيّ، وذلك في حال الإدّعاءِ في حالاتِ تسرُّب اليباناتِ من أنظمتِها، فيختلفُ عندها الأمرُ إذا كان هناك من رابِطة عقديّةٍ أم لا، وهل يمكن للجاهِل أنْ يستفيدَ من التذُّرعِ بِجهله للقوانين أو عدم إعتماد معايير الحِمايةِ الضروريةِ أو عدم الإلتزامِ بهذه المعاييرِ، خَرقاً لحِمايةِ المُستهلِكِ ومُستخدم الشبكةِ، إلى ما هنالك من الشروطِ الواجبِ توفّرها لتحقّق شروطِ الضررِ كأساس للمُطالبة بالتعويضِ عن العطلِ والضررِ.

٥.عقد "اتفاق عربي للملاذ الآمن" Arab Safe Harbor

بما أنّ الدول العربية تفتقر إلى التعاون الفعال في مجال الأمن السيبراني وخدمات الحوسبة السحابية، لذلك تقترح الدراسة أهمية عقد اتفاق عربي للملاذ الآمن، يتضمن النقاط التالية:

- وضعُ معاييرُ مُشتركةٌ وتحديدُ مُتطلّبات تدفُّق المعلوماتِ عبر الحدودِ مع توافُر الحِمايةِ المُناسبةِ للأمنِ والخصوصيةِ.
- تحقيقُ تقدُّم تنظيميّ للتعامُل مع حِماية البياناتِ والإهتماماتِ الخاصةِ بالأمنِ؛
- التأكُّد مِن أنَّ الدولَ العربيةَ تُدرِكُ أفضلَ المُمارساتِ التنظيميّةِ؛
- التحضيرُ الدقيقُ لعقود التعاقُد الخارجيّ في الحوسبةِ السحابيةِ، بما في ذلك تضمِينها فقرات قويّة في شأن أمنِ البياناتِ لا سيما بياناتِ الأمنِ القوميّ؛
- التأكُّد من أنَّ عقودَ الحوسبة السحابية تتضمّن الإشتراطاتِ التنظيميةَ؛ وتضمينها بنوداً صارمةً في شأن أمن البياناتِ ومعالجتها وحمايتها.
- إنشاءُ مراكز البياناتِ في الدولِ العربيةِ وفي كُلّ دولةٍ منفردةٍ، لتقليل تكاليف عرض النِطاقِ وزيادة سرعة النفاذ؛
- التأكُّد من أنَّ مراكزَ البياناتِ سليمةٌ من الناحيةِ الإيكولوجيةِ؛
- إنشاءُ هيئةٌ رسميةٌ عربية لِلسهر على حُسن تطبيقِ أحكام هذا الإتفاق؛

- إدراجُ بندٌ تحكيميّ لِفضّ النزاعاتِ والخِلافاتِ عِبر وسائل التحكيمِ أو الوساطةِ أو اللجوءِ إلى المحاكِمِ المحليةِ؛
- إدراجُ "بندٌ جزائيّ" لتطبيقه في حال إخلالِ أحد الطرفَين بِبنود الاتفاقِ، لا سيما فيما يتعلّق بنقل البياناتِ إلى الخارِجِ من دون موافقةِ العميلِ أو عدم إستردادها أو إسترداد النسخةِ غير الأصلية؛
- ضمانُ التقيّيسُ والتنظيمُ عبر الحدودِ عن طريق المشاركةِ في مُبادراتِ تقييسِ الحوسبةِ السحابيةِ؛
- الإلتزامُ بعدد من المبادِئ، أبرزُها مبدأُ سيادةُ الدولِ والمساواةُ فيما بينها وحقُّها في الإستفادةِ مما تقدمه الحوسبةِ السحابيةِ وضمانُ القُدرةِ التنافسيّةِ لشركاتِها؛
- إنشاءُ هيئاتُ تحكيمٍ وطنيةٍ مُتخصّصة في الحوسبةِ السحابيةِ وخدماتٍ إستشاريّة وِقائية وعِلاجية.

اقتراح "ملاذ عربي آمن"	
• وضع معايير مُشتركةٌ • تحديد متطلبات تدفق المعلومات عبر الحدود مع توافُر الحِماية المُناسبةِ للأمن والخصوصية. • حِماية البياناتِ والإهتماماتِ الخاصةِ بالأمن؛ • إدراك أفضل المُمارسات التنظيميّة؛ • التحضير الدقيق لعقود التعاقُ الخارجيّ في الحوسبة السحابيةِ؛ • أمن البيانات ومعالجتها وحمايتها.	• إنشاءُ مراكز البيانات في الدولِ العربيةِ؛ • سلامة مراكز البيانات من الناحيةِ الإيكولوجيةِ؛ • إنشاءُ هيئة رسمية عربية؛ وهيئاتُ تحكيمٍ وطنية مُتخصّصة • إدراجُ بند تحكيميّ لِفض النزاعات والخِلافات؛ • إدراج "بندٌ جزائيّ"؛ • ضمانُ التقيّيسُ والتنظيمُ عبر الحدودِ؛ • الإلتزامُ بمبدأُ سيادةُ الدولِ.

خاتمة ومقترحات:

في الخِتام، يُمكن القول أنَّ الحوسبةَ السحابيةَ هي المرحلةُ المقبلةُ من التكنولوجيا أو الخطوةُ التاليةُ في تَطوُّر الإنترنت، وهي ليست تقنياتٍ جديدةً بقدر ما هي خدمات جديدة، وأنَّ أنظمتِها كغيرها من مفرزاتِ التكنولوجيةِ الحديثةِ تتضمّن شِقّين من المُفرزاتِ: الفوائِدُ والتحدياتُ، فهي تُقدّم إمكاناتٍ عديدةً على غِرار تسهيلِ المُشاركةِ، وزِيادة الإيراداتِ، وتوسيع الأعمال، وخلقِ فُرَص عملٍ جديدةٍ؛ كما تخلق تحديات تتعلق بالتعاقد، وضمان الأمن، وحماية خصوصية البيانات، والسيادة الوطنية، والإطار التشريعي والتنظيمي.

تبيّن لنا أنّ العصرَ الحديثَ يعتمدُ على تجسيد "المُجتمع الشبكيّ" والبياناتِ الضخمةِ والهواتِف المحمولَةِ ووسائلَ التواصُلِ الإجتماعيّ وتخزين الملفاتِ الضخمةِ، مما يُؤرقُ الدولُ والخبراءُ والمُنظمات والمُختصّين؛ لأنه يزيد من حوادثَ الأمنِ السحابي، ويُعزّز مشاكلَ التطبيقاتِ الشبكيةِ والتقليديّةِ وحُفظ البياناتِ، لا سيما فُقدان البياناتِ أو سرقتها ونقلها إلى الخارِجِ، وسِيادة الدولةِ على مُلكية البياناتِ، وقضايا

الإحتيالِ والتشفيرِ والقرصَنةِ، والإختراقاتِ الأمنيةِ، وحِماية العُملاءِ والمُستخدمين. وقد أطلقَتْ العديدُ من الدولِ العربيةِ مشاريعَ إستراتيجياتٍ لاعتماد تقنياتِ الحوسبةِ السحابيةِ إنما وِسط غِياب لبيئة تشريعيةٍ تُحدّد الإطارَ التشريعيّ أو التنظيميّ أو التنفيذيّ، أو إعتماد أي إستراتيجيّة وطنيّة قانونيّة أو تعاقديّة أو أمنيّة على هذا الصعيدِ، إضافةً إلى غِياب التعاونِ سواء على المستوى الداخلي أو على المستوى الخارجي. كما برزَ قِطاعُ الاتصالاتِ بِشكلٍ خاص كِقطاع أُفقّي يتقاطَعُ مع جميع القِطاعاتِ الأساسيةِ في الدولةِ وضِمن منظومة تقنيةٍ حديثةٍ لا يجدي نفعاً التعامُل معها بالوسائلِ التقليديةِ.

