التكنولوجيات الناشئة وتأثيرها على السياسات واللوائح في الشرق الأوسط وشمال أفريقيا

مايكل كندي ورياض البلوشي - ٢٩ مايو ٢٠٢٥

شكر وتقدير: نود أن نتقدم بالشكر إلى نرمين السعدني لدورها القيادي، وهنا صباغ وحنا قريطم لدعمهما المستمر للعمل في المنطقة، والدكتور جوزيف لورينزو هول، وناتالي كامبل، وكارل جانبيرج، وأولاف كولكمان، وجون

موريس، وكريستين رانيجار، وروبن ويلتون على مساهماتهم في هذا التقرير. كما ساهم صانعو السياسات والمشاركون في ورش العمل من عُمان والبحرين بمعلومات عن خصائص كل دولة.

تنويه: *تتحقق مجموعة أدوات تقييم تأثير الإنترنت التابعة لجمعية الإنترنت (مجموعة الأدوات) من تأثير اللوائح على الإنترنت لضمان تعزيزها لنهج الإنترنت في تكوين الشبكات، وذلك من خلال توفير إطار عمل لتحليل التغييرات المقترحة في السياسات والتشريعات واللوائح والجوانب الأخرى التي تؤثر على الإنترنت. استخدم كُتَّاب هذا التقرير مجموعة الأدوات كإطار عام لإجراء هذا التحليل المقارن للسياسات الإقليمية، وقد استخدمنا هذا المنظور الخاص بجمعية الإنترنت لنستنتج هذه الرؤية وما توصلنا اليه من نتائج.*

الملخص التنفيذي

السياق

يُقوم هذا التقرير، الذي كلفنا به من قبل جمعية الإنترنت، بتحليل تأثير السياسات واللوائح الحالية والمقترحة على التكنولوجيات الناشئة في منطقة الشرق الأوسط وشمال أفريقيا. وتستخدم الدراسة مجموعة أدوات تقييم تأثير الإنترنت الصادر عن جمعية الإنترنت (مجموعة الأدوات)، موضحة فائدتها في تقييم البيئات التنظيمية المعقدة وتعزيز طريقة الإنترنت في التواصل.

قامت جمعية الإنترنت، كمؤيد عالمي لإنترنت مفتوح وآمن وموثوق به، بتطوير مجموعة أدوات لتقييم مقترحات السياسات واللوائح التنظيمية. وتهدف هذه الدراسة بشكل رئيسي إلى توضيح كيفية إرشاد هذه المجموعة لصانعي السياسات في منطقة الشرق الأوسط وشمال أفريقيا لوضع لوائح تدعم الابتكار وتخفف المخاطر دون التأثير سلبًا على أسلوب الإنترنت في تكوين الشبكات، مما يعزز الابتكار ويصون حقوق المواطنين ويحافظ على المبادئ الأساسية للإنترنت.

يقوم التقرير بتقييم العديد من لوائح الإنترنت، مُستعرضًا الفرص والتحديات التي تُشكّلها لاثنين من التكنولوجيات الناشئة بالغة الأهمية: الذكاء الاصطناعي والحوسبة السحابية والحوسبة الطرفية. ويُقيّم المشروع اللوائح التنظيمية الرئيسية في ست دول من منطقة الشرق الأوسط وشمال أفريقيا، وهي البحرين، ومصر، والأردن، وعُمان، والمملكة العربية السعودية والإمارات العربية المتحدة، مُركّزًا على أربع مجالات رئيسية:

- **حوكمة البيانات** - اللوائح التي تحكم تخزين البيانات والوصول إليها ونقلها عبر الحدود.
- **حماية الخصوصية** - اللوائح التي تضمن خصوصية المستخدم، بما في ذلك الحماية من التنميط الآلي.
- **مسؤولية الوسيط** - مدى مسؤولية المنصات الإلكترونية ومقدمي الخدمات عن المحتوى الخاص بالطرف الثالث
- **لائحة التشفير** - الأطر القانونية التي تؤثر على استخدام تكنولوجيات التشفير وتوافرها.

يمكن أن تتداخل هذه اللوائح، وقد تؤثر على طبيعة الإنترنت المفتوحة والعالمية والمتوافقة، مما قد يؤدي إلى تفتيت او تشتت الإنترنت.

استخدمت الدراسة مدخلات من صانعي السياسات في كل من الدول الست التي تم التركيز عليها، بالإضافة إلى مساهمات من خبراء جمعية الإنترنت، وذلك لضمان تقديم تقييم شامل. تم عرض النتائج الرئيسية والتوصيات الأولية وتحسينها من خلال ورشة عمل عُقدت في عُمان في يوليو، ومؤتمر عُقد في البحرين في ديسمبر، حيث

تم جمع المزيد من ملاحظات أصحاب المصلحة. وتم تعريف أصحاب المصلحة بمجموعة الأدوات التي استُخدمت طوال فترة الدراسة لتقييم مدى توافق اللوائح الحالية والمقترحة مع أفضل الممارسات العالمية والمبادئ الأساسية للإنترنت.

الاستنتاجات والنتائج

قدّمت الدراسة مراجعة شاملة وحديثة للتشريعات الحالية والمقترحة في كل من الدول الست، للوصول إلى الاستنتاجات التالية حول تأثيرها على التكنولوجيات الناشئة والإنترنت على نطاق أوسع.

- **حوكمة البيانات:** قد تُقيّد متطلبات توطين البيانات في العديد من دول منطقة الشرق الأوسط وشمال أفريقيا الوصول إلى الخدمات السحابية، مما يُعيق التحوّل الرقمي. وقد تؤثر هذه اللوائح أيضًا على توافر تطبيقات الذكاء الاصطناعي وكفاءتها، لا سيما في مجالي الرعاية الصحية والخدمات المالية.
- **الخصوصية:** على الرغم من أن العديد من دول منطقة الشرق الأوسط وشمال أفريقيا قد وضعت قوانين لحماية البيانات، إلا أن القيود المفروضة على نقل البيانات عبر الحدود، والثغرات في الحماية من التنميط القائم على الذكاء الاصطناعي، لا يزالان قضايا رئيسية.
- **مسؤولية الوسطاء:** يؤدي غياب الحماية القانونية الواضحة للمنصات الإلكترونية في معظم دول منطقة الشرق الأوسط وشمال أفريقيا المخاطر القانونية، إلى إعاقة الابتكار المحلي، ويُثبّط الاستثمار في الخدمات الرقمية.
- **التشفير:** تُهدّد القيود (في بعض دول منطقة الشرق الأوسط وشمال أفريقيا) الأمن السيبراني والخصوصية والثقة في الخدمات الرقمية.

الملخص

تمر حكومات منطقة الشرق الأوسط وشمال أفريقيا بمرحلة حرجة في صياغة سياسات رقمية تؤثر على الابتكار والاستثمار وانفتاح الإنترنت. يمكن للحكومات أن تطلق العنان للإمكانات الكاملة للتكنولوجيات الناشئة مع الحفاظ على المزايا الأساسية لإنترنت متصل عالميًا وآمن وموثوق، وذلك خلال اعتماد أطر تنظيمية تدعم أسلوب الإنترنت في تكوين الشبكات، وتخضع لتقييم دقيق باستخدام مجموعة الأدوات. يُمثل هذا التحليل تقييمًا خاصًا لمنطقة الشرق الأوسط وشمال أفريقيا، ومثالًا أوسع نطاقًا لكيفية توظيف مجموعة الأدوات من قبل مختلف الجهات المعنية لتعزيز إنترنت مفتوح ومتصل عالميًا وآمن وموثوق.

المقدمة

تُعيد التكنولوجيات الرقمية الناشئة تشكيل أسلوب الحياة التقليدي، وطبيعة الاقتصادات، وكيفية استخدامنا للإنترنت. يُقدّم هذا التقرير، والذي كلفنا بإعداده من قبل جمعية الإنترنت، تحليلاً في الوقت المناسب لكيفية تأثير هذه التكنولوجيات على السياسات واللوائح التنظيمية في منطقة الشرق الأوسط وشمال إفريقيا. وبشكل أساسي، فهو يستخدم مجموعة أدوات تقييم تأثير الإنترنت الصادرة عن جمعية الإنترنت (مجموعة الأدوات) كإطار تحليلي رئيسي، موضحا فائدتها في تقييم البيئات التنظيمية المعقدة وتعزيز أسلوب تكوين الشبكات عبر الإنترنت.

بينما حظي ظهور الذكاء الاصطناعي باهتمام كبير مؤخراً، إلا أنه لا يعد التكنولوجيا الرقمية الناشئة الوحيدة التي تُؤثر على الحكومات والهيئات التنظيمية. تُغيّر الحوسبة السحابية بشكل جذري من الوصول إلى، ومن موقع، البيانات والمحتوى والخدمات. ويُمثل التحول الرقمي الذي تُحرّكه هذه التكنولوجيات وغيرها قضيةً مُلحة، بما في ذلك في منطقة الشرق الأوسط وشمال إفريقيا.

ونتيجة لذلك، تُراجع الحكومات بشكل مُتزايد السياسات القائمة وتدرس سياسات جديدة لتعزيز الابتكار والاستثمار واستخدام التكنولوجيات الجديدة، مع السعي في الوقت نفسه إلى حماية المواطنين من الأضرار المُحتملة. ومع ذلك، من المهم أن تكون هذه اللوائح ذكية بقدر التكنولوجيات التي تتناولها لتجنب التأثيرات غير المقصودة أو غير المتوقعة على الإنترنت.

يتزايد أهمية الدور الداعم لجمعية الإنترنت، كجهة رائدة فكريًا في حماية الإنترنت وتعزيزه. ففي الوقت الذي تدرس به الحكومات تعديل اللوائح الحالية أو فرض لوائح جديدة على التكنولوجيات الناشئة، تقوم جمعية الإنترنت بدعم أسلوب الإنترنت في تكوين الشبكات باعتبارها الأساس الجوهري للإنترنت، وقد طورت مجموعة الأدوات لتوجيه مثل هذه القرارات وضمان استمرار ازدهار الإنترنت. ويمكن لصانعي السياسات والمؤسسات الأكاديمية والشركاء والحلفاء ذوي التفكير المماثل الرجوع إلى جمعية الإنترنت والاستعانة بموارد مثل مجموعة الأدوات عند تشكيل سياساتهم واللوائح الخاصة بهم، خاصة أن الإجراءات الحكومية التي تقوض طبيعة الإنترنت المفتوحة والمتصلة عالميًا والآمنة والجديرة بالثقة يمكن أن تؤدي أيضًا إلى تفتيتها وتقليل فوائدها.

يهدف هذا التقرير بشكل أساسي إلى تقييم لوائح الإنترنت الرئيسية المتعلقة بالتكنولوجيات الناشئة من خلال توضيح التطبيق العملي وقيمة مجموعة أدوات تقييم تأثير الإنترنت التي أعدتها جمعية الإنترنت. وبشكل رئيسي، يهدف إلى توضيح كيفية إرشاد مجموعة الأدوات صانعي السياسات في منطقة الشرق الأوسط وشمال إفريقيا لوضع لوائح تدعم الابتكار وتخفف المخاطر دون التأثير سلبًا على أسلوب الإنترنت في تكوين الشبكات.

يُقيم التقرير العديد من لوائح الإنترنت، مُراعيًا الفرص والتحديات التي تُمثلها للتكنولوجيات الجديدة. ونركز هنا على اثنين من التكنولوجيات الناشئة وهما الذكاء الاصطناعي والحوسبة السحابية والطرفية. تشمل السياسات واللوائح الحكومية محل المراجعة هنا حوكمة البيانات، وحماية الخصوصية، وحماية مسؤولية الوسطاء وتنظيم التشفير. قد تتداخل هذه اللوائح، وقد تؤثر على طبيعة الإنترنت المفتوحة والعالمية والمتوافقة، مما قد يؤدي إلى تفتيت وتشتت الإنترنت.

يفي هذا التقرير احتياج كبير وذلك من خلال عرض كيفية استخدام إطار عمل منظم (مجموعة الأدوات) لتعزيز عملية صنع القرار فيما يتعلق بسياسات الإنترنت. ندرس في هذا التقرير اللوائح الحالية والمُقترحة ذات الصلة بالتكنولوجيات الجديدة على المستوى الدولي، ونقارنها بتلك الموجودة في ست دول في منطقة الشرق الأوسط وشمال إفريقيا وهم البحرين، ومصر، والأردن، وعُمان، والمملكة العربية السعودية، والإمارات العربية المتحدة، وذلك لتحديد أي فجوات.

