إيسيسكو
ICESCO

EMC
مسقط 2024
Muscat 2024

سلطنة عمان
وزارة التربية والتعليم

مؤتمر الإيسيسكو لوزراء التربية والتعليم

ICESCO EMC 3

ما بعد قمة تحويل التعليم: من الالتزامات إلى التطبيقات

3.5
التربية الرقمية

مسقط،
سلطنة عمان

3-2
أكتوبر

2024

إيسيسكو
ICESCO

مـؤتمـــــر الإيسيسكـــو لـوزراء التربيـــة والتعليـم

ICESCO EMC 3

مـــا بعـــد قمـــة تحويـــل التعليـم :
من الالتزامات ← إلى التطبيقات

3.5
التربيـة الرقميـة

2024 | 3-2 أكتـــوبر | مسقط، سلطنة عمـان

الفهـــرس

0
تقديـــم

أ. الأهداف؛

ب. أهمية حماية المعطيات الشخصية؛

ج. دور التربية الرقمية في حماية المعطيات الشخصية

د. نماذج من الدول الأعضاء في الإيسيسكو.

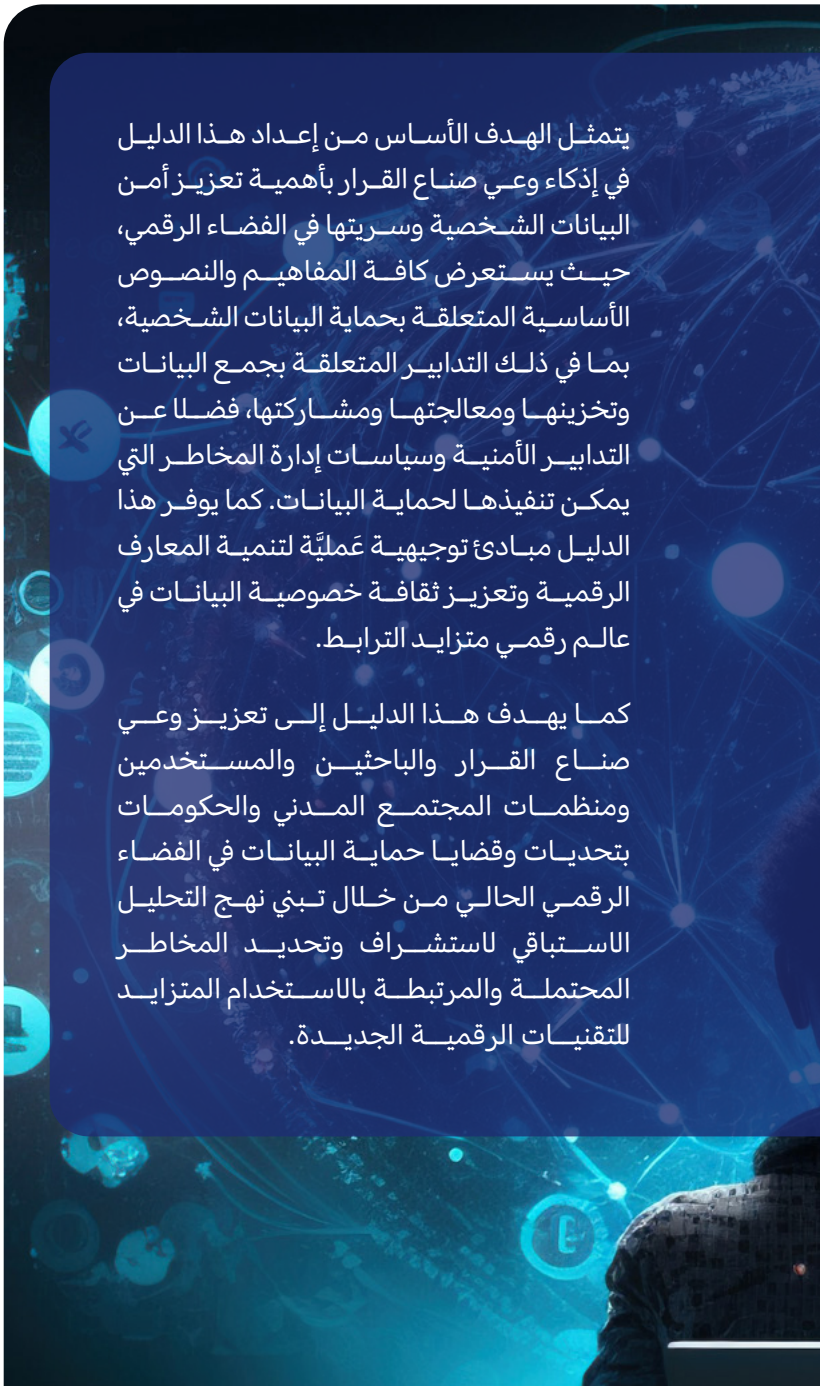
تقديم

ما فتئ يتزايد تأثير التكنولوجيا الرقمية والذكاء الاصطناعي على حياة الأفراد، حيث باتت البشرية محاطة بفضاء رقمي غيَّر حياة الأفراد بشتى الطرق ومختلف الأبعاد. وعلى الرغم من الفرص الموثقة والمثبتة التي يوفرها هذا الفضاء، لا سيما في مجال التعليم، قد يكون للأدوات الرقمية عدد من المخاطر التي تهدد سلامة مستخدميها وتمس بحقوقهم الأساسية، لعل أبرزها انتهاك البيانات الشخصية واستغلالها.

وفي هذا الصدد، يتعين على صناع السياسات والجهات المختصة، بما في ذلك الجهات التشريعية والسلطات الوصية وقطاع التكنولوجيا الرقمية، تعزيز المبادئ التوجيهية وتنفيذ التدابير اللازمة للوفاء بالتزاماتهم بحماية البيانات