ونُشيرُ بشكلٍ عام إلى أنّ العديدَ من الدولِ العربيةِ لم تُرسي بيئة تشريعيّة وتنظيميّة أو تنفيذيّة للمعاملات الإلكترونية أو لحماية البيانات أو معالجتها أو نقلها إلى الخارج، أو لمكافحة الجرائِم الإلكترونية بِشكل كامِل. والقليلُ مِنها أنشأَ مراكزَ اتصال أو مراكز طوارئ، فكيف بالإطارِ التشريعيّ للحوسبةِ السحابيةِ ومدى فاعلية البيئَةِ العربيةِ وإنسجامها مع البيئةِ الرقميةِ؟ ربما لا تزال عِبارة "الحوسبة السحابية" بِحدّ عينها جديدة على مَسمع العديدِ. كما أنَّ غموضَ مُصطلح الحوسبةِ السحابيةِ، نظراً إلى ما تحتويه من تِقنيات جارية وأُخرى مُستجدة يُعيق توحيد تعريفِها، وهي النُقطَة الأساس لأيّ إطارٍ تشريعيّ.

كما استنتجنا أنَّ تردُّد بعض الدولِ العربية والشركات المحلية لاستخدام تطبيقات الحوسبة السحابية يُعزى إلى خوف البعض من انقطاع الخدْمة من جِهة، والأمان بكُل أشكاله المعلوماتية والقانونية من جِهة أخرى. وتحتاجُ هذه الشركاتُ لِبنيّة تحتيّةٍ متوافِرة دائماً وبدون إنقطاع الإنترنت، وإلى خبرات إنسانية تقنية ومُتخصّصة، وإحترافية عالية في مجال تكنولوجيا المعلومات ضِمن الشركة نفسها، وبهدف الحماية الأمنية واللوجيستية لِمراكز البيانات التي تحتوي خدمات الحوسبة الحسابية من الإختراق والعبث في مُحتويات البيانات فيها.

نرجو أن تبادر الدولِ العربيةِ إلى إنشاءَ خدماتٍ خاصةٍ بها IAAS، فلهذِه الدُول الحقّ بالإحتفاظِ ببياناتِها ومعلوماتِها، حيث أن توفير هذه الخدمات محلياً يُوفّر أماناً أكبر، وخِدمة دعم أفضَل، وتواصُل أكثر مُرونة مع العُملاء والشركات، سواء أكانت البيانات للأفراد أو للقطاع الخاص أم لدوائرَها الرسميّة ومؤسساتِها الحكومية، لأنَّ هناك خطورة في تعرُّضها يوماً ما لِتهديد حقيقيّ يَمُسُّ الأمنَ القوميّ لهذا البلد العربي أو ذاك.

ناهيك عن أن استثمارّ الدولِ العربيةِ في تفعيل خدمات الحوسبة السحابية من شأنِه أنْ يوفرَ فرصَ عملٍ هائلةٍ لِلشباب العربيّ. ولا خَوْف من تبنّي هذه الخدماتِ فحتى الحواسيب الشخصيّة تحتوي ثغراتٍ أمنيةً.

ومن المعلومِ أنَّ هناك درجاتٍ مختلفةً من حساسية المعلوماتِ؛ فمثلاً المَعلومات المُرتبطة بالأمنِ القوميّ لا يمكنها أن تكون خارجَ سِيادةِ الدولةِ أو مبنى الوِزارةِ المعنيةِ، وهي تحتاجُ إلى سحابة خاصةٍ

مُؤمّنة بموظفيّين حكوميّين، لكن هذا لا يمنع أنَّ هناك معلوماتٍ وبياناتٍ وتطبيقاتٍ يمكن أنْ تكون على سحابة عامةٍ. وتبيّن لنا أنْ أحد أهمّ التحديّات الموضوعيّة والإجرائيّة لِضبط الحوسبةِ السحابيةِ هو عدم وجودِ تشريعٍ خاص مُلزِم عالمياً (أي إتفاقية دولية) يُغطّي جميعَ بلدانِ العالمِ، لكن أكثريةَ الدولِ إعتمدَت حمايةَ الخصوصيةِ والبياناتِ، وكثير منها يُنظِّم التدفُّق الدوليّ للبياناتِ كآليةٍ لِحماية خصوصيةِ الأفرادِ وإنفاذ السياساتِ الوطنيّة.

من هنا تأتي مُقترحات هذه الدراسةِ، مُقسّمةً على الصعيدين المحلي والإقليمي:

<u>أولاً: على الصعيد المحلي:</u>

- **<u>مقترحات تشريعية</u>:**

- أهمية استعراض القوانين المرعية الاجراء لمعرفة مدى امكانياتها في تيسير الاستخدام الوطني والدولي لخدمات الحوسبة السحابية.
- مشاركة واضعي السياسات العامة في الدول في وضع سياسات محلية تبرز أهمية الحوسبة ومواكبة التطور التقني بما يتلاءم مع الأولويات الوطنية.
- استحداث أو تطوير البيئة التشريعية والقواعد التنظيمية والقوانين المناسبة والمراسيم التنفيذية والقرارات التطبيقية.
- سن القوانين الخاصة بفرض ضرائب حديثة وإدخال ترددات الجيل الرابع 4G في كل المناطق.

- **<u>مقترحات تتنفيذية</u>:**

- تطوير البيئة الإدارية نظرا لارتباط أي تقدم محلي بتخصص الأجهزة المعنية وقدرتها على وضع القوانين قيد التنفيذ وضبط الآليات والأمور.
- مساهمة الدولة في تمكينُ الشركاتِ المحليةِ من خلق بيئةِ تقنياتٍ تُمكِّنها من المنافسة على الصعيدِ الإقليميّ والعالميّ (كإعفاءها من بعض التزامات المالية والضرائبية).
- الإفادةُ من أفضل الممارساتِ والتجارِبِ الناجِحةِ على الصعيدِ الدولي، وإعتماد المقاييس والمعايير الدولية التي تُعزّزُ الثقةَ في الحوسبةِ السحابيةِ وتؤمّن بيئةً داعِمةً للإنخراطَ في الإقتصادِ الرقميّ بكل مشاربه.
- أهميةُ إستفادةُ الدولِ العربيةِ من خدماتِ الحوسبةِ السحابيةِ مع الأخذِ بعين الإعتبارِ النِقاط التالية:

✓ حِمايةُ البيانات: للعميل الحقّ بِحفظ معلوماتِه وعدم تسرُّبها مُقابل واجباته في التأكُّدِ من إتصالِه بالإنترنت، وحفظ هذه المعلوماتِ بِشكلٍ آمنٍ وسليمٍ وصحيح؛ وضمان حقّه بالإستناد إلى وسائلّ حمايةٍ قانونيةٍ في بلده ومعايير دوليّة تضعُها الجهاتُ المختصّةُ.