على الرغم من أن الموضوعات التي تتناولها هذه اللوائح ذات صلة بسياسات الإنترنت منذ سنوات، إلا أن ظهور التكنولوجيات الجديدة قد يؤدي إلى إدخال لوائح جديدة أو تعديلات على اللوائح الحالية، مثل تلك المتعلقة بالخصوصية، ومسؤولية الوسطاء، وتوطين البيانات. لذلك، يسعى هذا المشروع إلى تحديد الفجوات ذات الصلة في اللوائح أو التغييرات المقترحة والتي من شأنها أن تستفيد من تطبيق مجموعة الأدوات لضمان توافقها مع أسلوب الإنترنت في تكوين الشبكات. يُعد هذا التحليل بمثابة تقييم محدد لمنطقة الشرق الأوسط وشمال أفريقيا، ومثال أوسع نطاقًا على كيفية استخدام مجموعة الأدوات من قبل مختلف الجهات المعنية لتعزيز إنترنت مفتوح، ومتصل عالميًا، وآمن وموثوق.

الموضوعات الرئيسية

يحدد هذا القسم السياسات واللوائح التي يتناولها هذا التقرير، بالإضافة إلى التكنولوجيات الناشئة ومجموعة الأدوات لتقييم اللوائح ذات الصلة. يُناقش القسم الثالث أدناه السياسات واللوائح الخاصة بكل دولة من دول منطقة الشرق الأوسط وشمال إفريقيا.

السياسات واللوائح

مع اتساع نطاق استخدام الإنترنت وشموله، وتغطيته لجميع جوانب حياة الأفراد، وعمليات الشركات، وسير عمل الحكومات، تتزايد كمية البيانات مع تطور طبيعتها لتعكس جميع الأنشطة الإلكترونية. ونتيجة لذلك، سعت الحكومات إلى تطبيق اللوائح غير المتصلة بالإنترنت على الإنترنت، وتطوير لوائح جديدة حسب الحاجة. يمكن لهذه اللوائح أن تزيد من قدرة الشركات وحوافزها على الابتكار والاستثمار في خدمات جديدة، وأن تزيد من ثقة الأفراد في هذه الخدمات. في هذا التقرير، ندرس أربع مجموعات من هذه اللوائح، وكيف يمكن أن تساعد في ضمان إنترنت مفتوح وموثوق.

حوكمة البيانات

حوكمة البيانات هي سياسة حكومية يمكن أن تُحدد فئات البيانات وتُوجه كيفية إدارة المؤسسات لكل فئة منها. تشمل أمثلة هذه الفئات البيانات الشخصية، وبيانات الشركات، وبيانات الأبحاث والبيانات العامة. تُعامل البيانات المالية أو الصحية في بعض البلاد بمعزل عن الفئات الأخرى. ومن ضمن الجوانب الأخرى، يمكن أن تشمل السياسات حوكمة فئات معينة من البيانات داخل البلد (في حالة السكون) بالإضافة إلى عمليات النقل عبر الحدود (أثناء النقل).

يجب أن توازن سياسات حوكمة البيانات بين عدة عناصر مهمة لإنترنت مفتوح ومتصل عالميًا وآمن وموثوق. وتحديدًا، يعتمد الإنترنت المفتوح على التدفق الحر للبيانات، لذا فإن الجهود المبذولة لتقييد عمليات النقل عبر الحدود قد تؤدي إلى تفتيت الإنترنت.[1] في الوقت نفسه، وبدون وجود قيود على معالجة البيانات في حالة السكون داخل البلد، أو ضمانات مماثلة خارجه، سيصبح الإنترنت أقل موثوقية.

هناك بعض التداخل مع الفئات الأخرى من السياسات الموضحة أدناه. تغطي سياسات الخصوصية حوكمة البيانات الشخصية تحديدًا، بينما تتناول سياسات حوكمة البيانات في بعض البلدان تشفير البيانات. نغطي في هذا التقرير الجوانب العامة لحوكمة البيانات، وفي الأقسام أدناه نرصد الجوانب الخاصة بحماية الخصوصية والتشفير.

حماية الخصوصية

تنص لوائح الخصوصية على حقوق الأفراد في الخصوصية وحماية بياناتهم الشخصية. وفي هذا السياق، تُعرف البيانات الشخصية بأنها أي معلومات تتعلق بشخص مُعرف أو قابل للتعريف، بما في ذلك الاسم ومعلومات الاتصال ورقم بطاقة الائتمان وغيرها من المعلومات. ويضيف الاتحاد الأوروبي لهذا التعريف تصنيف للبيانات الحساسة، يضم التوجه العرقي أو الإثني، والبيانات الصحية والوراثية، والمعتقدات السياسية والتوجه الجنسي.

تُحدد لوائح الخصوصية كيفية جمع هذه البيانات واستخدامها وتخزينها وحمايتها ومشاركتها. ويشمل ذلك كيفية استخدامها في التنميط أو اتخاذ القرارات الآلية، وهو أمر يتزايد أهميته مع تزايد استخدام الذكاء الاصطناعي في العمليات التجارية والحكومية.

تُعد حماية الخصوصية جزءًا من حوكمة البيانات المتعلقة ببيانات مُحددة، والتي قد تشمل متطلبات مُحددة بشأن معالجتها أثناء التخزين أو أثناء النقل، بما في ذلك عبر الحدود. إن عدم وجود حماية كافية للخصوصية يُمكن أن يُؤثر بشكل كبير على الأفراد الذين يتم تسريب بياناتهم ويُساء استخدامها، خاصةً إذا كانت البيانات حساسة، وقد يُقلل من ثقة جميع المستخدمين بالإنترنت، وليس فقط أولئك المُتأثرين بها بشكل مباشر.

حماية مسؤولية الوسطاء

الوسطاء هم كيانات تُمكّن أو تدعم تبادل المحتوى عبر الإنترنت بين المستخدمين (شركات، حكومات، أفراد، ومؤسسات). يتعامل الوسطاء مع المحتوى الذي يُنشئه هؤلاء المستخدمون، لكنهم غير مسؤولين عنه قانونًا. يشمل الوسطاء شبكات توصيل المحتوى (CDNs)، ومقدمي الخدمات السحابية، ومستضيفي المواقع الإلكترونية، ومحركات البحث، ومنصات التواصل الاجتماعي، ومقدمي خدمات الإنترنت (ISPs). بدون الوسطاء، لن يتمكن الأفراد من المشاركة في نقاشات كرة القدم عبر الإنترنت، أو إتاحة مقاطع الفيديو أو أي محتوى إبداعي آخر عبر الإنترنت، أو المشاركة على نطاق أوسع في حوار عالمي عبر الإنترنت.

على سبيل المثال، قد يقوم مستخدم بإنشاء فيديو ويستخدم مقدم خدمة إنترنت لتحميله على منصة تواصل اجتماعي. وقد تُرسله هذه المنصة إلى شبكة توصيل محتوى لتُوزعه بدورها على مخازن قريبة من قواعد المستخدمين الرئيسية للمنصة، ويصل المستخدمون النهائيون إلى الفيديو من مخزن قريب. لا تتحمل أي من الشركات التي تستضيف وتُقدم الفيديو أي مسؤولية تحريرية عن محتوى الفيديو. ومع ذلك، إذا كان المحتوى ينتهك حماية حقوق الطبع والنشر، أو كان ضارا أو غير قانوني، فقد تأمر المحكمة في بعض الولايات القضائية الوسيط بحذف الفيديو أو حجب الوصول إليه.

[1] للتعرف على حالات استخدام أسلوب الإنترنت في تكوين الشبكات حول تأثير توطين البيانات، انظر https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-/toolkit/use-case-data-localization

تقدم حماية مسؤولية الوسيط الحماية لهؤلاء الوسطاء من المسؤولية عن المحتوى الذي يقومون بنقله أو استضافته.[2] علاوة على ذلك، يمكن للشركات اتخاذ قرار بحذف المحتوى غير المقبول، دون أن تقع عليهم أي مسؤولية جراء ذلك. وقد مكّنت حماية مسؤولية الوسيط مجموعة واسعة من الوسطاء من تجربة وإطلاق خدمات جديدة ومبتكرة عبر الإنترنت. ومن المرجح أن يؤدي غياب أو تقييد حماية الوسيط إلى تثبيط الشركات عن تقديم تلك الخدمات أو إلى تقييد الوصول إلى خدماتها ونوع المحتوى الذي يمكن نقله بشكل كبير، مما قد يمنع الأفراد أو يقلل من مشاركتهم على الإنترنت.

التشفير

يحمي التشفير البيانات عبر الإنترنت بحيث لا يمكن استخدامها إلا من قِبل الأشخاص المعنيين بالوصول إليها.[3] على سبيل المثال، يُستخدم التشفير الآن بشكل كبير من قِبل خدمات المراسلة لحماية الرسائل من طرف إلى طرف، بحيث لا يستطيع حتى مقدم الخدمة قراءتها. يُستخدم التشفير أيضًا لحماية المعلومات المنقولة عبر شبكة الويب العالمية، مثلما يتم ذلك على مواقع التجارة الإلكترونية لحماية مشتريات عملائها ببطاقات الائتمان. وبشكل أعم، يمكن استخدامه لحماية البيانات في حالة السكون (في مركز البيانات) أو أثناء نقلها (عبر مقدمي خدمة الإنترنت).

يلعب التشفير دورا هاما في حماية الخصوصية والبيانات الحساسة، ومنع الجرائم الإلكترونية، والاعتراض غير القانوني. ونتيجة لذلك، فإن الإنترنت الآن أكثر أمانًا وموثوقية. يمكن أن تُلحق القيود القانونية على استخدام التشفير الضرر بالأفراد والشركات والمنظمات الأخرى، بما في ذلك الحكومات، التي تتعرض بياناتها للجرائم الإلكترونية أو الاعتراض غير القانوني. سيؤدي ذلك إلى الحد من استثمارات الشركات التي تعتمد على حماية التشفير، كما سيحد من استخدام الأفراد للبيانات الشخصية، لأن الإنترنت سيكون أقل أمانًا وموثوقية.

التكنولوجيات الناشئة

يتناول هذا التقرير الاستجابات السياسية والتنظيمية لاثنين من التكنولوجيات الناشئة: الذكاء الاصطناعي والحوسبة السحابية والحوسبة الطرفية. نشأت هاتان التكنولوجيتان منذ سنوات، ولكن لم يتم نشرهما على نطاق واسع في جميع البلاد، وتخضعان لتغيرات مستمرة. وعلى الرغم من أن الذكاء الاصطناعي لا يعد تقنية جديدة، إلا أن الذكاء الاصطناعي التوليدي حظي باهتمام واسع النطاق منذ عامين فقط في نوفمبر ٢٠٢٢، مع طرح شات جي بي تي Chatgpt للجمهور. وبالمثل، تُعد الحوسبة السحابية شكلاً معروفا لاستضافة وتقديم المحتوى والخدمات، ولكنها لا تتواجد حاليا في جميع البلاد، ومن ناحية أخرى، يتطلب ظهور الحوسبة الطرفية وصولاً محليًا.

[2] للاطلاع على حالات استخدام أسلوب الإنترنت في تكوين الشبكات لحماية مسؤولية الوسيط، انظر https://www.internetsociety.org/resources/doc/2024/a-policy-framework-for-/internet-intermediaries-and-content

[3] لوصف التشفير، انظر https://www.internetsociety.org/issues/encryption/what-is/

إن اعتماد واستخدام هذه التكنولوجيات له تأثير كبير، ويتأثر بدوره بوجود أو غياب السياسات واللوائح ذات الصلة. في الوقت نفسه، قد تسعى الحكومات إلى الموازنة بين الحاجة إلى معالجة التأثير المحتمل لهذه

التكنولوجيات من جهة، والسعي إلى تشجيع الاستثمار والابتكار من جهة أخرى. يمكن أن يساعد التقييم باستخدام مجموعة الأدوات في تحقيق كلا الهدفين. يتم عرض التكنولوجيات هنا، ويتم عرض مجموعة الأدوات في القسم التالي.