ومنه حماية خصوصية الأشخاص. كما أن إلمام الأطراف المعنية بهذه المشكلة المتنامية شرط أساسي لاتخاذ تدابير واعتماد مبادئ توجيهية متينة لحماية البيانات على أن تشمل هذه التدابير ممارسات سليمة لإدارة البيانات الشخصية وحمايتها وتعميم اعتمادها في كافة المؤسسات المعنية بمعالجة البيانات الشخصية واستخدامها. كما يجب أن تستند هذه التدابير إلى معايير ومبادئ القوانين والسياسات الدولية والوطنية لتعزيز ثقافة حماية البيانات الشخصية.

يروم هذا الدليل مساعدة صناع القرار وكافة الأطراف المعنية بالشأن الرقمي على فهم تحديات أمن البيانات من خلال تسليط الضوء على المبادئ والمعايير التي تم اعتمادها. يستعرض الدليل، على سبيل المثال لا الحصر، الممارسات الفضلى التي يمكن تقاسمها، ويظل احترام الخصوصية والبيانات الشخصية الشغل الشاغل لهذا الدليل لارتباطه ارتباطًا وثيقًا باحترام حقوق الإنسان.

أ. الأهداف



يتمثل الهدف الأساس من إعداد هذا الدليل في إذكاء وعي صناع القرار بأهمية تعزيز أمن البيانات الشخصية وسريتها في الفضاء الرقمي، حيث يستعرض كافة المفاهيم والنصوص الأساسية المتعلقة بحماية البيانات الشخصية، بما في ذلك التدابير المتعلقة بجمع البيانات وتخزينها ومعالجتها ومشاركتها، فضلا عن التدابير الأمنية وسياسات إدارة المخاطر التي يمكن تنفيذها لحماية البيانات. كما يوفر هذا الدليل مبادئ توجيهية عَمليَّة لتنمية المعارف الرقمية وتعزيز ثقافة خصوصية البيانات في عالم رقمي متزايد الترابط.