- ✓ نِظام إدراةُ الهُويّة: التأكُد من صِحّة هُوية العميلِ ومُلكيّته، لِحسابه وعدم تعرُّضه للقرصَنةِ، فواجبُ موفّر الخِدمة تأمين نِظام معلوماتيّ آمِن يصعُبُ خرقُه.
- ✓ الأمنُ المادّي: للشبكة وللتطبيقات وللخوادم وعدم توفُّر أي ثغرة أمنية خاصة بها.
- ✓ أمنُ التطبيقات: من خِلال توفير أدوات مُعالجة البياناتِ والأدوات البرمجية بكفاءة عالية.
- ✓ حِمايةُالخصوصيةُ والبياناتُ الشخصيةُ، وذلك لإتقان الحمايةِ الذاتيةِ والتنظيم الذاتيّ ولضمان إلِمام المستهلكين بالقيمَةِ الحقيقيةِ لمعلوماتهم الشخصيةِ ومعرفة قيامِ الدعاوى المختصة.
- ✓ إنتباهُ المستخِدم إلى تخزين المعلوماتِ المُهمّة والسياديّةِ والسرية على وسائطَ تخزينٍ محليةٍ وليس عالمية.

- **<u>مقترحات توعوية وبناء قدرات:</u>**

- أهميةُ إصدارُ دليلٍ للتعرّف على بعض أسس الحوسبةِ السحابيةِ، وتحديد مدى وكيفية الإستفادة منها وما يجوز أو لا يجوز تخزينه على السحاباتِ، والأهم التأكُّد من أنّ مزودَ الحوسبةِ السحابيةِ معترفٌ به دولياً.
- إنشاءُ الهيئةُ الوطنيّة المُختصّة للحوسبة السحابيةِ في كُلّ بلد عربيّ وإنشاء مراكز إتصال بينهم.
- بناءُ قدراتٌ وطنيةٌ وعربيةٌ مُتمكّنة، وتدريبُ أجهزة إنفاذ القانونِ، والنهوض بالخبرات لمُواكبة أحدث التطوّرات التقنيةِ والإجتماعيةِ في الحوسبةِ السحابيةِ، ولتحديث نماذج العمل للتعامل مع مسائلَ الحوسبةِ السحابيةِ والخدمات التي تقدّمها، وهي شركات متعددة الجنسية غريبة عن المؤسساتِ والإداراتِ الحكومية.
- أهميّةُ نشرُ قواعد أخلاقية ومناقبية وسلوكية.
- أهميةُ الأبحاثُ المتخصّصةُ بالإطار التشريعيّ للحوسبةِ السحابيةِ، والندوات وورش عمل تكوينية وبرامج تدريبية.
- أهمية إدراكُ المؤسسات التربويّة لا سيما التعليم العالي لضرورة إرساء آلياتِ تشجيعِ الأبحاثِ ومتابعة مستجدّات الحوسبةِ السحابيةِ، والأنظمة الذكيّة، وهندسَة البرمجياتِ والإتصالاتِ والشبكاتِ، وإدرة البياناتِ ومُعالجتها ونقلها، ونظم المعلومات.

<u>ثانياً: على الصعيد الإقليمي:</u>

وبما أنّ تقنياتِ الحوسبةِ السحابيةِ في تطوُّر مُستمر ووِسط تخزينِ البياناتِ الهائلةِ العابرة للحدود، الأمر الذي يتطلّب من الدولِ العربيةِ مواكبةَ التغييراتِ التي تستجدّ وتضافُر الجهود فيما بينها للمبادرة بالخطوات التالية:

- إتفاقٌ عربي للملاذ الآمن (أعلاه مذكورة مقترحات بنوده).
- أهميةُ تعاون الدول العربية على الصعيدَين الإقليمي والدولي مع الهيئاتِ الدوليةِ المُختصةِ.
- وضعُ نماذجُ "عقود التعاقد بين العميلِ ومزوّد الخدماتِ" خالية من بنود الغُبْنِ والبنودِ الأسديّة.
- مُشاركةُ كل الأطراف المعنية في إرساء بُنيةٍ تشريعيّة عربيّة وتنظيميّة للحوسبةِ السحابيةِ من واضعي السياساتِ في الدولِ، والمُنظماتِ الدوليةِ والإقليميةِ الفاعِلةِ والمختصةِ، والهيئات المعنية بالتنسيق، والخبراء والمراكز البحثيّة، وممثلي الشركات العالمية.
- وضعُ إرشاداتٌ تحتوي على أُطُر متناغمة لِلمنطقة العربيةِ.
- تبادل الخبرات العربية والغربية.

ختاماً، نتبنّى مقولة "الإتحاد الدولي للإتصالات":

"Indeed, Cybersecurityis a process, not a destination.No country starts from zero, and no country has completed the process"

ITU

* *

[1] Le Cloud Computing: un défi pour la loi informatique et libertés? – http://www.zdnet.fr/actualites/saas-et-legislation-europeenne-ce-qu-il-faut-savoir-39794305.htm

[2]MATTATIA (Fabrice): Cloud computing - Traitement des données personnelles - Le guide juridique – La loi Informatique et libertés et la CNIL – Jurisprudences – Editions EUROLLES – 2013 – P: 19

[٣]يشير تقرير شركة "سيسكو"CISCO الأميركية المتخصصة في مجال المعدات الشبكية،إلى ان هذه المنطقة ستشهد نموا سنويا في حركة استخدام الحوسبة السحابية يصل إلى ٧٩%.

[4] LESSIG (Lawrence): The law of the horse: What cyberlaw might teach? – in: CyberLaw – – Volume I – The international library of essays in law & Legal theory – Second series – ASHGATE DARTMOUTH – Australia. - P: 250

[5]LE METAYER (Daniel): Les technologies de l'information au service des droits: opportunités, défis, limites – 2010 – Cahiers du Centre d Recherches Informatique et Droit - Bruylant - P: 47

[6] FITZGERALD (Brian): Cyber-Law – Volume I – The international library of essays in law & Legal theory – Second series – ASHGATE DARTMOUTH – Australia - P: XVII

[7] GOLA (Romain): Bases de données et logiciels nécessaires au fonctionnement du site web – in: Droit du commerce électronique – Guide pratique du e-commerce - Gualino - Lextenso Editions – 2013 - P: 181 et suiv.

[8] BENSOUSSAN (Alain): Informatics, Télécoms, Internet: Réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques – 5e édition – 2012 – Editions Francis LEFEBEVRE - Définition du cloud computing - P: 352

[٩]الأهمية الاقتصادية للحوسبة السحابية – البيانات الشخصية لها قيمة تجارية ضخمة، إلى حد الإشارة إليها على أنها موردنفطجديد.–

https://itunews.itu.int/ar/Note.aspx?Note=3727 -No. 1 – 2013

[10]فقد توقعت شركة "ديلويت" الإستشارية Consulting Deloitte ، أنّ الحوسبة الحسابية قد تشهد نموا من ٤٠,٧ مليار دولار أميركي عام ٢٠١١ الى ٢٤١ مليار دولار أميركي عام ٢٠٢٠. كما توقعت دراسة أصدرتها جمعية صناعة تقنيات الكمبيوتر "كومبتيا"CompTIA، ان أكثر من ٨٠% من الشركات حول العالم تستخدم حلول الحوسبة السحابية Cloud Solutions.