الذكاء الاصطناعي

بينما يحظى الذكاء الاصطناعي بتأثير كبير وواسع الانتشار في مختلف المؤسسات والمجتمعات، فإننا نركز في هذه الدراسة على نوعين رئيسيين منه - أنظمة خبراء الذكاء الاصطناعي والذكاء الاصطناعي التوليدي - حيث يُرجّح أن يكون للأنظمة ذات الصلة تأثير أكبر.

تُساعد *أنظمة خبراء الذكاء الاصطناعي* أو تُأتمة عملية اتخاذ القرار البشري في مجال مُحدد. على سبيل المثال، يُمكنها مساعدة الأطباء في تشخيص أنواع مُحددة من مرض السرطان من خلال الصور، وفي وضع العلاجات. تُدرّب هذه الأنظمة باستخدام صور متاحة ومصنفة بمعلومات ذات صلة بالمريض حول مسار مرض السرطان، وبمُدخلات من خبراء مما يوفر قاعدة معرفية. تُقدّم أنظمة الذكاء الاصطناعي تلك مساعدة قيّمة للمهنيين الذين يتخذون قرارات صعبة، إلا أن قيمتها تعتمد على جودة بيانات التدريب.

يمكن للأنظمة التي تُحدّد البيانات اللازمة لتدريب أنظمة خبراء الذكاء الاصطناعي، مثل البيانات الصحية، أن تُحدّ من قيمة أنظمة الخبراء لمواطني تلك البلاد. وبالأخص، يُمكن أن تُقدّم أنظمة التشخيص الطبي تشخيصات غير صحيحة أو خطط علاج غير فعّالة، في حال وجود مرض مُتوطن في بلد أو منطقة لا تتوفر منها البيانات ذات الصلة. وقد ينتج عن ذلك أيضا عدم توفر نظام الخبراء الطبي أو استخدامه في تلك البلاد. ويعد ذلك مثالا لتأثير تفتيت الإنترنت، والذي قد يكون له آثارا ملموسة على المواطنين الذين قد يستفيدون من أنظمة الخبراء.

قد تستخدم أنظمة الخبراء الأخرى المعلومات الشخصية لتحديد هوية المستخدمين أو في أنظمة صنع القرار، بما في ذلك التوصيات والقرارات المالية. إذا تم ذلك دون علم المستخدمين أو موافقتهم، فإنه ينتهك حقوقهم في الخصوصية، وبمجرد فهمه، فإنه سيقوض الثقة في استخدام الإنترنت. يمكن للوائح الخصوصية معالجة هذا الأمر من خلال اشتراط الموافقة على استخدام البيانات الشخصية في مثل هذه الأنظمة أو تمكين المستخدمين من إلغاء تضمين بياناتهم فيها.

تتعلم *نماذج الذكاء الاصطناعي التوليدي* من بيانات التدريب المدخلة، ثم تُنشئ محتوى جديدًا، والذي يمكن أن يشمل النص والصوت والصور والفيديو والرموز الحاسوبية. تُنتج مجموعة فرعية من نماذج الذكاء الاصطناعي التوليدي، تُعرف باسم النماذج اللغوية الكبيرة، نصًا، ويمكن تدريبها على نص متاح لا يحتاج إلى تصنيف، وهي منهجية تُعرف أيضًا باسم التعلم غير الخاضع للإشراف. وبالتالي، يمكن استخدام جميع النصوص المتاحة على الإنترنت كبيانات تدريب، إلى جانب الكتب والنصوص الأخرى. قد تتطلب أشكال أخرى من الذكاء الاصطناعي التوليدي بيانات مصنفة، مثل التعرف على الصور.

تبرز مخاوف عديدة في ظل الزيادة السريعة في استخدام أنظمة الذكاء الاصطناعي التوليدي، والتسابق لتحديث الأنظمة الحالية وإدخال أنظمة جديدة. تتضمن تلك المخاوف احتمال انتهاك هذه الأنظمة لحقوق الطبع والنشر في بيانات التدريب، وإمكانية إنشاء صور أو مقاطع فيديو مزيفة لنشر معلومات مضللة وإمكانية استخدامها لإنشاء رسائل بريد إلكتروني عشوائية تحتوي على برامج ضارة لإصابة الأجهزة، وإمكانية "تخيل" نتائج خاطئة بشكل واثق ولا أساس له.

تدفع هذه المخاطر الحكومات إلى النظر في وضع لوائح أو إرشادات لأنظمة الذكاء الاصطناعي ذات الصلة. وقد اتخذ قانون الاتحاد الأوروبي للذكاء الاصطناعي بالفعل نهجًا لمواءمة مستوى اللوائح مع مخاطر الذكاء الاصطناعي، كما هو موضح أدناه. لا تزال بعض القضايا التنظيمية مطروحة، مثل إمكانية النظر في تدابير حماية مثل حماية مسؤولية الوسطاء، وفي هذه الحالة يطرح تساؤل حول طبيعة هذه التدابير والمسؤوليات المقابلة لمقدمي خدمات الذكاء الاصطناعي. ينبغي على الحكومات الاسترشاد بمجموعة أدوات مجتمع الإنترنت في تقييم التأثير المحتمل للوائح المقترحة على الإنترنت.

الحوسبة السحابية والحوسبة الطرفية

تُمكّن الخدمات السحابية المؤسسات من الوصول إلى البنية التحتية أو المنصات أو البرامج من خلال جهات خارجية، وتتيح المحتوى للمستخدمين عبر الإنترنت. يُقلل هذا من حاجة المؤسسات لاستضافة البرامج والمحتوى والخدمات ضمن بنيتها التحتية الخاصة، مما يُقلل من تكاليف الاستثمار والحاجة إلى معدات وكوادر بشرية واسعة، مع توفير حماية متطورة للأمن السيبراني. قد يجمع مقدمو الخدمات السحابية البيانات في موقع واحد أو عدة مواقع للمعالجة و/أو التخزين داخل منطقة معينة، وبالتالي قد لا تُستضاف في البلد الذي تُستمد وتُستخدم منه البيانات.

هناك امتدادات للحوسبة السحابية يُمكنهما نقل المحتوى أو الخدمات إلى بلاد أخرى ليكون الوصول إليها أقرب إلى المستخدمين. تُمكّن شبكات توصيل المحتوى (CDNs) مقدمي الخدمات من تخزين المحتوى الشائع مؤقتًا بالقرب من شبكات مقدمي خدمة الإنترنت أو بداخلها لتقليل تكلفة وزمن وصول إيصاله إلى المستخدمين. قد تُطوّر شركات الخدمات السحابية شبكات توصيل المحتوى الخاصة بها أو تستخدم شبكات توصيل المحتوى التابعة لجهات خارجية لتقديم المحتوى. تُقرّب الحوسبة الطرفية الوصول إلى الخدمات ذات الصلة من المستخدمين، خاصةً للخدمات منخفضة زمن الوصول مثل أتمتة المصانع أو المركبات ذاتية القيادة. تخزن شبكات توصيل المحتوى البيانات، بينما تعالج الحوسبة الطرفية البيانات - وكلاهما يستخدم الإنترنت لجلب البيانات ذات الصلة ثم تسليمها للمستخدمين النهائيين عند الحاجة.

قد تمنع اللوائح المستخدمين من الاستفادة الكاملة من الخدمات السحابية والمحتوى. وقد تمنع لوائح حوكمة البيانات أو الخصوصية التي تشترط توطين البيانات في بلد ما تجميع البيانات من قبل شركات الخدمات السحابية في المراكز الإقليمية، وقد تمنعها من الاستثمار في تلك البلد. قد تمنع القيود المفروضة على المحتوى تدفق البيانات إلى بلد ما، بينما قد يمنع نقص حماية مسؤولية الوسيط شركات الخدمات السحابية من استضافة المحتوى كوسطاء في تلك البلد. وأخيرًا، قد تؤثر القيود المفروضة على استخدام التشفير في تلك البلد على توافر أو استخدام خدمات السحابة، نظرًا لصعوبة حماية الخصوصية والتعرض للجرائم الإلكترونية.

إن القيود التنظيمية المفروضة على شركات الحوسبة السحابية، وما يقابلها من استخدام شبكات توصيل المحتوى أو الحوسبة الطرفية، قد تجعل الإنترنت في تلك الدولة أقل انفتاحًا، أو اتصالا بالعالم، أو أمانًا، أو موثوقية. ينبغي تقييم هذه القيود باستخدام مجموعة الأدوات المعروضة في القسم التالي.

مجموعة أدوات تقييم جمعية الإنترنت

تشكل مجموعة أدوات تقييم تأثير الإنترنت التابعة لجمعية الإنترنت الإطار التحليلي الذي تستند إليه النتائج والتوصيات الواردة في هذا التقرير. ويُعد فهم مكوناتها أمرًا أساسيًا لتقدير النهج المنهجي المُتبع لتقييم تأثير السياسات على الإنترنت.

تدعم جمعية الإنترنت أسلوب الإنترنت في تكوين الشبكات كركيزة لإنترنت قوي، لمناصرة القضايا التي تُعزز انفتاح الإنترنت، وترابطه العالمي وأمنه وموثوقيته. وتتحقق مجموعة أدوات تقييم تأثير الإنترنت الصادرة عن جمعية الإنترنت من تأثير اللوائح التنظيمية على الإنترنت لضمان تعزيزها لأسلوب الإنترنت في تكوين الشبكات، وذلك من خلال توفير إطار لتحليل التغييرات المقترحة في السياسات والتشريعات واللوائح والجوانب الأخرى التي تؤثر على الإنترنت.

يُحدد أسلوب الإنترنت في تكوين الشبكات خمس خصائص أساسية للإنترنت، إلى جانب عدد من عوامل التمكين لمساعدته على تحقيق مجموعة من الأهداف. تصف الخصائص الأساسية الأسس التي يحتاجها الإنترنت ليستمر في الوجود، بينما تصف العوامل المُمكّنة الظروف التي تُساعده على الازدهار.

على سبيل المثال، تخيل أن هناك مدينة، وبها مجموعة من البنى التحتية التي تُعرّف المدينة وتُمكّنها من البقاء مثل الطرق، والمواصلات العامة، وشبكات الصرف الصحي، والمطارات، ومنطقة الأعمال، والمساكن، والساحات، وما إلى ذلك. إلا أن ما يُسهم في ازدهار المدينة هو المتاجر والمطاعم والمكاتب والفنون والألعاب والحفلات الموسيقية، التي تملأ بنيتها التحتية بالأنشطة والناس. إذا عدنا إلى سنوات الإغلاق خلال الجائحة، نجد أن المدن استمرت في البقاء، إلا أن إغلاقها وإلغاء أنشطتها حال دون ازدهارها. ففي حقيقة الأمر، حل الإنترنت محل كل ما سُلب في هذه الفترة، ووفّر بعض الوسائل التي ساعدت الناس على الازدهار. وفي المقابل، ضمنت الخصائص الأساسية استمرار وجود الإنترنت، وساعدت عوامل التمكين على ازدهاره. إن الخصائص الأساسية التي تُعزز الإنترنت هي التي تجعله فريدا من نوعه وهي ضرورية لتطوره السليم وتحقيق فوائده، كما هو موضح في الجدول رقم ١.

الجدول رقم ١ : الخصائص الأساسية للإنترنت (المصدر: جمعية الإنترنت)

الخصائص الأساسية	الفوائد
1. بنية تحتية سهلة الوصول ببروتوكول مشترك مفتوح وذو عوائق دخول منخفضة.	يوفر الوصول غير المقيد والبروتوكولات المشتركة اتصالًا عالميًا ويشجع على نمو الشبكة. ومع تزايد عدد المشاركين، تزداد قيمة الإنترنت للجميع.

2. بنية مفتوحة لوحدات بناء قابلة للتشغيل البيني وإعادة الاستخدام، تستند إلى عمليات تطوير معايير مفتوحة يتبناها مجتمع المستخدمين طواعية.	تنشئ البنية المفتوحة خدمات مشتركة قابلة للتشغيل البيني، مما يتيح ابتكارًا سريعًا لا يتطلب الإذن في كل مكان. تضمن عملية التقييس الشاملة والاعتماد القائم على الطلب تبني التغييرات المفيدة، بينما تختفي التغييرات غير الضرورية.
3. إدارة لامركزية ونظام توجيه موزع واحد، قابل للتوسع وسريع.	يوفر التوجيه الموزع شبكة مرنة وقابلة للتكيف من الشبكات المستقلة، مما يسمح بإجراء تحسينات محلية مع الحفاظ على الاتصال العالمي.
4. مُعرّفات عالمية مشتركة واضحة وعالمية.	توفر مجموعة المُعرّفات المشتركة إمكانية عنونة متسقة ورؤية متماسكة للشبكة بأكملها، دون تفتيت أو تصدعات.
5. شبكة محايدة تكنولوجيًا، متعددة الأغراض، بسيطة وقابلة للتكيف	توفر العمومية مرونة. يخدم الإنترنت باستمرار مجتمعًا متنوعًا ومتطورًا باستمرار من المستخدمين والتطبيقات. ولا يتطلب دعم هذه البيئة الديناميكية تغييرات كبيرة.