كما يهدف هذا الدليل إلى تعزيز وعي صناع القرار والباحثين والمستخدمين ومنظمات المجتمع المدني والحكومات بتحديات وقضايا حماية البيانات في الفضاء الرقمي الحالي من خلال تبني نهج التحليل الاستباقي لاستشراف وتحديد المخاطر المحتملة والمرتبطة بالاستخدام المتزايد للتقنيات الرقمية الجديدة.

بالإضافة إلى ذلك، يتوخى هذا الدليل تعزيز ثقافة المساءلة والشفافية في إدارة البيانات الشخصية من خلال تشجيع المنظمات على اعتماد سياسات وممارسات تتوافق مع المعايير الدولية والقوانين الحالية لحماية البيانات. ولا يتأتى ذلك إلا بتطوير آليات التعاون وإطار عمل تعاوني بين الأطراف المعنية في الدول الأعضاء في الإيسيسكو لتعزيز تبادل المعلومات والممارسات الفضلى، وتشجيع التعاون وتبادل الخبرات بين الجهات الفاعلة في الأوساط الرقمية، وهو ما من شأنه أن يقوي أواصر التآزر في مجال حماية البيانات، ويعين على تطوير معايير مشتركة وبناء القدرات والامتثال لمعايير حماية البيانات.

ب. أهمية حماية المعطيات الشخصية

في سياق النظم المعقدة لعالم التكنولوجيا والاتصالات، تلعب حماية البيانات الشخصية دورًا حاسمًا على عدة مستويات، أبرزها الحفاظ على خصوصية الأفراد وتحكمهم في معلوماتهم لتجنب أي شكل من أشكال الاستغلال في فضاء يعج بالبيانات الشخصية على نحو لم يسبق له مثيل.

علاوة على ذلك، تُعد حماية البيانات ركيزة أساسية لبناء الثقة الرقمية، إذ أن وضع معايير صارمة للأمن والسرية كفيل بتعزيز مناخ الثقة بين المستخدمين والشركات والحكومات، وهو أمر ضروري لتعميم تكنولوجيا المعلومات والاتصالات بما لها من تأثير على تشجيع الابتكار والنمو الاقتصادي.

والحق أن حماية البيانات عنصر أساسي من عناصر الأمن السيبراني في ظل تفشي التهديدات السيبرانية العالمية، وهو ما يستدعي اتخاذ تدابير حماية متينة للحد من انتهاكات البيانات والجرائم السيبرانية التي قد تعرض استقرار وأمن مستخدمي الإنترنيت للخطر.

ومن جانب آخر، تُعد حماية البيانات قضية أخلاقية وسياسية بالغة الأهمية، حيث تثير أسئلة عديدة حول حماية الخصوصية وتعزيز الحريات الفردية والمساءلة الاجتماعية للشركات والحكومات. إن ضمان الاستخدام الآمن والأخلاقي والمسؤول للبيانات سيكفل القيم الديمقراطية والحقوق الأساسية في فضاء رقمي دائم التغير.

والحق أن حماية البيانات الشخصية هي ضرورة أخلاقية واقتصادية واجتماعية وَجب إيلاءها عناية فائقة وحث جميع الأطراف المعنية بها على توحيد الجهود والالتزام بها.

ج. دور التربية الرقمية في حماية المعطيات الشخصية

تلعب التربية الرقمية دورا أساسيا في تعزيز حماية البيانات الشخصية إذ تُذكي وعي الأفراد بقضايا سرية وأمن البيانات الشخصية في الفضاء الرقمي. كما أن تزويد الأشخاص بالمعارف والمهارات اللازمة لفهم مبادئ حماية البيانات يضمن استخدامهم الآمن للفضاء الرقمي، ويُمكِّنُهم من اتخاذ قرارات مستنيرة حول تقديم معلوماتهم وبياناتهم الشخصية وإدارتها وحمايتها.