[11]الأهمية الاقتصادية للحوسبة السحابية– مرجع سابق – https://itunews.itu.int/ar/Note.aspx?Note=3727

[12]سيما دراسات "مركز دراسات النزاعات" و "مركز الدراسات السياسية الأوروبية".

[13]BENBOUSSAN:Traitement fiscal - Chapitre I: Logiciels – in: op.cit. - P: 690 et suiv.

[14] CAPRIOLI (Eric): La sécurité des services de confiance in: Signature électronique et dématérialisation - 2014 - LexisNexis – P: 248

[15]وفقاً لدراسة استقصائية أجرتها مؤسسة أبحاث Special Eurobarometer لمواقف الأفراد في ٢٠١١، كانت نسبة ٧٤ في المائة ممن شملتهم الدراسة يرون أن إفشاء المعلومات على الخط يمثل جزءاً متزايداً من حياتهم اليومية. وأعربت الغالبية عن مخاوف بشأن تسجيل سلوكهم عن طريق الهواتف المتنقلة، وبطاقات الدفع والإنترنت المتنقلة، ولكن نسبة ٥٨ في المائة رأت أنه لا يوجد بديل لإفشاء المعلومات الشخصية إذا كانوا يريدون الحصول على منتجات وخدمـــات.
https://itunews.itu.int/Ar/Note.aspx?Note=3726

[16]دراسة قدمت الى الإسكوا في أغسطس ٢٠١٥

[17]http://www.moict.gov.jo/documents/%D9%88%D8%AB%D9%8A%D9%82%D8%A9%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9%20%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9%20%D9%84%D9%84%D8%AD%D9%83%D9%88%D9%85%D8%A9%202003.pdf

[18]
قانون امارة دبي الخاص بالمعاملات والتجارة الالكترونية - قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية – دبي – ١٢ فبراير ٢٠٠٢
http://www.sca.gov.ae/arabic/legalaffairs/LegalLaws/Electronic_Trading_Transaction.pdf

[19] قانون اتحادي رقم (١) لسنة ٢٠٠٦ م في شأن المعاملات والتجارة الإلكترونية – أبو ظبي – ٣ يناير ٢٠٠٦
http://www.dubaided.ae/Arabic/DataCenter/BusinessRegulations/pages/federallaw1of2006.aspx

[20] قانون مكافحة جرائم تقنية المعلومات (٢ / ٢٠٠٦) - دولة الامارات العربية المتحدة
http://www.f-law.net/law/threads/43935-قانون-مكافحة-جرائم-تقنية-المعلومات-(-٢٠٠٦-٢-)-دولة-الامارات-العربية-المتحدة

[21] مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات – أبو ظبي - ١٣ أغسطس ٢٠١٢
http://www.wipo.int/wipolex/ar/details.jsp?id=13909

[22]الأسكوا: الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية E/ESCWA/TDD/2015/1– ٢٠١٥ - ص: ٣٣

[23]www.aecert.ae

[24]قانون حماية البيانات الشخصية – رقم ١ – ٢٠٠٧ – خاص بالمركز المالي الدولي لدبي DIFC
http://dp.difc.ae/legislation/dp_protection/
قانون حماية البيانات الشخصية – رقم ٢٠٠٦/١١ – **المادة ٨** - الامارات العربية المتحدة.

[25] European Parliament and Council Directive – 95/46/EC of 24 October 1995 – on the protection of individuals with regard to the processing of personal data and on the free movement of such data – Official Journal – L 281 – 23.11. 1995

[26]http://www.emaratalyoum.com/local-section/other/2015-10-17-1.831307

[27] http://bibliotdroit.blogspot.com/2016/03/blog-post_185.html

[28] http://www.wam.ae/ar/news/emirates/1395239228828.html

[29] http://www.mcit.gov.sa/Ar/InformationTechnology/Pages/IntentionalNews/Tech-News-Inte-21081435_590.aspx

[30]www.cert.gov.sa

[31]http://www.cert.sd/ar/index7bd7.html

[32] Sudan e-Governement - http://www.sudan.sd/policy.aspx

[33]http://www.moj.gov.iq/uploaded/4274.pdf

[34]https://www.cait.gov.kw/National-Projects/Kuwait-Information-Network.aspx

[35] https://www.cait.gov.kw/

[36]http://www.gcc-legal.org/LawAsPDF.aspx?country=1&LawID=4100

[37]يتعلق الأمر بالقانون رقم ٠٩,٠٨ الصادر بتنفيذه الظهير رقم ١,٠٩,١٥ بتاريخ ١٨ فبراير ٢٠٠٩، والمنشور بالجريدة الرسمية رقم ٥٧١١ بتاريخ ٢٣ فبراير ٢٠٠٩.

[38]http://www.justice-lawhome.com/vb/archive/index.php?t-9166.html

[39]www.tuncert.ansi.tn
[40] http://www.anrtic.km/
[٤١]إطلاق شبكة WiMax في إطار مشروع "قرية الألفية" في ١٩ ديسمبر ٢٠١٣، - فرصة لتعزيز النفاذ إلى الخدمات الأساسية في الصحة والتعليم– ٢٠١٤ https://itunews.itu.int/Ar/Note.aspx?Note=5057

[٤٢]تمت مراجعته من قبلنا نحن شخصياً، عبر الإسكوا في أغسطس ٢٠١٥

[43]www.cert.gov.om
[44]www.nans.gov.sy
[45]www.sytra.gov.sy
[٤٦]استراتيجية الحكومة الإلكترونية في سوريا http://www.moct.gov.sy/moct/?q=ar/node/61
[٤٧]السياة الوطنية لأمن المعلومات في سوريا http://nans.gov.sy/images/stories/doc/isc_doc/finalpolicy.pdf
[48]http:// www.moct.gov.sy/ICTSandards/ar_pdf/2.pdf
[٤٩] قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية ٢٠١٤/١٤ - http://www.almeezan.qa/LawPage.aspx?id=6366&language=ar

[٥٠]قانون رقم (٧) لسنة ٢٠٠٥ بإصدار قانون مركز قطر للمال ٧ / ٢٠٠٥ - http://www.almeezan.qa/mojportal/LawView.aspx?opt&LawID=3987&language=ar
[٥١]لوائح حماية البيانات الخاصة بمركز قطر للمال - الإصدار رقم ١ http://www.complinet.com/net_file_store/new_rulebooks/q/f/QFCRA_1559_VER1_ARABIC.doc
[52]www.qcert.org
[٥٣]الجمهورية اللبنانية - وزارة الاتصالات - ١ تموز/يوليو ٢٠١٥ http://www.mpt.gov.lb/index.php/ar/2013-02-17-13-15-34/mpt-news-ar/50-latest/373-2015-07-01-15-17-30
[54]http://cim.gov.ly/page95.html
[٥٥]شاركت شخصياً في مراجعته في مارس ٢٠١٤
[56]http://www.mcit.gov.eg/Ar/TeleCommunications/Telecom_Act_Law/Telecom_Act
[٥٧]http://www.egcert.eg/
[٥٨]http://www.ntra.gov.eg/arabic/main.asp
[٥٩]التنظيم في الحوسبة السحابية - https://itunews.itu.int/ar/Note.aspx?Note=3728
[60]http://www.alecso.org/cloud/
[٦١]مبدأ صحة معالجة ملفات البيانات، مبدأ تحديد الغاية من جمعها ومعالجتها، ومبدأ وصول الأشخاص المعنين الى الملفات وتصحيحها او شطبها، مبدأ عدم التمييز العنصري او العرقي او الاتني او السياسي او الجنسي او النقابي او المهني او الفلسفي، ومبدأ أمن البيانات لمنع فقدانها او تسربها او الاطلاع عليها...