علاوة على ذلك، يمكن لعوامل التمكين مساعدة الإنترنت على تحقيق مجموعة من الأهداف، كما يلي.

الجدول رقم ٢: عوامل تمكين شبكة إنترنت مفتوحة، ومتصلة عالميًا، وآمنة، وموثوقة (المصدر: جمعية الإنترنت)[4]

الأهداف	**عوامل التمكين**
إنترنت مفتوح يُتيح للجميع المشاركة دون قيود، ويتيح الاستخدام، والابتكار، وتنمية الإنترنت واستدامته كقوة للخير	· وصول سهل وغير مُقيد للشبكات والمستخدمين · استخدام ونشر غير مُقيد لتقنيات ومعايير الإنترنت · تطوير وإدارة وحوكمة تقنيات ومعايير الإنترنت بشكل تعاوني

[4] لمزيد من التفاصيل، انظر https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

إنترنت مُتصل عالميًا، شامل، يُتيح للجميع التواصل دون قيود جغرافية، واستخدام كامل إمكانات الشبكة	· إمكانية وصول غير مقيدة، ليتمكن المستخدمون من الوصول إلى جميع الموارد والتكنولوجيات المتاحة على الإنترنت · سعة متاحة، كافية لتلبية احتياجات المستخدمين، بما في ذلك المنافذ، وعرض النطاق الترددي، والخدمات
إنترنت آمن يتمكن من مواجهة الهجمات، ويُساعد الجميع في الحفاظ على سلامة البيانات وسريتها. كما يعني الإنترنت الآمن أن استخدامه لا يُسبب أي انعدام للأمن، مثل شبكات الروبوتات المُستخدمة في عمليات التصيد الاحتيالي.	· سرية بيانات المعلومات والأجهزة والتطبيقات، والتي تتم عادة باستخدام التشفير لحماية البيانات في أثناء النقل وفي حالة السكون · سلامة المعلومات والتطبيقات والخدمات، بحيث لا يتم تعديل البيانات أثناء النقل أو السكون، ولا يمكن التلاعب بالخدمات.
إنترنت موثوق يُمكن للناس الاعتماد عليه، بحيث يمكن أن يكون الإنترنت قاعدة للخدمات العالمية، من الترفيه إلى التجارة إلى المعلومات	· موثوقية ومرونة وتوافر، لتقديم الخدمات كما وعُد، حتى في ظل التحديات. · المساءلة، التي تُطمئن المستخدمين بأن الجهات تعمل بشفافية وعدالة · الخصوصية، التي تُمكن الأفراد والمجموعات من فهم المعلومات التي تُجمع عنهم والتحكم فيها، وكيفية استخدامها.

تتحقق مجموعة أدوات تقييم تأثير الإنترنت من آثار اللوائح على الإنترنت بطريقتين: تحديد آثار اللوائح على الخصائص الأساسية للإنترنت بهدف الحفاظ على القيمة الفريدة للإنترنت، وتحليل تأثير اللوائح على عوامل التمكين للمساعدة في فهم الآثار الناتجة عن إنترنت مفتوح، ومتصل عالميًا، وآمن، وموثوق. إن الهدف الشامل هو مساعدة أصحاب المصلحة في مجال الإنترنت على تحديد الآثار المحتملة للسياسات واللوائح، سواءً كانت إيجابية أو سلبية، ليتمكنوا من اتخاذ قرارات أكثر استنارة.

تقدم الأقسام التالية أمثلة دولية على اللوائح ذات الصلة بالذكاء الاصطناعي والحوسبة السحابية والحوسبة الطرفية عالميًا، وتحدد اللوائح المقترحة أو الحالية في دول الشرق الأوسط وشمال إفريقيا الست، وتستخدم مجموعة الأدوات لتقييم تلك اللوائح وتقديم التوصيات.

السياسات واللوائح التنظيمية

يعرض هذا القسم بعض من أبرز الأمثلة الدولية على السياسات واللوائح التنظيمية التي يتناولها هذا التقرير قبل دراسة القوانين في كل من الدول محط الدراسة.

أمثلة دولية

حوكمة البيانات

إحدى النقاط المهمة في حوكمة البيانات تتعلق بنقل البيانات خارج البلاد. وهذا أمر مفهوم، حيث إن هذه العمليات أصبحت شائعة بشكل متزايد، نتيجة الزيادة في التفاعلات العابرة للحدود بين الأفراد والمنظمات، وكذلك عندما تقوم شركات الخدمات السحابية بتجميع البيانات لمعالجتها و/أو تخزينها. وفي حين أن بعض الدول مازال لا يوجد لديها قوانين تنظم مثل هذه التحويلات، مما يسمح بتدفق البيانات عبر الحدود بحرية، فرضت دول أخرى قوانين توطين بيانات على فئات معينة من البيانات التي لا تسمح بمثل هذا النقل. وبين هذا وذاك، تفرض العديد من القوانين حول العالم قيودًا على القدرة على إجراء عمليات نقل بيانات عبر الحدود، وذلك لضمان أن تكون حماية البيانات في البلد الوجهة ملتزمة بالمتطلبات القانونية التي تفرضها قوانينها المحلية.

فعلى سبيل المثال، تشترط اللائحة العامة لحماية البيانات للاتحاد الأوروبي (GDPR) وجود ضمانات كافية لنقل البيانات خارج المنطقة الاقتصادية الأوروبية (EEA). ويأتي برنامج إطار خصوصية البيانات الخاص بالولايات المتحدة الأميركية والاتحاد الأوروبي والمملكة المتحدة وسويسرا كمثال دولي لافتاً للنظر، جاء كنتاج للائحة العامة لحماية البيانات الخاصة بالاتحاد الأوروبي، وهو برنامج يسعى إلى تحقيق توازن بين الحاجة إلى التحكم في عمليات نقل البيانات عبر الحدود وبين الحاجة إلى تسهيل نقل البيانات لهيئات الأعمال لكي تتمكن من تقديم خدمات عبر الحدود. يهدف هذا البرنامج إلى تسهيل نقل البيانات من أوروبا إلى الولايات المتحدة مع الامتثال لمبادئ حماية البيانات في الاتحاد الأوروبي والمملكة المتحدة وسويسرا باستخدام نظام الاعتماد الذاتي self- certification الذي يسمح للشركات بنقل البيانات إلى الولايات المتحدة إذا امتثلت لمبادئ هذا الإطار.

الخصوصية

في السنوات القليلة الماضية، شهدت منطقة الشرق الأوسط وشمال أفريقيا تطورات كبيرة في تنظيم الخصوصية حيث أصدرت العديد من الدول قوانين لحماية البيانات الشخصية لأول مرة أو أدخلت تلك القوانين حيز التنفيذ. بالإضافة إلى حماية البيانات في حالة السكون، وبجانب أي قيود مفروضة على نقل البيانات، فإن هذه القوانين توفر حماية ضرورية ضد إساءة استخدام البيانات الشخصية لمستخدمي الإنترنت من خلال مطالبة الشركات بالحصول على موافقة قبل معالجة أي بيانات.

إلا أنه ما زالت هناك فجوات في بعض القوانين فيما يتعلق باستخدام البيانات الشخصية فيما يخص الممارسات الجديدة مثل التنميط الآلي. ومن الأمثلة الدولية الجيدة التي تحاول سد هذه الفجوة هو أيضاً الـ GDPR ، الذي ينظم التنميط الآلي ويتطلب توفر الشفافية بشأن كيفية استخدام التنميط لتقييم سلوك الشخص وتوقعه. ورغم أنه لا يُحظر تمامًا، يحد GDPR من استخدام التنميط لاتخاذ قرارات آلية تؤثر بشكل كبير على الأفراد ويمنح الأفراد الحق في الاعتراض على معالجة بياناتهم بهذه الطريقة.

مسئولية الوسطاء

في الأيام الأولى للإنترنت التجاري، أصدرت المحاكم الأميركية حكمين منفصلين بشأن محتوى تشهيري تم عرضه من قبل مستخدمين على لوحات إعلانية الكترونية، كانت من أوائل أشكال المنصات الوسيطة. ووفقا لهذه الأحكام فإن اللوحات الإعلانية لا تعد مسئولة عن المحتوى التشهيري وذلك لعدم قيامها بفلترة المنشورات الالكترونية، بينما تعد اللوحات الالكترونية التي تقوم بفلترة المحتوى مسئولة قانونياً عن المحتوى الذي يتم تقديمه من خلال خدماتها. وقد شجعت هذه القرارات على تجنب المنصات القيام بفلترة المحتوى لتجنب المسائلة

القانونية، وهو الأمر غير المرغوب فيه، ومن ثم قام الكونجرس الأمريكي بتبني قوانين تنص على حماية مسئولية الوسطاء مما أدى بدوره إلى نمو وتنوع المنصات كما نراها اليوم.

لتمكين حرية التعبير للأفراد، اتجه الكونجرس الأمريكي لحماية الوسطاء الكترونياً فيما يتعلق بمحتوى الأطراف الثالثة. وهذا التحول قد تم من خلال ما يعرف باسم " القسم 230" من قانون الاتصالات الأمريكية، والقسم 512 الخاص بحقوق النشر من قانون حقوق النشر للألفية الرقمية. يحمي القسم 230 من قانون أدب الاتصالات المنصات من المساءلة القانونية عن معظم المحتوى، بما في ذلك المحتوى الإجرامي، إلا في حالة قيام الوسيط بإنشاء المحتوى. لا يفرض القسم 230 أي إلزام لحذف المحتوى. كما يوفر قانون حق النشر للألفية الرقمية أيضا "مساحة آمنة" مماثلة (القسم 512) لمواجهة التعدي على حق النشر. المنصات التي تتبع اجراءات قانون حق النشر للألفية الرقمية وتقوم بحذف المحتوى السيئ يمكنها أن تتجنب المساءلة القانونية عن انتهاك مستخدميها لحق النشر. هذه القوانين تمكن المنصات من العمل والازدهار دون وجود تحديات قانونية مستمرة ودون المخاطرة بالتعرض لمسئولية مالية مدمرة.

التشفير

معظم الدول حول العالم لا تقوم بتقييد القدرة على استخدام تكنولوجيات التشفير. إلا أنه قد توجد بعض اللوائح التنظيمية، مثل القيود التي تفرض على قدرة التشفير، أو المتطلبات التي تفرض على الشركات للمساعدة على فرض القانون فيما يتعلق بفك التشفير. وتسعى الدول لتحقيق التوازن لأهمية الحفاظ على فوائد أمن الإنترنت التي يحققها التشفير والتي تساعد في الترويج للإنترنت الآمن والموثوق.

بالإضافة إلى الفئات الأربعة من القوانين المذكورة آنفا والتي تؤثر على التكنولوجيات الناشئة، بدأت الدول في وضع لوائح تنظيمية تركز على الذكاء الاصطناعي بشكل مباشر. فعلى سبيل المثال وكما يتضح فيما يلي، تبنى الاتحاد الأوروبي مؤخرا قانون ذات صلة.