إن للتربية الرقمية فضلا في تعريف المستخدمين الشباب بالممارسات الجيدة والفضلى لحماية البيانات الشخصية. ولا يتأتى ذلك إلا عن طريق دمج مفاهيم حماية البيانات الشخصية والخصوصية في المناهج الدراسية لتزويد المتعلمين بالمهارات التي ستعينهم على توخي أمن البيانات وسريتها في الفضاء الرقمي. بالإضافة إلى ذلك، تشجع التربية الرقمية في مجال البيانات الشخصية على تطوير حلول رقمية مبتكرة لزيادة حماية البيانات. كما أن النهوض بالبحث والابتكار في مجال الأمن السيبراني وحماية الخصوصية سيعزز تطوير مقاربات وأدوات جديدة لضمان أمن وسلامة البيانات الشخصية في عالم رقمي يتغير باستمرار.

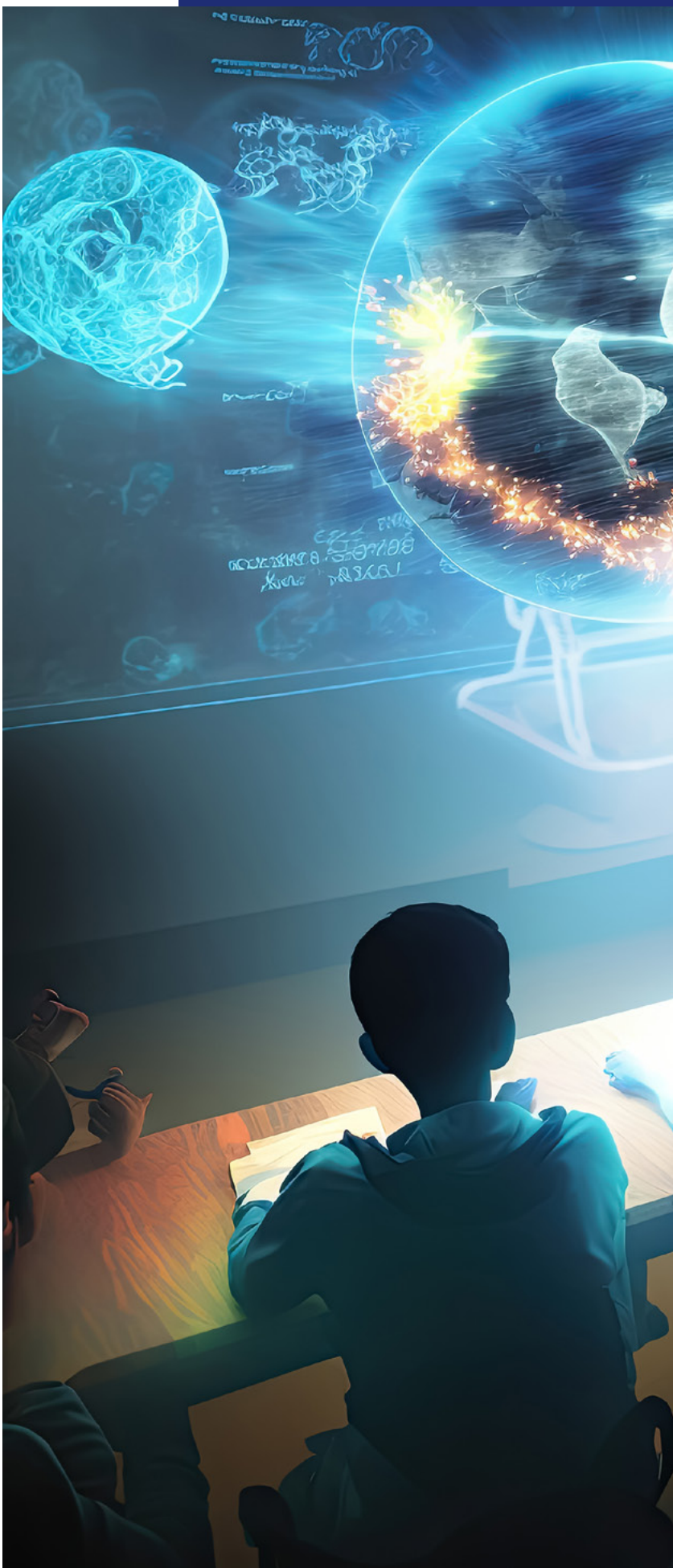
وتساهم التربية الرقمية كذلك في ترسيخ ثقافة المسؤولية والمواطنة الرقمية. وينعكس ذلك في مقاربة ذات شقين، هما: مبدأ الحق في الخصوصية وحماية البيانات لكل مواطن، ومسؤولية كل مستخدم عن حماية بياناته الشخصية وبيانات المستخدمين الآخرين، كلما أمكن ذلك. وبالتالي، فإن التدريب والتعلم في مجال التربية الرقمية سيضمنان تجربة رقمية أكثر أمانًا وأخلاقية وشمولية ومسؤولية وإنصافًا لجميع المستخدمين.