[62] United Nations - General Assembly: Guidelines for the regulation of computerized personal data files – A/RES/45/95 – December 14, 1990.

[٦٣]مبدأ محدودية عمليات جمع البيانات، نوعية البيانات، تحديد الاستخدام والهدف، تأمين وسائل حماية وأمن المعلومات، العلانية، والحق في المشاركة والمساءلة[٦٣]... المبادئ عينها عادت الأمم المتحدة وتضمنتها عام ١٩٩٠ موصية الدول الاعضاء بإعتمادها في تشريعاتها المحلية.

Annex to the Recommendation of the Council of 23rd September 1980: GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA – https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[٦٤] ارشادات الإسكوا للتشريعات السيبرانية – الارشاد الرابع - معالجة وحماية البيانات ذات الطابع الشخصي –مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية – اللجنة الاقتصادية والاجتماعية لغربي آسيا – إدراة تكنولوجيا المعلومات – ٢٠١٢ - بيروت http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Dir-4-DataProtection.pdf

[65]BENBOUSSAN: Traitement des opérateurs acheminant du trafic international – in op.cit. – P: 798
[66]FERAL-SCHUL (Christiane): Cyberdroit, Le droit à l'épreuve de l'internet – 2009-2010 - Dalloz - P:83
[67] US-EU: International Safe Harbor Privacy Principles https://en.wikipedia.org/wiki/Safe_Harbor_Principles#cite_note-inval-9
[68]European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) 25 August 2000, retrieved 30 October 2015.

[69]Commission Européenne: Décision 2004/535/EC – JOUE – 235 – 6 JUILLET 2004 –p: 11-22 http://eur-lex.europa.eu/LexUriSerc/site/en/oj/2004/l_235l_23520040706enoo110022.pdf

[70]Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security - Official Journal L 0215 , 11/08/2012 P. 5 - 0014

[71]^ Jump up to: *"Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid"(press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3.Retrieved 7 October 2015.*

[٧٢]عدلت هذه التوصية بموجب التوجيه رقم ٥٨ / ٢٠٠٢ حول حماية الحياة الخاصة والاتصالات الالكترونية ثم بموجب التوجيه رقم ٢٠٠٦/٢٤ حول حفظ البيانات.

European Parliament and the Council of Europe: Directive 2006/24/EC – on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC.

[73]2010/87/: Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil [notifiée sous le numéro C(2010) 593] (Texte présentant de l'intérêt pour l'EEE) - OJ L 39, 12.2.2010, p. 5–18

[74] Directive 2002/19/EC of the European Parliament and of the Council of 7 march2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive

[75] Convention on Cybercrime (Budapest, 23 November 2001), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[76]Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350, 30.12.2008

[77]EU Commission: Industry calls for true digital single market in recommendations on European cloud strategy.

[78] Code of Practice: Protection of personal Data – 2009 https://dataprotection.ie/documents/code%20of%20practice/RevenueCOP.pdf

[79]Personal data protection: processing and free movement of data (General Data Protection Regulation) http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29

[80]**Cloud computing: A legal maze for Europe** / Euractiv, 18/4/2012 - Overview of cloud computing, its benefits and the associated legal issues.http://www.euractiv.com/innovation-enterprise/cloud-computing-legal-maze-europe-linksdossier-511262

[81]DEMOULIN (Marie), SOYEZ (Sébastien): L'archivage électronique dans le secteur public: entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit (sous la direction: Marie DEMOULIN) – CRIDS – Larcier – 2012 – Bruxelles – P: 37 et suiv.

[82] Canada: Personal Information Protection and Electronic Documents Act, 2000

[83] UK: Data Protection Act – 1998 – www.legislation.gov.uk

[84] USA Patriot Act – October 2001 - www.justive.gov.usa

[85]Commission nationale de l'informatique et des libertés CNIL: Guide sur les transferts de données à caractère personnel vers des pays non membres de l'union européenne. – 2008 - http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

[86]BENBOUSSAN: Traitements automatisés – Champs d'application de la loi – in: op.cit. - P: 508

[87] Mattatia: Transfert de données hors de l'Union européenne – En Pratique: devant les tribunaux et la CNIL – in: op.cit. - P: 156

[88]Loi N°.78/17 du 6 janv. 1978 – relative à l'informatique, aux fichiers et aux libertés – J.O. – 7 janv. 1978 – www.legifrance.gouv.fr

[89]Loi N°.88/227 – du 11 mars 1988 – Loi relative à la transparence financière de la vie politique – J.O. – 12 mars 1988; Loi N°92–1336 - 16 décembre 1992 - relative à l'entrée en vigueur de nouveau code pénal – J.O. – 23 déc. 19 92 – www.legifrance.gouv.fr; Loi N°.94-548 – 1er Juillet 1994 - relative au traitement des données nominatives ayant Pour fin la recherche dans le domaine de la santé - J.O. - 2 juillet 1994; Loi N°. 2000/321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations – J.O. – No. 88 – 13 avril 2000 – P: 5646; Loi N°.2003/239 du 18 mars 2003

pour la sécurité intérieure – J.O. – 19 mars 2003; Loi N°.57/298 du 11 mars 1957 sur la propriété littéraire et artistique – www.legifrance.gouv.fr

[90]Loi N°.2004/801 – du 6 août 2004 – relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel – et modifiant la loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - J.O. – N°. 182 – 7 août 2004 – P: 14063

[91]Convention for the protection of individuals with regard to Automatic Processing of Personal Data - 24.1.1981 – http://convenyions.coe.int/Treaty/FR/Treaties/Html/108.htm.

[92]Loi 801/2004 – pour la confiance dans l'économie numérique – 21 juin 2004

[93]Cass. Civ.: 1ere Chambre civile – 9 décembre 2003.

[94] Jurisprudences pour le statut de données personnelles: Conseil d'Etat – 10e et 9e sous-sections réunies – No. 288149 – 23 mai 2007; TGI Bobigny: 15e chambre – 14 décembre 2006; C.A Rennes: 3e chambre - 22 mai 2008; CA Rennes: 3e Chambre 23 juin 2008.

[95]Jurisprudences contre le statut de données personnelles: C.A. Paris: 13e chambre – section B – 27 avril 2007; C.A. Paris: 13e chambre section A – 15 mai 2007.

[96] LOI n°2015-912 du 24 juillet 2015 - art. 4
https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418316&cidTexte=LEGITEXT000006070719

[٩٧]وتم بمقتضاها تقرير عقوبات مشددة تصل إلى ٧ سنوات حبسا وغرامة قدرها ٧٥,٠٠٠ أورو متى تم ارتكاب فعل الدخول او البقاء غير القانوني أو فعل العرقلة العمدية أو فعل الغش والاحتيال في مواجهة نظام للمعالجة الآلية للمعطيات الشخصية الذي تسييره أو تنفيذه الدولة. بالطبع يهدف المشرع الفرنسي من هذا التجريم، المحافظة على كرامة الانسان وحقوقه الاساسية.