اللائحة التنظيمية للذكاء الاصطناعي

في عام 2024، تبنى الاتحاد الأوروبي قانون الذكاء الاصطناعي الخاص بالاتحاد الأوروبي بشكل رسمي، والذي بُني على أساس حساب المخاطر وهو ينظم الذكاء الاصطناعي من وجهة نظر سلامة المنتج. ومن خلال هذا النهج، يتم منع أي تكنولوجيا للذكاء الاصطناعي تسفر عن مخاطر غير مقبولة، أما التكنولوجيات التي تنطوي على مخاطر بسيطة فلا تخضع لهذا التنظيم، ويتم تحديد خطورة التكنولوجيات سواء عالية المخاطر أو ذات المخاطر المحدودة في إطار تنظيمي مخصوص. يكون التركيز الأساسي لهذه التنظيمات على مقدمي خدمات نظام الذكاء الاصطناعي، والملتزمين بضمان الجودة والشفافية والرقابة البشرية والأمن. في بعض الحالات الخاصة، قد يطلب تقديم تقييم لأثر الحقوق الأساسية. يفرض قانون الذكاء الاصطناعي التابع للاتحاد الأوروبي غرامات قد تصل الى 35 مليون يورو. وسيدخل هذا القانون حيز التنفيذ بعد عامين، وسيستغرق الأمر بعض من الوقت لتقييم مدى نجاح القانون في حماية مستخدمي تكنولوجيا الذكاء الاصطناعي.

اللوائح التنظيمية في الدول محل الدراسة

يتناول هذا القسم بمزيد من التفصيل القوانين واللوائح التنظيمية لدول ست يتطرق لها هذا التقرير وهذه الدول هي البحرين، ومصر، والأردن، وعمان، والمملكة العربية السعودية، والإمارات العربية المتحدة، ويتناول

التقرير طريقة تناول هذه الدول لتنظيم حوكمة البيانات والخصوصية ومسئولية الوسطاء والتشفير فيما يتعلق بالتكنولوجيات الناشئة.

البحرين

في مجال **حوكمة البيانات**، فإن البحرين لديها إطار موسع ينظم استخدام البيانات من خلال قانون حماية البيانات الشخصية لعام 2018 بجانب مجموعة من القرارات التي أصدرتها وزارة العدل، والشئون الدينية والأوقاف، والتي تغطي قضايا مثل حقوق أصحاب البيانات، وقواعد معالجة البيانات الحساسة، وآليات الشكاوى، وقواعد تحويل البيانات الشخصية خارج البحرين. هذه الأدوات القانونية تهدف إلى تحقيق التوازن بين التدفق الحر للبيانات من ناحية وضمان حماية تلك البيانات بشكل كاف من ناحية أخرى.

ومن الأساليب التي تتبعها البحرين لخلق هذا التوازن هو فرض القيود على نقل البيانات الشخصية خارج البحرين وذلك بموجب المادة 12 من قانون حماية البيانات الشخصية لعام 2018. بموجب هذه المادة، يحظر نقل البيانات الشخصية خارج البحرين إلا في أحد الحالات التالية:

1- أن يتم نقل البيانات إلى دولة أو منطقة مدرجة في سجل تديره وتحدثه الهيئة المعنية، وأن يضم هذا السجل الدول والمناطق التي ترى الهيئة أنها توفر حماية تشريعية وتنظيمية كافية للبيانات الشخصية، وذلك بقرار من الهيئة. هذا السجل يتم نشره في الصحيفة الرسمية.

2- أن يتم نقل البيانات بموجب إذن من الهيئة وتدرس على أساس كل حالة على حدة بشرط أن تكون البيانات خاضعة لمستوى معين من الحماية. وهذا المستوى من الحماية يقيم في ضوء الظروف المحيطة بعملية نقل البيانات، والتي تتضمن ما يلي:

أ- طبيعة البيانات التي يتم نقلها، والغرض منها وفترة التشغيل

ب- الدولة أو المنطقة منشأ البيانات، ووجهتها الأخيرة، والإجراءات المتاحة في هذه الدول والمناطق لحماية البيانات الشخصية، و

ج- الاتفاقيات والتشريعات الدولية ذات الصلة التي يتم تنفيذها في الدولة أو المنطقة، التي يتم نقل البيانات إليها.

التفويض المذكور قد يعتمد على بعض الشروط أو قد يكون لفترة زمنية محددة''.

أتاح هذا التوجه نقل البيانات الشخصية البحرينية خارج الدولة في حالة أن تكون عملية النقل تتم لدولة على "القائمة البيضاء" والتي تم وضعها وفقا للمادة 12 (1) المذكورة أعلاه، أو في حالة نقل البيانات لدولة تسمح لها السلطات البحرينية ذلك، بعد دراسة كل حالة على حدى. وعلى الرغم من أن هذا التوجه قد يبدو معقولاً، إلا أنه ما زال ينطوي على عدد من القيود على عملية التدفق الحر للبيانات عبر الحدود، خاصة في حالة أن تكون الدولة المعنية غير مدرجة على القائمة البيضاء أو أن يتطلب ذلك موافقة محددة من السلطات البحرينية. لا يوجد سجل عام لعدد الطلبات التي تم تقديمها للحصول على مثل هذه الموافقات أو لنتائج هذه الطلبات. ويوصى بأن تقوم دولة البحرين بإعادة النظر في قواعد موقع البيانات التي ينص عليها القانون البحريني لحماية البيانات بحيث يسمح بتدفق البيانات بشكل حر بين البحرين ودول أخرى على شرط أن يكون لديها مستويات ملائمة من حماية البيانات.

تمتلك البحرين إطارا معقدا **للخصوصية** من خلال قانون حماية البيانات الشخصية وقرارات تنفيذه الصادرة عن وزارة العدل، والشئون الدينية والأوقاف. وعلى الرغم من أن قانون البحرين لحماية البيانات الشخصية يعد واحد

من أوائل قوانين حماية البيانات في المنطقة إذ تم إصداره عام 2028، فإنه يشمل بالفعل بنود لحماية الأفراد من أن يتعرضوا لقرارات تتخذ من خلال أدوات آلية، وذلك لأن القانون يعطي الحق، بمقتضى المادة 22، الحق في الاعتراض على القرارات التي تتم من خلال عمليات التشغيل الآلي لو كانت هذه القرارات مرتبطة بالأداء في العمل، أو بالموقف المالي، أو بالاستحقاق الائتماني للشخص، ويعطي أيضاً الشخص الحق في اعادة النظر في القرارات باستخدام وسائل ليست آلية بالكامل.

فيما يتعلق **بمسئولية الوساطة**، فإن الإطار القانوني الحالي في البحرين يمكن اعتباره واحد من أكثر الآليات تعقيداً في المنطقة وذلك بسبب وجود بعض البنود في قانون حق النشر البحريني لعام 2006 والذي يمنح الحماية لمقدمي الخدمات من المسائلة القانونية عن الأعمال المدنية التي يقوم المستخدمين من خلالها بانتهاك حق النشر، وذلك في حالة أن يقوم الوسيط بالإيفاء بشروط معينة تعتمد على دور الوسيط في تشغيل المواد المسيئة، مثل أن يكون بث المواد التشهيرية لم يبدأ ولم يتم تحت إشراف الجهة الوسيطة أو ألا يقوم الوسيط باختيار المحتوى أو مستقبلي المحتوى. إلا أن البحرين لم يقم حتى الآن بتقديم حماية أكثر شمولية للوسيط من المسائلة القانونية عن محتوى الطرف الثالث. هذه الشروط توفر ثقة قانونية لمقدمي خدمات الاستضافة، ولمنصات التواصل الاجتماعي ولغيرها من الوسطاء، في توفير الحماية ضد المساءلة المدنية عن محتوى الطرف الثالث الذي يتم رفعه على الخوادم أو المنصات، وهو الأمر الذي يعد أداة تمكين للأعمال الموجودة في البحرين لإنشاء خدمات ومنصات استضافة محلية وغيرها من خدمات الوساطة المبتكرة.

بدون هذه الحماية يتم إعاقة الابتكار المحلي وتقويض الاستثمار الأجنبي ويُحرم المستخدمين المحليين من الوصول للمنصات ذات الصلة التي تخرج بدورها من السوق، وذلك في مقابل أن يكون هناك مبادئ واضحة للإنترنت الحر والمفتوح. ولكي يتمكن مقدمو خدمة الاستضافة وغيرهم من المنصات من العمل بثقة قانونية في البحرين، فإنه من المهم أن تقوم البحرين بالنظر في طرح إطار شامل لحماية هذه الكيانات من المساءلة عن محتوى الطرف الثالث.

إن استخدام **التشفير** في البحرين لا يخضع للتنظيم، ومن ثم لا يبدو أن هناك قيود على استخدامه خارج إطار قانون الجريمة السيبرانية الذي يمنع استخدام التشفير (كخطوة تصعيدية) بهدف ارتكاب أو إخفاء جريمة ما.

يدعم تنظيم شئون الخصوصية والتشفير في البحرين مبادئ الإنترنت المفتوح المتصل عالميا، والآمن والموثوق، بينما تتناول التوصيات الخاصة بنا أمور حوكمة البيانات الحالية وأوضاع مسئولية الوسطاء.

مصر

في مجال **حوكمة البيانات**، يقدم القانون المصري لحماية البيانات الشخصية لعام 2020 إطارا شاملا لحماية الخصوصية وحوكمة استخدام البيانات الشخصية. إلا أن الفصل السابع من هذا القانون، والذي يسمى "عمليات نقل البيانات الشخصية عبر الحدود" ينص في المادة الرابعة عشر على أن "عملية نقل البيانات الشخصية، والتي يتم تجميعها أو تجهيزها بهدف التشغيل، إلى بلد أجنبي، أو تخزينها أو مشاركتها، يمكن تنفيذها فقط في حالة أن يكون مستوى حماية أو أمن البيانات في الدولة الأجنبية يتساوى مع (أو يتفوق على) المتطلبات التي يضعها هذا القانون، وبشرط الحصول على رخصة أو إذن ذات صلة من المركز"

هذه القيود الخاصة بالحصول على رخص أو أذون من الحكومة قبل نقل البيانات للخارج لا تتماشى مع أفضل الممارسات المنصوص عليها في القوانين العالمية بما في ذلك قوانين الدول الأخرى في المنطقة. كما أن فرض هذه القيود يمثل صعوبة على مقدمي الخدمات لتجميع البيانات من مختلف الدول، الأمر الذي يؤدي إلى تفتيت الإنترنت. كما يمكن لهذه القيود أن تصعب الأمر على مقدمي وتطبيقات الخدمات السحابية الأجنبية للالتزام بالقانون، الأمر الذي يحد بدوره من الاستثمار ومن قدرة المستخدمين في مصر على الاستفادة بهذه الخدمات،

وهو ما يتعارض مع المبادئ الأساسية للإنترنت الحر والمفتوح. ومن ثم نوصي أن تقوم مصر بإعادة النظر في قوانين موقع البيانات الموجود في الفصل السابع من القانون المصري لحماية البيانات بالشكل الذي يسمح للبيانات بالحركة بين مصر ودول أخرى على شرط أن يكون لدى هذه الدول مستوى ملائم من حماية البيانات دون الحاجة للحصول على ترخيص.

كما ذكر آنفا، فإن القانون المصري لحماية البيانات الشخصية يطرح إطارا شاملا لحماية الخصوصية كما يضمن الحقوق الرئيسية لأصحاب البيانات، إلا أن هذا القانون يفتقر إلى تناول التحديات التي تواجه الخصوصية وتنشأ بسبب الذكاء الاصطناعي وعمليات صنع القرار الآلية، وذلك لأنه يفتقر إلى وجود شروط محددة لحماية الأفراد من التحيز والتفرقة اللوغاريتمية، خاصة في مجالات مثل التوظيف والجدارة الائتمانية. هذا الافتقار للحماية يضع حقوق خصوصية المستخدمين في خطر ويقلل من الثقة في الإنترنت.

ومن أجل ضمان توفير حماية قوية **للخصوصية** في العصر الرقمي الذي نحياه، يجب أن تقوم مصر بتضمين بنود في قانون حماية البيانات الشخصية للحماية من عمليات التشغيل والتنميط الآلية، بهدف حماية الخصوصية، وتمكين المستخدمين من فهم أو التحكم في طريقة استخدام البيانات.

في مجال **مسئولية الوسطاء**، فإن قانون المصري للجريمة السيبرانية به عدد من البنود التي تعتبر مالك المنصة مسؤول عن المحتوى الذي يتم نشره من قبل طرف ثالث، ومن ثم يمكن أن يكون عرضة للعقاب إذا كان على علم بوجود هذا المحتوى الإجرامي ولم يقم بإبلاغ السلطات أو قام بتسهيل حدوث ذلك. وبالمثل فإن مصر لا تمتلك إطارا للحد من المسئولية المدنية لمالك الموقع الالكتروني عن انتهاكات الملكية الفكرية التي يقوم طرف ثالث بإضافتها على المنصات.