د. نماذج من الدول الأعضاء في الإيسيسكو

تعتبر الخصوصية حقا من حقوق الإنسان تكفله المادة 12 من الإعلان العالمي لحقوق الإنسان والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية. كما تتوفر جميع دول العالم، بما فيها الدول الأعضاء في الإيسيسكو، على قوانين لحماية البيانات تعزز حماية الخصوصية، حيث قامت أكثر من 132 دولة بسَنِّ هذه القوانين واعتمادها استناداً إلى المعايير الدولية. والحق أن حماية البيانات الشخصية أصبح الشغل الشاغل للدول الأعضاء في الإيسيسكو في ظل التحول الرقمي السريع في مجتمعاتنا.

وعلى الرغم من تفاوت مستويات التطور في سياسات واستراتيجيات وأنظمة حماية البيانات الشخصية بين الدول الأعضاء، إلا أن كافة الدول واعية بالأهمية المحورية لحماية البيانات الشخصية والخصوصية والسرية في الفضاء الرقمي.

وعليه، شرعت الدول الأعضاء في الإيسيسكو في تطوير أطر قانونية وتنظيمية لضمان حماية البيانات الشخصية بما يتماشى مع المعايير الدولية والمبادئ الإسلامية.



والحـق أن الجهـود بُذلـت لتعزيـز التعـاون الدولـي والإقليمـي وفيمـا بينهـا، وذلـك بهـدف تـدارس سـبل التعامـل مـع هـذه القضايـا، وإنشـاء آليـات للتبـادل والتعـاون تعيـن علـى خلـق فضـاءات رقميـة سـليمة وشـاملة في الـدول الأعضـاء بالإيسيسـكو.

يُـعنى هـذا الدليـل، الـذي صغنـاه علـى سـبيل المثـال لا الحصـر، بإعطـاء نبـذة عـن الجهـود القانونيـة والتنظيميـة التي بذلتهـا الـدول الأعضـاء في الإيسيسـكو. وتشـمل هـذه الجهـود سـنّ تشـريعات لحمايـة البيانـات الشـخصية، وتطويـر آليـات رقابـة لضمـان الامتثـال للقوانيـن والتنظيمـات ذات الصلـة، وتعزيـز الوعـي وتوفيـر التدريـب لـكل مـن المهنييـن والمواطنيـن حـول قضايـا الخصوصيـة وأمـن البيانـات. وتهـدف هـذه المبـادرات إلـى تعزيـز قـدرة الـدول علـى حمايـة المعلومـات الشـخصية في الفضـاء الرقمـي.

1

حماية المعطيات الشخصية: الإطار القانوني والمحاور والركائز

أ. تعاريف مختلفة للبيانات الشخصية؛

ب. ركائز حماية البيانات الشخصية؛

ج. تطور ممارسات جمع ومعالجة واستخدام البيانات الشخصية؛

د. قضايا ومخاطر حماية البيانات الشخصية وبناء الثقة الرقمية.