[98]Décret No. 2008-632 – 27 juin 2008 – Portant création d'un traitement automatisé de données à caractère personnel dénommé "EDVIGE" – J.O. – 1 juillet 2008 – No. 0152

[٩٩]الأمم المتحدة – الجمعية العمومية: مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الالكترونية – قرار رقم ٩٥/٤٥ – تاريخ ١٤ ديسمبر ١٩٩٠.

Council of Europe: Convention on the protection of individuals with regard to automatic processing of personal data – 1980

OECD: Guidelines on the protection of privacy and Transborder flow of Personal data – 1980 – www.oecd.org/document/18/0,23,40en_2649_34255_1815186_1_1_1_1,00.html

[100]BENBOUSSAN: informatique et atteintes aux intérêts fondamentaux de la nation: Trahison et espionnage – in: op.cit. – P: 921

[101] JHOSON (David): Law and Borders: The rise of law in cyberspace – in cyberlaw – op.cit. – P: 419

[102]MICONNET (Thomas): Le Cloud computing - un nuage d'insécurités juridiques – 2013
http://avocats-publishing.com/Le-Cloud-computing

[103] BENSOUSSAN: Caractéristiques du recours aux services de type cloud computing - op.cit. P: 371

[١٠٤]أهمية الاقتصادية للحوسبة السحابية- https://itunews.itu.int/ar/Note.aspx?Note=3727

[١٠٥]جنان الخوري: الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود – ٢٠٠٩ – صادر – بيروت – ص: ٤١٥ وما يليها

[106] NELKEN (David): Comparative criminal Justice and Globalization – 2011 – ASHGATE – P: 69

[١٠٧]لا سيما المنخرطين في الاتجار غير المشروع العابر للحدود على سبيل المثال لا الحصر، الاتجار بالمخدرات، والأسلحة، والاتجار بالبشر، وبالأعضاء البشرية، وتعزيز النزاعات المسلحة، وتبييض الأموال وتمويل الارهاب...

[108] CHERMAK (Steven), FREILICH (Joshua): Transnational terrorism – Ashgate – 2013 – P: 3

[109] AWAN (Imran), BLAKEMORE (Brian): Policing Cyber Hate, Cyber Threats and Cyber Terrorism – ASHGATE – 2012 – UK - P: 149

[110]DEMOULIN (Marie): Les cas spécifique des archives publiques : entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit – CRIDS – Larcier – 2012 – Bruxelles – P: 91 et suiv.

[111] ROOQUES-BONNET (Marie-Charlotte): Les bases de données de l'Etat: Les fichiers publics – in: Le droit peut-il ignorer la révolution numérique? – Michalon – 2010 – France - P: 23

[112]Gola: Droit du commerce électronique – guide pratique du e-commerce – op.cit. – 402 et suiv.

[113]DEBRAS (Jérôme): Guide juridique des contrats en informatiques – Editions ENI – 2013 – France–38.

[114]https://itunews.itu.int/Ar/Note.aspx?Note=3726

[115] QUEMENER (Myriam), PINTE (Jean-Paul): L'économie à l'ère numérique – in: Cyber-sécurité des acteurs économiques – risques, réponses stratégiques et juridiques – 2013 - Lavoisier – Paris - P: 165

[116] BENSOUSSAN (Alain): Exploitations des bases de données privées – in: Informatiques, Télécoms, Internet – 5e édition – Editions Francis LEFEBVRE – 2013 - P: 245 et suiv.
[117]DE MAISON ROUGE (Olivier): Le droit de l'intelligence économique – Patrimoine informationnel et secrets d'affaires – Lamy – 2012 - France P: 85

BIBLIOGRAPHY

BOOKS:

1. AWAN (Imran), BLAKEMORE (Brian): Policing Cyber Hate, Cyber Threats and Cyber Terrorism – ASHGATE – 2012 – UK .
2. BENSOUSSAN (Alain): Informatics, Télécoms, Internet: Réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques – 5e édition – 2012 – Editions Francis LEFEBEVRE.
3. CAPRIOLI (Eric): La sécurité des services de confiance in: Signature électronique et dématérialisation - 2014 – LexisNexis.
4. CHERMAK (Steven), FREILICH (Joshua): Transnational terrorism – ASHGATE – 2013
5. DEBRAS (Jérôme): Guide juridique des contrats en informatiques – Editions ENI – 2013 – France – 38 et suiv.
6. DE MAISON ROUGE (Olivier): Le droit de l'intelligence économique – Patrimoine informationnel et secrets d'affaires – Lamy – 2012 - France P: 85

7. DEMOULIN (Marie), SOYEZ (Sébastien): L'archivage électronique dans le secteur public: entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit (sous la direction: Marie DEMOULIN) – CRIDS – Larcier – 2012 – Bruxelles – P: 37 et suiv.
8. DEMOULIN (Marie): Les cas spécifique des archives publiques : entre archivage légal et archivage patrimonial – in: L'archivage électronique et le droit – CRIDS – Larcier – 2012 – Bruxelles – P: 91 et suiv.
9. FERAL-SCHUL (Christiane): Cyberdroit, Le droit à l'épreuve de l'internet – 2009-2010 - Dalloz - P:83
10. FITZGERALD (Brian): Cyber-Law – Volume I – The international library of essays in law & Legal theory – Second series – ASHGATE DARTMOUTH – Australia - P: XVII
11. GOLA (Romain): Bases de données et logiciels nécessaires au fonctionnement du site web – in: Droit du commerce électronique – Guide pratique du e-commerce - Gualino - Lextenso Editions – 2013.
12. LE METAYER (Daniel): Les technologies de l'information au service des droits: opportunités, défis, limites – 2010 – Cahiers du Centre d Recherches Informatique et Droit - Bruylant - P: 47
13. LESSIG (Lawrence): The law of the horse: What cyberlaw might teach? – in: CyberLaw – op.cit. - P: 250
14. MATTATIA (Fabrice): Cloud computing - Traitement des données personnelles - Le guide juridique – La loi Informatique et libertés et la CNIL – Jurisprudences – Editions EUROLLES – 2013
15. NELKEN (David): Comparative criminal Justice and Globalization – 2011 – ASHGATE.
16. QUEMENER (Myriam), PINTE (Jean-Paul): L'économie à l'ère numérique – in: Cyber-sécurité des acteurs économiques – risques, réponses stratégiques et juridiques – 2013 - Lavoisier – Paris
17. ROOQUES-BONNET (Marie-Charlotte): Les bases de données de l'Etat: Les fichiers publics – in: Le droit peut-il ignorer la révolution numérique? – Michalon – 2010 – France

المراجع باللغة العربية:

- الخوري (جنان): الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود – ٢٠٠٩ – صادر – بيروت

UNITED NATIONS:

United Nations - General Assembly: Guidelines for the regulation of computerized personal data files – A/RES/45/95 – December 14, 1990.