ونتيجة ذلك، فإن إنشاء وإدارة المنصات في مصر التي تسمح للمستخدمين بتحميل ومشاركة المحتوى أصبح أمرا يحمل مخاطرة لمالكي ومديري تلك المنصات، لأنهم سيكونوا مطالبين بمراقبة كل محتوى تم وضعه على المنصة، وإلا سيكونون معرضين للمسائلة، وهو الأمر الذي يستحيل المحافظة عليه. ومن ثم أصبح الأمر يحمل مخاطرة قانونية كبيرة على المصريين أن يقوموا بإنشاء بدائل لمنصات التواصل الاجتماعي مثل فيسبوك، ومنصة اكس، ويوتيوب، أو انستجرام، ويخلق نوع من أنواع عدم الثقة في هذه المنصات، وهو ما يتعارض مع مبادئ الإنترنت الحر والمفتوح. ويوصى بأن تقوم مصر بالنظر في وضع إطار قانوني لحماية منشئي ومديري المنصات من المساءلة عن محتوى الأطراف الثالثة.

وأخيرا، فإن مصر من الدول القليلة في المنطقة التي يستلزم الأمر بها الحصول على إذن من الحكومة قبل استخدام تكنولوجيا **التشفير**. وهو ما تنص عليه المادة 64 من قانون الاتصالات لعام 2003 والذي ينطبق على كل مستخدمي خدمات الاتصالات بما في ذلك شركات الإنترنت:

"إن مقدمي خدمات تكنولوجيا الاتصالات، ومقدمي الخدمات، وموظفيهم ومستخدمي هذه الخدمات لا يحق لهم استخدام أدوات تشفير خدمات الاتصالات دون الحصول على موافقة كتابية من كل من جهاز تنظيم الاتصالات والقوات المسلحة والأمن الوطني."

إن هذه القيود على استخدام التكنولوجيا يضع مستخدمي الإنترنت في مخاطرة، حيث أن التشفير هو أمر أساسي لتحقيق التشغيل الآمن للإنترنت، وهو أمر أساسي أيضاً لإتمام عمليات الدفع وتوثيق المستخدمين، وحماية البيانات بشكل عام عند النقل أو عند السكون. إن غياب التشفير يهدد أمن واستقرار وأمان الأفراد. بالإضافة إلى ذلك، فإن هذه الشروط تقيد من قدرة الشركات المحلية في مصر على الابتكار في مجال الأمن السيبراني، وذلك

لصعوبة الحصول على الموافقة الحكومية المطلوبة لاستخدام التشفير، وتضع قيود على الاستثمارات الخاصة بهذه الشركات مثل شركات الخدمات السحابية، التي يحتاج عملائها إلى تشفير البيانات الشخصية والحساسة الخاصة بهم. ومن ثم يوصى أن تقوم مصر بإزالة القيود على القدرة على استخدام التشفير بحيث لا يؤثر القانون على أمن وموثوقية الإنترنت.

الأردن

قامت الأردن مؤخرا بإصدار قانون جديد لحماية البيانات الشخصية وقامت بإصدار اللائحة التنظيمية الخاصة به، وهذا القانون ينص على الكثير من مبادئ **حوكمة البيانات** المعترف بها، مما يوازن بين التدفق الحر للبيانات من ناحية وضمان حماية البيانات بشكل كاف من ناحية أخرى. وهو ما يتماشى مع أفضل الممارسات الدولية مثل اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي، ومما يبدو أن القانون لا يفرض أي قيود حازمة على التدفق الحر للبيانات.

أما فيما يتعلق ب**الخصوصية**، فإن القانون الأردني يتضمن أيضا الحق في الموافقة على استخدام البيانات الشخصية، والحق في الوصول للبيانات الشخصية والحق في طلب مسح البيانات الشخصية. كما يتناول هذا القانون أيضا مبدأ "التنميط" وهو الإجراء الذي يفرض تحديات جديدة على المستخدمين في عصر الذكاء الاصطناعي. إلا أن الشروط التي تتعلق بالتنميط محدودة حيث تتمثل فقط في حق الاعتراض لو تطور الأمر لأكثر من الهدف الذي تم بسببه تجميع البيانات، أو في حالة أن يشتمل الأمر على أي تفرقة. ويقع هذا ضمن إطار الحماية التي تقدمها بعض القوانين المتطورة والتي تعطي صاحب البيانات الحق في ابلاغه عن إجراء التنميط ويحق له المطالبة بأن يتم إعادة النظر في أي قرار يتم اتخاذه إزاء البيانات الخاصة به بسبب التنميط، وذلك عن طريق استخدام وسائل أخرى غير التنميط الآلي، وإضافات تضمن موثوقية الإنترنت. ومن الموصى به أن تقوم الأردن بإعادة النظر في الشروط التي تتعلق بالتنميط، مثل ابلاغ أصحاب البيانات بالتنميط، والسماح لأصحاب البيانات بالاعتراض على القرارات التي يتم اتخاذها من خلال التنميط، وفرض إجراءات اضافية لتصحيح هذه القرارات.

في مجال **مسئولية الوسطاء**، فإن القانون الأردني للجريمة السيبرانية يفرض مسؤولية صارمة ضد الشخص المسئول عن الموقع الالكتروني أو عن منصة التواصل الاجتماعي عن المحتوى الذي يتم نشره على هذا الموقع أو المنصة، حتى لو تم نشر أو إنشاء هذا المحتوى من قبل طرف ثالث. وبالمثل فإن الأردن ليس لديها إطار محدد لتقييد المسئولية المدنية لمالك الموقع أو المنصة، والمتعلقة بانتهاك حق النشر، عن المحتوى الذي ينشره الأطراف الثالثة على المواقع أو المنصات الخاصة بهم، وهو الأمر الذي يجعل من إنشاء وإدارة المواقع والمنصات في الأردن أمرا خطراً لما يتطلبه ذلك من مراقبة كل محتوى منشور على المنصة وإلا يتعرض ملاك ومديري المواقع للمساءلة. إن الحفاظ على ذلك أمر صعب ومكلف وبالتالي يكون من المستحيل أن يقوم الأردنيون بإنشاء بدائل لمنصات التواصل الاجتماعي مثل فيسبوك، ومنصة اكس، ويوتيوب، أو انستجرام دون أن يضعوا أنفسهم في خطر المساءلة القانونية. وهو ما يتعارض مع مبادئ الإنترنت المفتوح والحر. ويوصى بأن تقوم الأردن بوضع إطار قانون لحماية الوسطاء من المساءلة عن محتوى الطرف الثالث.

إن استخدام **التشفير** في الأردن لا يخضع لأي لوائح تنظيمية ولا يبدو أن هناك قيود على استخدامه.

إن تنظيم حوكمة البيانات والتشفير في الأردن يدعم مبادئ الإنترنت المفتوح والمتصل عالمياً والآمن والموثوق، وتتناول توصياتنا الأوضاع الحالية لمسئولية الوسطاء والخصوصية.

عمان

في مجال **حوكمة الإنترنت**، فإن القانون العماني الصادر مؤخرا بخصوص حماية البيانات الشخصية لا يفرض أي قيود صارمة على القدرة على نقل البيانات الشخصية خارج الدولة. فهو يتطلب أن يضمن مسئول البيانات أن يكون لدى الدولة التي يتم نقل البيانات إليها مستوى من الحماية مماثل لما يقدمه القانون العماني.

وعلى صعيد آخر، فإن عمان تمتلك عدد من التنظيمات القطاعية الخاصة بمتطلبات توطين البيانات والتي تشترط أن يتم تخزين البيانات محليا داخل الدولة. فعلى سبيل المثال، فإن اللائحة التي تنظم تقديم خدمة اتصالات الصوت أو الفيديو من خلال بروتوكول الإنترنت والتي أصدرتها هيئة تنظيم الاتصالات عام 2022 تتطلب في المادة 12 ما يلي " أن يكون مقر مراكز البيانات الخاصة بالبيانات الشخصية للمستفيد موجودة ومحتفظ بها داخل الحدود الجغرافية لسلطنة عمان." مما يعني أن مقدم خدمات تطبيقات الاتصالات عبر الصوت والفيديو مثل زووم يشترط أن تقوم بتخزين البيانات الخاصة به في عمان، حتى يمكن أن يقوم بتقديم الخدمات في عمان. بالمثل فإن اللائحة التنفيذية للقانون العماني الخاص بالنقل عبر الأراضي والذي أصدرته وزارة النقل والاتصالات عام 2018 لديه فصل مخصص لحوكمة تطبيقات النقل والتي يتطلب أن تكون البيانات الخاصة بهذا التطبيقات داخل الدولة.

هذه التنظيمات تجعل الأمر صعبا للغاية لبعض من أكثر التطبيقات انتشارا في العالم في أن تلتزم بالقانون العماني وذلك مثل تطبيق فيس تايم، وواتس آب، وأوبر، وبالتالي فإن هذه التطبيقات ممنوع استخدامها في عمان. وهذا يحد من قدرة المستخدمين في عمان على الاستفادة من هذه التطبيقات، ويتعارض مع المبادئ الأساسية للإنترنت الحر والمفتوح. يجب على عمان أن تنظر في تطبيق القانون العام لحماية البيانات على خدمات نقل الصوت عبر الإنترنت وبيانات النقل حتى يمكن نقل البيانات لخارج البلاد في حال توفر الشروط الملائمة، وذلك لتمكين الوصول بشكل كامل للتطبيقات ذات الصلة والايفاء بهدف الوصول إلى تحقيق إنترنت متصل عالمياً.

أما في مجال **الخصوصية**، فإن قانون حماية البيانات الشخصية واللائحة التنظيمية الخاصة به يعترف بالحقوق الأساسية للخصوصية مثل حق الحصول على الموافقة على استخدام البيانات الشخصية، وحق الوصول للبيانات الشخصية، وحق طلب حذف البيانات الشخصية. وهذا يتماشى مع أفضل الممارسات الدولية مثل اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي. إلا أن هذا القانون الجديد لا يتطرق لبعض من التحديات الجديدة التي تواجه المستخدمين في عصر الذكاء الاصطناعي، ولا يتضمن أي شروط خاصة بالاستخدام الآلي للبيانات الشخصية من خلال استخدام الذكاء الاصطناعي، ولا الحق في الإبلاغ عن استخدام تنميط التكنولوجيات في مجالات مثل التوظيف والتعليم. إن غياب الحماية فيما يتعلق بهذه الاستخدامات الجديدة للبيانات الشخصية يمكن أن يضع حقوق خصوصية المستخدمين في خطر، كما أنه لا يتماشى مع أفضل الممارسات الدولية في هذا المجال، بما في ذلك قوانين بعض الدول الأخرى في المنطقة. ومن الموصى به أن تقوم عمان بطرح شروط

للحماية ضد الاستخدام والتنميط الآلي للبيانات بهدف حماية الخصوصية وتمكين المستخدمين من فهم والتحكم في طريقة استخدام البيانات الخاصة بهم.

فيما يتعلق **بمسئولية الوسطاء**، فإن عمان مثلها في ذلك مثل البحرين، هي واحدة من الدول القليلة في المنطقة التي لديها قوانين محددة تتناول مسئولية الوسطاء في حماية الملكية الفكرية، مما يوفر الحماية للمنصات مثل يوتيوب وغيرهم فيما يتعلق بمحتوى الأطراف الثالثة. هذه القاعدة قد تم إصدارها بمقتضى قرار هيئة تنظيم الاتصالات رقم 151 لعام 2008 والخاص فيما يتعلق بمسئولية مقدم الخدمة عن المحتوى الإلكتروني على الإنترنت. ووفقا لهذا القرار، فإنه يمكن حماية الوسطاء من المسائلة عن المحتوى الذي ينتهك الملكية الفكرية طالما أن المحتوى تم تحميله من قبل طرف ثالث، ولا يتم تعديله من قبل الوسيط، ويتم حذف من قبل الوسيط فور الإبلاغ عن وجود محتوى تشهيري من قبل صاحب الحق في الإبلاغ.