أ. تعاريف مختلفة للبيانات الشخصية

تختلف تعريفات مصطلح البيانات الشخصية باختلاف السياق القانوني والتنظيمي. وفيما يلي بعض التعاريف المعتمدة:

عرَّفت المادة 4 من اللائحة العامة لحماية البيانات في الاتحاد الأوروبي [1] (GDPR) "البيانات الشخصية" على أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد (يشار إليه فيما بعد بـ "صاحب البيانات")؛ ويُعتبر الشخص الطبيعي قابلاً للتحديد إذا أمكن التعرف عليه، سواء بشكل مباشر أو غير مباشر، خاصة بالإشارة إلى معلومة عنه مثل الاسم أو رقم بطاقة التعريف أو موقعه الجغرافي أو معرِّف إلكتروني أو أحد سماته الجسدية أو الفسيولوجية أو الوراثية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص. ويشمل ذلك معلومات مثل عنوان الآي-بي والبيانات البيومترية وغيرها من المعطيات.

وأما قانون حماية المعلومات الشخصية والوثائق الإلكترونية في كندا [2] (PIPEDA) فيُعرّف البيانات الشخصية على أنها أي معلومات أو معطيات مفصلة تتعلق بشخص قابل للتحديد، وبالتحديد المعلومات المتعلقة بصحة الفرد الجسدية أو العقلية.

ومن جهته، عرَّف قانون حماية البيانات في المملكة المتحدة [3] (DPA) البيانات الشخصية على أنها أي بيانات يمكن استخدامها لتحديد هوية شخص حي. إلا أن القانون المذكور لم يتطرق بالتفصيل للبيانات المجهولة أو المجمعة، غير أنه نصَّ على أن هذه البيانات تخضع لقوانين صارمة في حالة النبش في المعطيات للتعرف على الأفراد والكشف عن هويتهم من خلالها. وتشمل هذه البيانات معلومات مثل الاسم والعنوان والبريد الإلكتروني ورقم الهاتف والبيانات الطبية والمالية وما إلى ذلك.

[1] لائحة الاتحاد الأوروبي رقم 2016/679 الصادرة عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي بتاريخ 27 أبريل 2016، بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية انتقال هذه البيانات، والتي تلغي التوجيه EC/95/46 (اللائحة العامة لحماية البيانات – GDPR)

[2] القانون الكندي بشأن حماية المعلومات الشخصية والوثائق الإلكترونية (S.C. 2000, c. 5).

[3] صدر قانون حماية البيانات في المملكة المتحدة سنة 2018، وحصل على الموافقة الملكية في 23 ماي، أي قبل يومين من تاريخ دخول اللائحة 2016/679 حيز التنفيذ..

[4] يهدف قانون خصوصية المستهلك في كاليفورنيا لحماية المعلومات الشخصية القابلة للتعريف لسكان ولاية كاليفورنيا الأمريكية، أُصدر سنة 2018 ودخل حيز التنفيذ سنة 2020.

وأمـا في الولايـات المتحـدة، يعـرِّف قانـون خصوصيـة المسـتهلك في كاليفورنيـا [4](CCPA) البيانـات الشـخصية بأنهـا أي معلومـات تتعلـق أو تصـف أو يمكـن ربطهـا، سـواء بشـكل مباشـر أو غيـر مباشـر، بمسـتهلك مـا أو أسـرة معينـة. يَكفـل قانـون خصوصيـة المسـتهلك في كاليفورنيـا حقـوق الخصوصيـة ويحمـي المعطيـات الشـخصية للمسـتهلكين المقيميـن في ولايـة كاليفورنيـا. كمـا يهـدف إلـى تعزيـز خصوصيـة المسـتهلك مـن خـلال فـرض التزامـات علـى الشـركات التي تجمـع وتعالـج البيانـات الشـخصية.