EUROPEAN UNION:

- US-EU: International Safe Harbor Privacy Principles
- https://en.wikipedia.org/wiki/Safe_Harbor_Principles#cite_note-inval-9
- European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) 25 August 2000, retrieved 30 October 2015
- Commission Européenne: Décision 2004/535/EC – JOUE – 235 – 6 JUILLET 2004 –p: 11-22
- http://eur-lex.europa.eu/LexUriSerc/site/en/oj/2004/l_235l_23520040706enoo110022.pdf
- Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security - Official Journal L 0215 , 11/08/2012 P. 5 - 0014
- Jump up to: abc"Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid"(press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3. Retrieved 7 October 2015.

- European Parliament and the Council of Europe: Directive 2206/24/EC – on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC.
- 2010/87/: Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil [notifiée sous le numéro C(2010) 593] (Texte présentant de l'intérêt pour l'EEE) - OJ L 39, 12.2.2010, p. 5–18
- Directive 2002/19/EC of the European Parliament and of the Council of 7 march2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters - OJ L 350, 30.12.2008
- EU Commission: Industry calls for true digital single market in recommendations on European cloud strategy.
- Code of Practice: Protection of personal Data – 2009
- https://dataprotection.ie/documents/code%20of%20practice/RevenueCOP.pdf
- Personal data protection: processing and free movement of data (General Data Protection Regulation)
- http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29
- Cloud computing: A legal maze for Europe / Euractiv, 18/4/2012 - Overview of cloud computing, its benefits and the associated legal issues.http://www.euractiv.com/innovation-enterprise/cloud-computing-legal-maze-europe-linksdossier-511262
- OECD: Guidelines on the protection of privacy and Transborder flow of Personal data – 1980 – www.oecd.org/document/18/0,23,40en_2649_34255_1815186_1_1_1_1,00.html
- Council of Europe: Convention on the protection of individuals with regard to automatic processing of personal data – 1980

Local Legislations:

1. Canada: Personal Information Protection and Electronic Documents Act, 2000
2. Patriot Act – 2001 – USA
3. **FRANCE**:
   - Code de la santé publique, dernière modification: 1 juillet 2014
   - Décret No. 960/2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires) – 15 mai 2007.
   - Loi N°.78/17 du 6 janv. 1978 – relative à l'informatique, aux fichiers et aux libertés – J.O. – 7 janv. 1978 – www.legifrance.gouv.fr
   - Loi N°.88/227 – du 11 mars 1988 – Loi relative à la transparence financière de la vie politique – J.O. – 12 mars 1988;
   - Loi N°92–1336 - 16 décembre 1992 - relative à l'entrée en vigueur de nouveau code pénal – J.O. – 23 déc. 1992 – www.legifrance.gouv.fr;
   - Loi N°.94-548 – 1er Juillet 1994 - relative au traitement des données nominatives ayant Pour fin la recherche dans le domaine de la santé - J.O. - 2 juillet 1994;
   - Loi N°. 2000/321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations – J.O. – No. 88 – 13 avril 2000 – P: 5646;

- Loi N°.2003/239 du 18 mars 2003 pour la sécurité intérieure – J.O. – 19 mars 2003; Loi N°.57/298 du 11 mars 1957 sur la propriété littéraire et artistique – www.legifrance.gouv.fr
- Loi N°.2004/801 – du 6 août 2004 – relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel – et modifiant la loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - J.O. – N°. 182 – 7 août 2004 – P: 14063
- Loi 801/2004 – pour la confiance dans l'économie numérique – 21 juin 2004

القوانين العربية

الأردن:

- قانونَ الإحصاءاتِ العامةِ، المُؤقتِ عام ٢٠٠٨.
- قانون جرائم أنظمة المعلومات، رقم ٣٠، لعام ٢٠١٠ (جريدة رسمية رقم ٥٠٥٦ – تاريخ ٢٠١٠/٩/١٦ – صفحة ٥٣٣٤)
- قانون الإتصالات السلكية واللاسلكية رقم ١٣ لسنة ١٩٩٥، الذي عدل بموجب قانون التعديل رقم ٢١ لسنة ٢٠١١ (الجريدة الرسمية رقم ٤٠٧٢ بتاريخ ١٩٩٥/١٠/٠١).

الإمارات العربية المتحدة:

- قانونُ العقوباتِ الإماراتيّ (رقم ١٩٨٧/٣)
- قانون "مؤسسة الإمارات للاتصالات" (رقم1 لسنة١٩٩١)
- قانون تنظيم قطاع الاتصالات رقم (٣) لسنة ٢٠٠٣
- "قانون التوقيع الإلكتروني والتجارة"، عام ٢٠٠٢
- [١١٧] قانون اتحادي رقم (١) لسنة ٢٠٠٦ م في شأن المعاملات والتجارة الإلكترونية – أبو ظبي – ٣ يناير ٢٠٠٦
- قانون امارة دبي الخاص بالمعاملات والتجارة الالكترونية - قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية – دبي – ١٢ فبراير ٢٠٠٢ القانون الإتحادي المُتعلّق بـ"مكافحةِ جرائم تقنية المعلومات"، رقم ٢٠٠٦/٢ – الإمارت العربية المتحدة مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات - أبو ظبي - ١٣ أغسطس ٢٠١٢
-
- التعميم رقم ٦ بشأن سياسة ومعايير حكومة أبو ظبي لأمن المعلومات عام ٢٠١٣.
- مجلس الوزراء الإماراتي القرار رقم ٢٠١٣/٢١ المتعلق بلائحة أمن المعلومات في الجهات الإتحادية،
- قانون حماية البيانات الشخصية – رقم ١ – ٢٠٠٧ – خاص بالمركز المالي الدولي لدبي DIFC
- قانون حماية البيانات الشخصية – رقم ٢٠٠٦/١١ – المادة ٨ -الامارات العربية المتحدة.
- قانونَ إمارة دبي، لِنشر وتبادُل البياناتِ (قانون البيانات المفتوحة في ١٧ أكتوبر ٢٠١٥).
- قانون إمارة دبي، المُتعلّق، بإنشاءَ وحمايةِ شبكةِ الإتصالاتِ الصادر عام ٢٠٠٢، وقانون رقم ٢٠٠٤/٥ حول الأمنِ المعلوماتيّ.
- قرار المجلس التنفيذي رقم ٢٠١٢/١٣ بشأن أمن المعلومات في إمارة دبي.

البحرين:

- قانون الاتصالات والإنترنيت رقم ٤٨ لعام ٢٠٠٢.
- القانون رقم ٢٨ /٢٠٠٢ المتعلق بالمعاملات والتجارة الإلكترونية، والقانون رقم ٢٠١٤/٦٠ بشأن جرائم تقنية المعلومات.
- المرسوم رقم ٩ لعام ٢٠٠٢ لإعادة تنظيم الجهاز المركزي للمعلومات
- والقرار رقم ٢٥ لعام ٢٠٠٥، لتشكيل لجنة عليا لتقنية المعلومات والإتصالات.

الجزائر:

- القانون رقم ٠٩-٠٤ المؤرخ في ١٤ شعبان عام ١٤٣٠ الموافق ٠٥ اوغست سنة ٢٠٠٩

السعودية:

- نظامُ مكافحة جرائم المعلوماتية لعام ٢٠٠٧.
- قرار المجلس الوزراي رقم ٤٠ تاريخ ٢٠٠٦/٣/٢٧، المتعلق بضوابط التعاملات الإلكترونية الحكومية؛ القرار رقم ٦٦٦٧ تاريخ ١٤٢٦/٧/١ هـ، المتعلق بشروط مزاولة مهنة الإستشارات في مجال الإتصالات وتقنية المعلومات.