إلا أن عمان لا تمتلك شروط قانونية واضحة تحد من مسئولية الوسطاء عن المحتوى التشهيري وغيره من المحتوى غير القانوني بخلاف انتهاكات الملكية الفكرية. إن غياب هذه القواعد يعرض المنصات لمواجهة خطر حقيقي لو أصبحت مسؤولة عن المحتوى الذي يتم تحميله على المنصات من قبل طرف ثالث. وهو ما يؤدي بدوره إلى إعاقة الابتكار المحلي وتقويض الاستثمار الأجنبي وحرمان مستخدمي المنصات، وهو ما يتعارض مع مبادئ حرية الإنترنت وانفتاحها. ومن الموصى به أن تقوم عمان بحماية الوسطاء من المساءلة في كافة الأمور خارج حدود حماية الملكية الفكرية لتشمل كل المحتوى الذي يقوم أطراف ثالثة بإنشائه، من أجل ضمان وجود إنترنت مفتوح متصل عالميا.

وأخيرا فيما يتعلق **بالتشفير**، فإن قانون تكنولوجيا الاتصالات العماني لعام 2002 هو واحد من آليات التشريع القليلة في المنطقة التي تتطلب الحصول على إذن من الحكومة قبل استخدام تكنولوجيا التشفير، وهذا ما تنص عليه المادة 48 من القانون:

"لا يسمح باستخدام التشفير في تكنولوجيا الاتصالات أو في شبكات الكمبيوتر، دون الحصول على إذن من الوزير المختص. هذا الإذن يحدد الأشخاص الذين يمكنهم العمل، وشروط استخدام التشفير، والرسوم المفروضة لاستخراج الإذن، والشروط المتعلقة بحفظ مفتاح التشفير، كما هو منصوص عليه في اللائحة التنفيذية للقانون."

وفقا للإعلان العام الذي أعلنته الحكومة بشأن منصات التواصل الاجتماعي، فإن شركة واحدة قد حصلت من قبل على هذا الإذن منذ إصدار القانون منذ أكثر من حوالي 20 عام. إن وضع هذه القيود على استخدام التكنولوجيا قد يعرض مستخدمي الإنترنت لخطر، لأن التشفير يعد أمرا أساسياً للتشغيل الآمن للإنترنت، وهو ضروري لتنفيذ عمليات الدفع، وتوثيق المستخدمين، وحماية البيانات عند النقل وعند السكون، وغياب التشفير يهدد أمن واستقرار وأمان الأفراد. إن بنود مثل المادة 48 من القانون العماني لتكنولوجيا الاتصالات تقيد أيضا من قدرة الشركات المحلية في عمان على الابتكار في مجال الأمن السيبراني نظرا لصعوبة الحصول على موافقة الحكومة اللازمة لاستخدام التشفير، كما أنه من الممكن أن يقيد ذلك أيضا من استثمار الشركات والذي يتضمن شركات الخدمات السحابية الذين يحتاج عملاؤها إلى تشفير البيانات الشخصية والبيانات ذات الحساسية العالية. ومن الموصى به أن تقوم عمان بحذف هذا الشرط، من أجل السماح للبيانات بالتدفق بحرية خارج الدولة طالما أن دولة الوجهة لديها مستوى كاف من الحماية. بالإضافة إلى ذلك يوصى أن تقوم عمان بإلغاء شرط الحصول على إذن لاستخدام تكنولوجيات التشفير.

المملكة العربية السعودية

مثلما هو الحال مع الدول الأخرى في المنطقة، قامت المملكة العربية السعودية مؤخرا بإصدار قانون لحماية البيانات الشخصية يوفر إطارا **لحوكمة البيانات** لاستخدام البيانات الشخصية ويضمن عدد من حقوق أصحاب

البيانات. على الرغم من ذلك، فإن هذا القانون يفرض بعض الشروط المعقدة للسماح بحركة البيانات خارج السعودية، إذ ينص على إمكانية نقل البيانات خارج الدولة في حالة أن تكون الحماية المتوفرة للبيانات في دولة الوجهة على الأقل متكافئة مع معايير الحماية التي يوفرها القانون السعودي وفقاً للمقاييس التي تضعها الحكومة السعودية. هذه المقاييس تم ترجمتها إلى نظام "القائمة البيضاء" الذي يتم بمقتضاه نقل البيانات بحرية إلى قائمة الدول المحددة فقط في هذه القائمة. إن فكرة القائمة البيضاء تم طرحها في سبتمبر 2024 وحتى وقت الكتابة، لم يتم نشرها بعد.

بالإضافة إلى ذلك، فإن القانون السعودي يسمح بنقل البيانات خارج القائمة البيضاء في حالة الإيفاء ببعض الشروط منها متطلبات إصدار الشهادات لمنظم البيانات. وبما أن كل هذه الإجراءات لا تزال حديثة العهد، فإنه لا يزال من غير الواضح على أرض الواقع كيف سيتم التنفيذ لأنه لا يوجد قائمة بيضاء كما أن مقدمي خدمات الشهادات لم يتم تحديدهم بعد. وبينما يبدو الأمر للوهلة الأولى أمرا معقولا لحماية حقوق المستخدمين، فإن وجود قائمة بيضاء محددة وفرض شروط صارمة للتراخيص قد يضع قيودا كبيرة على قدرة مقدمي وتطبيقات الخدمات السحابية المحلية والأجنبية للالتزام بالقانون، مما يعمل بدوره على إعاقة الابتكار وتقويض الاستثمار تقييد قدرة المستخدمين في المملكة السعودية على الاستفادة من هذه الخدمات، بل ويتعارض مع المبادئ الأساسية للإنترنت الحر والمفتوح. ويوصى أن تقوم السعودية بالنظر في قواعد توطين البيانات التي يقدمها القانون السعودي لحماية البيانات الشخصية بطريقة تسمح بتحرك البيانات بين السعودية والدول الأخرى التي لديها مستويات ملائمة لحماية البيانات.

وكما هو موضح أعلاه، فإن القانون السعودي لحماية البيانات الشخصية واللائحة التنظيمية الخاصة به تعترف بالحقوق الرئيسية **للخصوصية** مثل حق الموافقة على استخدام البيانات الشخصية، وحق الوصول للبيانات الشخصية، وحق طلب حذف البيانات الشخصية، وهي حقوق تتماشى جميعها مع أفضل الممارسات الدولية مثل اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي. إلا أن هذا القانون لا يقر بوجود بعض من التحديات الجديدة التي تواجه المستخدمين في عصر الذكاء الاصطناعي، ولا يوفر أي شروط خاصة لعملية التشغيل الآلي للبيانات الشخصية باستخدام الذكاء الاصطناعي أو الحق في الإبلاغ عن استخدام تكنولوجيات التنميط في مجالات مثل التوظيف والتعليم.

إن غياب الحماية من مثل هذه الاستخدامات الجديدة للبيانات الشخصية لا يتماشى مع أفضل الممارسات الدولية ذات الصلة في العديد من القوانين، بما في ذلك القوانين الخاصة ببعض الدول الأخرى في المنطقة التي توفر الحماية من عملية التشغيل والتنميط الآلي. مثل هذا الغياب قد يضع حقوق المستخدمين في الخصوصية في خطر، ويقلل من الثقة في الإنترنت. يوصى أن تقوم المملكة العربية السعودية بطرح شروط للحماية ضد التشغيل الآلي للبيانات والتنميط، وذلك لحماية الخصوصية وتمكين المستخدمين فهم أو التحكم في طريقة استخدام البيانات.

فيما يتعلق **بمسئولية الوسطاء**، فإن القانون السعودي لا يضع شروطا محددة لتقييد مسئولية المنصات عن المحتوى الذي تقوم أطراف ثالثة بنشره. ينص نموذج قانون الجريمة السيبرانية لدول مجلس الخليج العربي والذي تبنته المملكة العربية السعودية، على أن المحكمة قد تعفي مالك أو مدير الموقع من المسئولية فقط في حالة حذف المحتوى بشكل فوري بناء على طلب السلطات. هذه الحالة من عدم الثقة تجعل من إنشاء وإدارة منصات المواقع الإلكترونية في المملكة العربية السعودية، للسماح للمستخدمين بتحميل ومشاركة المحتوى، أمرا يحمل مخاطرة على مالكي ومديري مثل هذه المنصات، لأنهم سيكونوا مطالبين بمراقبة كل بند تم رفعه على المنصة وإلا سيكونون مسئولين عنه. وهذا الأمر من المستحيل تحقيقه، وكنتيجة لذلك، من المستحيل أن يقوم السعوديون بإنشاء بدائل لمنصات التواصل الاجتماعي مثل فيسبوك، ومنصة اكس، ويوتيوب، أو انستجرام، دون أن يضعوا أنفسهم في مخاطرة قانونية كبيرة، مما يخلق درجة عالية من عدم الثقة في هذه المنصات، وذلك يتعارض مع

مبادئ الإنترنت الحر والمفتوح، ويمكن أن يعمل على إعاقة الابتكار المحلي وتقويض الاستثمار الأجنبي، وحرمان المستخدمين المحليين للمنصات، مما يتعارض مع مبادئ الإنترنت الحر والمفتوح. ويوصى بأن تقوم السعودية بالنظر في وضع إطار قانوني لحماية مالكي ومديري المواقع من التعرض للمساءلة بسبب ما تقوم أطراف ثالثة من نشره من محتوى.

إن استخدام **التشفير** في المملكة العربية السعودية لا يخضع للتنظيم، ومن ثم لا يبدو أن هناك قيود على استخدامه. وهذه اللائحة التنفيذية تدعم وجود إنترنت مفتوح، ومتصل عالميا، وآمن وموثوق.

الإمارات العربية المتحدة

تمتلك الإمارات العربية المتحدة إطارا معقدا **لحوكمة الإنترنت** فيما يتعلق بحماية البيانات الشخصية، وذلك بمقتضى قانون حماية البيانات الشخصية، والذي لا يبدو أنه يفرض أي قيود صارمة على تدفق البيانات بين الإمارات العربية المتحدة ودول أخرى. إلا أن الإمارات العربية المتحدة لديها تشريع خاص ببعض القطاعات يفرض بعض متطلبات توطين البيانات. فعلى سبيل المثال فإن المادة 13 من قانون معلومات الرعاية الصحية الخاص بالإمارات العربية المتحدة ينص على:

" من غير المسموح أن يتم الاحتفاظ، أو تشغيل، أو إنشاء أو تحويل بيانات ومعلومات صحية خارج الدولة- البيانات والمعلومات التي ترتبط بخدمات الصحة المتاحة داخل الدولة- إلا في حالة إصدار قرار من هيئة الصحة بالتعاون مع الوزارة"

وبينما يبدو الأمر من الوهلة الأولى معقولا أن يكون هناك مثل هذه القوانين لحماية حقوق المرضى في الخصوصية، إلا أن وجود البيانات داخل الدولة لا يعني بالضرورة أن البيانات ستكون أكثر أمنا أو أن خصوصية المستخدمين ستكون محمية بشكل أكبر. هذه القيود قد تجعل الأمر أيضاً صعباً على بعض مقدمي خدمات الرعاية الصحية للاستفادة من الفرص التي يتيحها مقدمو الخدمات السحابية الأجانب، وهو ما يحد من الاستثمار ومن قدرة المستخدمين في الإمارات العربية المتحدة على الاستفادة من هذه الخدمات، كما يتعارض مع المبادئ الرئيسية للإنترنت الحر والمفتوح. ويوصى بأن تقوم الإمارات العربية المتحدة بإعادة النظر في قواعد توطين البيانات الموجودة في قانون المعلومات الصحية بطريقة تسمح بحركة البيانات بين الإمارات العربية المتحدة ودول أخرى لديها مستويات ملائمة من حماية البيانات.

فيما يتعلق بحماية **الخصوصية** بشكل عام، وكما ذكرنا آنفا، فإن الإمارات العربية المتحدة لديها قانون لحماية البيانات الشخصية يضمن حقوق أصحاب البيانات ويتضمن شروط خاصة تتعلق بالتشغيل الآلي للبيانات وذلك بمقتضى المادة 18:

1- إن مالك البيانات لديه الحق في الاعتراض على أي قرارات تصدر من عملية التشغيل الآلي، بما في ذلك التنميط، وخاصة القرارات التي يكون لديها تأثير قانوني أو تأثير غير مرغوب فيه على صاحب البيانات.

2- على الرغم مما تنص عليه الفقرة 1 من المادة، فإن صاحب البيانات قد لا يعترض على القرارات الناتجة عن عملية التشغيل الآلي في الحالات التالية:

أ- أن يكون هناك اتفاق مسبق على عملية التشغيل الآلي بمقتضى عقد بين صاحب البيانات من جهة والمتحكم في البيانات من جهة أخرى.

ب- أن تكون عملية التشغيل الآلي تتم بمقتضى تشريعات أخرى مطبقة في الدولة.

ج- أن يكون صاحب البيانات قد أعطى موافقة مسبقة على عملية التشغيل الآلي، كما هو منصوص عليه في المادة 6 من هذا القرار وبمقتضى القانون.

3- يقوم المتحكم في البيانات بتنفيذ إجراءات ملائمة لحماية الخصوصية والسرية للبيانات الشخصية لصاحب البيانات في الحالات المشار إليها في الفقرة الثانية من هذه المادة ولا يقوم بأي أعمال بها تحيز لحقوق صاحب البيانات.

4- يقوم المتحكم في البيانات بتضمين العامل الإنساني أثناء مراجعة قرارات التشغيل الآلي وذلك بطلب من صاحب البيانات.

تعد هذه المادة واحدة من أكثر البنود شمولية في المنطقة والتي تحمي أصحاب البيانات من عملية التشغيل الآلي للبيانات الشخصية، من خلال التنميط وغيرها من الممارسات، كما أنها أيضا تعطي صاحب البيانات الحق في أن يطلب القيام بمراجعة بشرية فيما يخص القرارات الصادرة عن عملية تشغيل البيانات الآلي، وهو حق متطور ومطلوب لحماية حقوق أصحاب البيانات في عصر الذكاء الاصطناعي.

فيما يتعلق **بمسئولية الوسطاء،** فإن قانون الإمارات العربية المتحدة لا يتضمن شروط معينة لتحديد مسؤولية المنصة عن المحتوى الذي يقوم أطراف ثالثة بنشره. إن المادة 53 من القانون الخاص بمكافحة الشائعات والجرائم السيبرانية يبدو أنه يقترح أن تكون المنصة مسؤولة عن أي محتوى تقوم بنشره أو تخزينه، حتى لو تم تحميل هذا المحتوى من قبل طرف ثالث، وذلك في حالة عدم قيام المنصة بحذف المحتوى بناء على طلب من الحكومة في خلال فترة زمنية محددة. وهو ما يجعل من إنشاء وإدارة منصات المواقع الإلكترونية في الإمارات العربية المتحدة بالشكل الذي يتيح للمستخدمين فرص تحميل ومشاركة المحتوى، أمرا يحمل مخاطرة لمالكي ومديري هذه المنصات، وذلك لأنهم سيكونوا مجبورين على حذف أي محتوى تأمرهم الحكومة بحذفه، وإلا سيكونون مسئولين عنه. هذا القانون يطرح آلية للاعتراض على هذه الأوامر بمقتضى المادة 63، إلا أن هذه الآلية لا يبدو أنها تسمح للمنصات بعدم تنفيذ الأمر، وفي كل الحالات، حتى في حالة الاستئناف، فإن القانون يعتبر الاستئناف مرفوضاً لو لم ترجع الحكومة برد في خلال 7 أيام.

وهو الأمر الذي يجعل الأمر صعبا على الإماراتيين أن يقوموا بإنشاء بدائل لمنصات التواصل الاجتماعي مثل فيسبوك، ومنصة اكس، ويوتيوب، أو انستجرام، دون أن يعرضوا أنفسهم لمخاطرة قانونية كبيرة، وهو ما يخلق نوع من أنواع عدم الثقة في هذه المنصات، ويتعارض مع مبادئ الإنترنت الحر والمفتوح. ويوصى أن تقوم الإمارات بالنظر في وضع إطار قانوني لحماية مالكي ومديري المواقع الالكترونية من المساءلة عن محتوى الأطراف الثالثة.

إن استخدام **التشفير** في الإمارات العربية المتحدة لا يخضع للتنظيم ولا يبدو أن هناك قيود على استخدامه.

إن تنظيم الخصوصية والتشفير في الإمارات العربية المتحدة يدعم مبادئ الإنترنت المفتوح والمتصل عالميا والآمن والموثوق، بينما تتناول توصياتنا أوضاع الحوكمة الحالية للبيانات ومسئولية الوسطاء.

الخاتمة

بينما تطرح التكنولوجيات الرقمية الجديدة مثل الذكاء الاصطناعي فرص وتحديات جديدة للأفراد والأعمال والحكومات، فإنه من المهم أن نضمن أن تتناول استجابة الحكومات لهذه التحديات عدم التأثير على أسس بقاء وازدهار الإنترنت. لا يعد الذكاء الاصطناعي التكنولوجيا الرقمية الناشئة الوحيدة ذات التأثير، فإن الحوسبة السحابية والحوسبة الطرفية تغير من طريقة الوصول للبيانات، ومن موقع البيانات والمحتوى والخدمات. وقد أوضح هذا التقرير فائدة مجموعة أدوات تقييم تأثير الإنترنت والتي أصدرتها جمعية الإنترنت لهذا الغرض في سياق التطبيق على عدد ست دول من دول منطقة الشرق الأوسط وشمال أفريقيا.

بينما تقوم الحكومات بدراسة الفجوات أو البدائل الموجودة للوائح التنظيمية القائمة أو تقوم بفرض لوائح جديدة للقيام بدورها الداعم للإنترنت، قامت جمعية الإنترنت بوضع مجموعة أدوات لتقييم تأثير الإنترنت لمساعدة الحكومات على القيام بدورها. مجموعة الأدوات تلك توفر إطار يمكن من خلاله تحديد مدى فاعلية اللوائح التنظيمية في ترويج "أسلوب الإنترنت في تكوين الشبكات"، والذي يتضمن عدد من الخصائص الحيوية التي تحتاجها الإنترنت كي تستمر، ويتضمن أيضاً مجموعة من العوامل التمكينية التي تضمن ازدهار الإنترنت وتحقيق الأهداف المرجوة من وجود إنترنت مفتوح، ومتصل عالميا وآمن وموثوق يحقق الفائدة للجميع.

يستخدم هذا التقرير مجموعة الأدوات لتقييم أربعة لوائح تنفيذية للإنترنت، مما يعكس الفرص والتحديات التي تفرضها هذه اللوائح على التكنولوجيات الحديثة، ويتناول التقرير اثنين من هذه التكنولوجيات الناشئة وهي الذكاء الاصطناعي والحوسبة السحابية والحوسبة الطرفية. أما السياسة الحكومية واللوائح التنظيمية التي يتناولها التقرير فهي حوكمة البيانات، وحماية الخصوصية، وحماية مسئولية الوسطاء، وتنظيم التشفير، وذلك في ست دولة من منطقة الشرق الأوسط وشمال أفريقيا وهم البحرين ومصر والأردن وعمان والمملكة العربية السعودية والإمارات العربية المتحدة.

وبشكل عام، نجد أن كل هذه الدول لديها لوائح تنظيمية ذات صلة، إلا أن بعض منها قد لا يغطي كل الموضوعات القائمة أو الناشئة التي تثيرها التكنولوجيات الحديثة، وفي بعض الأحوال الأخرى قد توجد بعض الفجوات. ولضمان أن تؤدي اللوائح التنظيمية دورها في ضمان وجود إنترنت مفتوح ومتصل عالميا وآمن وموثوق، نقوم بطرح عدد من التوصيات. وبشكل عام فإن هذه التوصيات تأتي في أربع مجالات من السياسة تنص على ما يلي:

- *حوكمة البيانات:* قد تستخدم قوانين حماية البيانات لضبط إدارة قطاعات مختلفة من البيانات في الدولة، ووضع الشروط التي يتم بمقتضاها نقل البيانات إلى دول أخرى. معظم الدول محل الدراسة هنا قد وضعت بعض من القيود على نقل البيانات لدول أخرى. وبينما كان من المهم ضمان نقل البيانات للدول التي توفر مستويات معقولة من حماية البيانات، فإن اللوائح التي تمنع النقل أو تقيد من حركة البيانات لمجموعة محددة من الدول يمكن أن يؤدي هذا الإجراء إلى تفتيت الإنترنت ومنع تطور نظم شاملة للذكاء الاصطناعي واستخدام الخدمات السحابية والطرفية.
- *حماية الخصوصية:* وهي مجموعة فرعية من تنظيمات حوكمة الإنترنت تهدف إلى تأسيس حقوق خصوصية الأفراد وحماية البيانات الشخصية الخاصة بهم، وبينما كان من المهم حماية هذه الحقوق عند نقل البيانات الشخصية إلى دول أخرى، فإن اللوائح التنظيمية الصارمة قد تؤدي إلى تفتيت الإنترنت وتقييد توفر الخدمات التي تستخدم البيانات الشخصية. ومع ظهور الذكاء الاصطناعي، فإن البيانات الشخصية قد تستخدم لأغراض التنميط او اتخاذ القرار الآلي، ويجب أن تقوم القوانين بتوفير حق إبلاغ المستخدمين في حالة أن يكونوا هم أصحاب هذه التكنولوجيات الخاصة بالتنميط. كل الدول محل الدراسة هنا لديها قوانين تتناول

خصوصية البيانات الشخصية، إلا أن معظمها لا تتضمن بنود تحمي من استخدام البيانات الشخصية من التنميط أو اتخاذ القرار الآلي.

- *حماية مسئولية الوسطاء*: يقوم الوسطاء مثل شبكات توصيل المحتوى، ومقدمي الخدمات السحابية، وشركات التواصل الاجتماعي، ومقدمي خدمة الإنترنت باستضافة وتوصيل حركة الإنترنت بين نقاط نهائية، إلا أنهم غير مسئولين عن المحتوى. إن حماية مسئولية الوسطاء تحميهم من المساءلة عن المحتوى الذي يقومون باستضافته، بما في ذلك المحتوى الذي قد ينتهك القوانين المحلية أو حقوق النشر. معظم الدول محل الدراسة لا تضع شروط محددة تحمي الوسطاء من المسائلة، ولا يوجد إلا دولتين تضع شروط تحدد مسئولية الوسطاء في أي انتهاك قد يحدث لحقوق النشر (ولكن ليس لأنواع أخرى من المحتوى غير القانوني). إن غياب هذه الحماية قد يؤدي إلى إعاقة الابتكار المحلي وتقويض الاستثمار الأجنبي في المنصات التي تستضيف المحتوى في الدولة.
- *تنظيم التشفير*: يعمل التشفير على حماية المعلومات الالكترونية بحيث لا يستطيع قراءتها إلا من لديهم حق الوصول إليها، ومن أمثلة ذلك الرسائل النصية، وحركة الويب، والبيانات الشخصية في حالة الانتقال أو السكون. إن معظم الدول محل الدراسة هنا لا تضع أي قيود على التشفير. إن اللوائح التنظيمية التي تحد او تمنع استخدام التشفير يمكن أن تحد من حماية الخصوصية، وتزيد من خطر الجريمة السيبرانية، وتقيد من الاستثمارات التي قد تقوم بها شركات الخدمات السحابية وغيرها اعتمادا على حماية التي يوفرها التشفير.

إن التوصيات التي يأتي بها هذا التقرير فيما يتعلق بالمجموعات الأربعة من التنظيمات في كل واحدة من الدول محل الدراسة تهدف إلى توفير إنترنت مفتوح ومتصل عالميا، غير منقسم، وآمن وموثوق، وألا يكون الإنترنت هدف سهل للجريمة السيبرانية وتسريب البيانات. وهو ما يتيح الاستثمارات في مجال التكنولوجيات السحابية والطرفية في مختلف الدول لمصلحة الأفراد والمنظمات، ويتيح الابتكار في أنظمة الذكاء الاصطناعي مما يتيح خدمات وفرص جديدة للمواطنين.

هذا التحليل المطروح يوضح جليا أن مجموعة أدوات تقييم تأثير الإنترنت يمكن أن يوجه عملية وضع اللوائح التنظيمية "الذكية" والتي تستجيب للتكنولوجيات الناشئة في إطار ثابت ومنظم. قامت جمعية الإنترنت بتفويض القيام بهذا العمل لتقدم مثالاً حقيقياً على طريقة استخدام مجموعة الأدوات، كما أن موظفي وأعضاء جمعية الإنترنت على أتم الاستعداد لمساعدة الحكومات وباقي أصحاب المصلحة على تطبيق مجموعة الأدوات لتحقيق الهدف الاسمي وهو الحفاظ على إنترنت مفتوح ومتصل عالميا وآمن وموثوق للجميع.