السودان:

قانون المعاملات الإلكترونية عام ٢٠٠٧ وقانون مكافحة جرائم المعلوماتية عام ٢٠٠٧

العراق:

- قانون العلامات والبيانات التجارية رقم ٢١ لعام ١٩٧٥، والذي تعدّل بموجب قانون ٢٠١٠، تاريخ ٢٠١٠/١/٤.
- قانون حماية المستهلك رقم ١ تاريخ ٢٠١٠/١/٤.
- القانون رقم ٢٠١٢/٧٨، المتعلق بالتوقيع الإلكتروني والمعاملات الإلكترونية.

الكويت:

- القانون بالمرسوم رقم (٥) لسنة1999 م، متضمنًا حماية المصنفات والحاسب الآلي من البرامج وقواعد البيانات (م١).
- قانون رقم ٢٠١٤/٣٧ استحداث هيئة تنظيم الاتصالات وتقنية المعلومات.

المغرب

- القانون رقم ٠٩,٠٨ الصادر بتنفيذه الظهير رقم ١,٠٩,١٥ بتاريخ ١٨ فبراير ٢٠٠٩، والمنشور بالجريدة الرسمية رقم ٥٧١١ بتاريخ ٢٣ فبراير ٢٠٠٩.
- قانون رقم ٢٠٠٩/٨ لحماية البيانات الشخصية؛ قانون رقم ٢٠٠٣/٧ لمكافحة جرائم المعلوماتية؛ قانون رقم ٥٣,٠٥ المتعلق بالتبادل الالكتروني للمعطيات الالكترونية؛ قانون حماية المستهلك على الانترنيت رقم ٢٠٠٨/٣١

اليمن:

- القانون رقم ٤٠ لعام ٢٠٠٦ بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية
- القرار الجمهوري رقم ١٩٩٥/١٥٥، لإنشاء "المركز الوطني للمعلومات"، لمواكبة تطورات مجتمع المعلومات. وفي عام
- قرار مجلس الوزراء رقم ٢٠٠٢/٤ " لإنشاء مدينة تكنولوجيا الإتصالات والمعلومات

تونس:

- القانون رقم ٢٠٠٤/٦٣ المتعلق بحماية البيانات الشخصية – ٢٧ جويليه ٢٠٠٤؛ القانون عدد ١٩٩٨/٣٨ المتعلق بمجلة البريد؛ القانون عدد ٢٠٠٠/٨٣ المتعلق بالمبادلات والتجارة الإلكترونية، ٩ أب/أغسطس ٢٠٠٠؛ الأمر عدد ٢٠٠٠/٢٣٣١ المتعلّق بضبط التنظيم الإداري والمالي وطرق تيسير الوكالة الوطنية للمصادقة الإلكترونية؛ الأمر ٢٠٠١/١٩٦٧ المتعلق لضبط خدمات المصادقة الإلكترونية، الأمر رقم ٢٠٠١/١٩٦٨؛ القانون رقم ٢٠٠٤/٥ المتعلق بتنظيم مجال السلامة المعلوماتية – تاريخ ٣ شباط/فبراير ٢٠٠٤؛ القانون رقم ٢٠٠٥/٥١ المتعلق بالتحويل الإلكتروني – تاريخ ٢٧ حزيران/يونيو ٢٠٠٥؛ القانون التوجيهي عدد ٢٠٠٧/١٣ المتعلق بإرساء الإقتصاد الرقمي – تاريخ ١٩ شباط/فبراير ٢٠٠٧؛ أمر ٢٠٠٧/١٢٧٤ قائمة الأنشطة المرتبطة بالإقتصاد الرقمي – تاريخ ٢١ آيار/مايو ٢٠٠٧.

جيبوتي:

- قانون الحماية ومكافحة الغش وحماية المستهلك، رقم ٢٨ عام ٢٠٠٨.

سلطنة عمان"

- قانون المُعاملات الإلكترونيةِ (٢٠٠٨/٦٩).
- قانون مكافحة جرائم تقنية المعلومات-المرسوم السلطاني، رقم ٢٠١١/١٢، (الجريدة الرسمية عدد ٩٢٩ – تاريخ ٦ فبراير ٢٠١١).

سوريا:

- قانونَ التوقيعِ الإلكترونيّ وخدمات الشبكة، رقم ٢٠٠٩/٤،
- قانونَ تنظيمِ قطاع الإتصالاتِ، رقم ٢٠١٠/١٨،
- قانون الإعلام بالمرسوم الإشتراعي، رقم ١٠٨، تاريخ ٨ آب/أغسطس ٢٠١١،
- المرسوم الإشتراعي، رقم ٢٠١٢/١٧ المُتعلّق بِتنظيمَ التواصِلِ على الشبَكَة ومكافحة جريمَةِ المعلوماتيّةِ

فلسطين:

- قانون الإحصاءات العامة رقم ٤ لعام ٢٠٠٠ بشأن الحق في الوصول الى معلومات الإحصاءات.
- قرار مجلسِ الوزراءِ، في فلسطين، رقم ٣٥ لعام ٢٠٠٤، الذي يتناولُ، حقَّ النفاذِ إلى الشبَكَةِ العالميَةِ (الإنترنيت) والبريد الإلكتروني عبر مركز الحاسوب الحكومي.
- مرسوم رقم ٣٥ لعام ٢٠٠٤ لحق الوصول الى شبكة المعلومات العالمية
- قرار مجلس الوزراء رقم ٣ لعام ٢٠٠٤ بشأن منع بيع وتسويق خدمات الإتصالات وتقنية المعلومات والبريد السريع.
- قرار مجلس الوزراء رم ٢٦٩ لعام ٢٠٠٥، بالمصادقة على السياسات العامة لإستخدام الحاسوب وشبكة الإنترنيت في المؤسسات العامة.
- قرار مجلس الوزراء رقم ٧٤ لسنة ٢٠٠٥ بشأن الإستراتيجية الوطنية للإتصالات وتكنولوجيا المعلومات.
- قرار مجلس الوزراء رقم ٦٥ لعام ٢٠٠٥ للمصادقة على اعتماد مبادرة فلسطين الإلكترونية.
- قرار رقم ٢٠ لعام ٢٠٠١، الذي أنشأ الهيئة الوطنية لمسميات الإنترنيت.
- قانون المعاملات الإلكترونية لعام ٢٠١٠.

قطر:

- قانونُ الإتصالاتِ، في قطر رقم ٢٠٠٦/٣٤،
- قانون معاملات التِجارةِ الإلكترونية - رقم ٢٠١٠/١٦ (في ٢٠١٠/٨/١٩)،
- قانون مركز قطر المالي - قانون رقم (٧) لسنة ٢٠٠٥ بإصدار قانون مركز قطر للمال ٧ / ٢٠٠٥ - Qatar Financial Centre.

قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية **لبنان:**

- القانون رقم ١٤٠ بتاريخ ٢٧ تشرين الأول/أكتوبر ١٩٩٩ المتعلّق بصون الحق بسرية المكالمات الهاتفية.

مصر:

- القانونِ رقم ١٠ لعام ٢٠٠٣ - قانون تنظيم الإتصالات.
- القانون رقم ١٢٠ لعام ٢٠٠٨.