ومـن البيانـات الشـخصية مـا يسـمى "البيانـات الحساسـة"، وهـي معلومـات ذات طبيعـة خاصـة قـد يُـفضي الكشـف عنهـا إلـى تعريـض خصوصيـة أو أمـن الأفـراد الجسـدي أو الأخـلاقي للخطـر. وتتعلـق هـذه البيانـات عـادة بمعطيـات حـول الأصـل العـرقي أو الإثني للشـخص أو آرائـه السياسـية أو معتقداتـه الدينيـة أو الفلسـفية أو انتمـاءه النقـابي، أو معطياتـه الجينيـة والبيومتريـة، أو حالتـه الصحيـة أو أسـرار مـن حياتـه الحميميـة. وبسـبب طبيعتهـا الحساسـة، تسـتوجب هـذه البيانـات حمايـة أكبـر وتخضـع عـادة لمعاييـر أكثـر صرامـة لتجميعهـا ومعالجتهـا ومشـاركتها وفقًـا للقوانيـن واللوائـح المعمـول بهـا.

لا يختلـف تعريـف البيانـات الشـخصية في الـدول الإسـلامية عـن التعريفـات المُعتمـدة في الاتحـاد الأوروبي والـدول الغربيـة الأخـرى، وهـي أنهـا بيانـات شـخصية أو معلومـات تتعلـق بشـخص طبيعـي محـدد أو قابـل للتحديـد مـع اختلافهـا في بعـض التفاصيـل باختـلاف قوانيـن كل بلـد.

والحـق أن التعريفـات تختلـف مـن نظـام إلـى نظـام قانـوني آخـر، لكنهـا تشـترك جميعهـا في فكـرة أن البيانـات الشـخصية هـي معلومـات يمكـن اسـتخدامها لتحديـد هويـة شـخص معيـن.

ب. ركائز حماية البيانات الشخصية

ناقش مؤتمر القمة العالمية لمجتمع المعلومات(WSIS) ، المنعقد في تونس في نوفمبر 2005، قضية حماية البيانات في وثائقه وإعلاناته. خرجت القمة "بإعلان المبادئ" الذي اعتُمِد خلال المرحلة الأولى في عام 2003 وحث على ضرورة بناء الثقة والأمان في استخدام تكنولوجيا المعلومات والاتصالات من خلال تعزيز حماية البيانات الشخصية والخصوصية، بالإضافة إلى أمان المعاملات. وهما ركيزتان لضمان الاستخدام الآمن والموثوق لتكنولوجيا المعلومات والاتصالات.

يؤكد هذا الإعلان على الأهمية البالغة لحماية البيانات الشخصية والخصوصية أثناء استخدام تكنولوجيا المعلومات والاتصالات، كما يشدد على ضرورة خلق فضاء تعمه الثقة والأمان للمستخدمين.

تستند حماية البيانات الشخصية إلى عدد من الركائز، يمكن تقسيمها إلى ستة مبادئ رئيسية [5] وهي: الموافقة والشفافية، والغرض من جمع البيانات ومعالجتها، وضمان دقة البيانات، والالتزام بمعايير الأمان والسرية، واحترام حقوق الأفراد في بياناته الشخصية.

الموافقة والشفافية: ومعنى ذلك أن يوافق الأفراد موافقة واضحة وصريحة على جمع بياناتهم الشخصية أو معالجتها أو مشاركتها. ويجب على المنظمات والأشخاص، سواء طبيعيين أو اعتباريين، أن يتوخوا الشفافية بشأن كيفية استخدام البيانات الشخصية ويقدموا معلومات واضحة ومفهومة حول الغرض من جمعها ومعالجتها ويضمنوا سريتها.

الغرض من جمع البيانات ومعالجتها: يجب جمع ومعالجة البيانات الشخصية لغرض محدد ومشروع فقط، ولا يجوز استخدامها لاحقاً بطريقة تتعارض مع الغرض الأولي من جمعها. وعليه، فإن المنظمات مُلزمة بأن تحد من جمع البيانات إلى الحد الأدنى اللازم، أي المعطيات ذات صلة والمتناسبة مع أغراض المعالجة.

دقة البيانات: تتحمل المنظمات مسؤولية ضمان أن البيانات الشخصية التي تحتفظ بها دقيقة وكاملة ومحيَّنة.

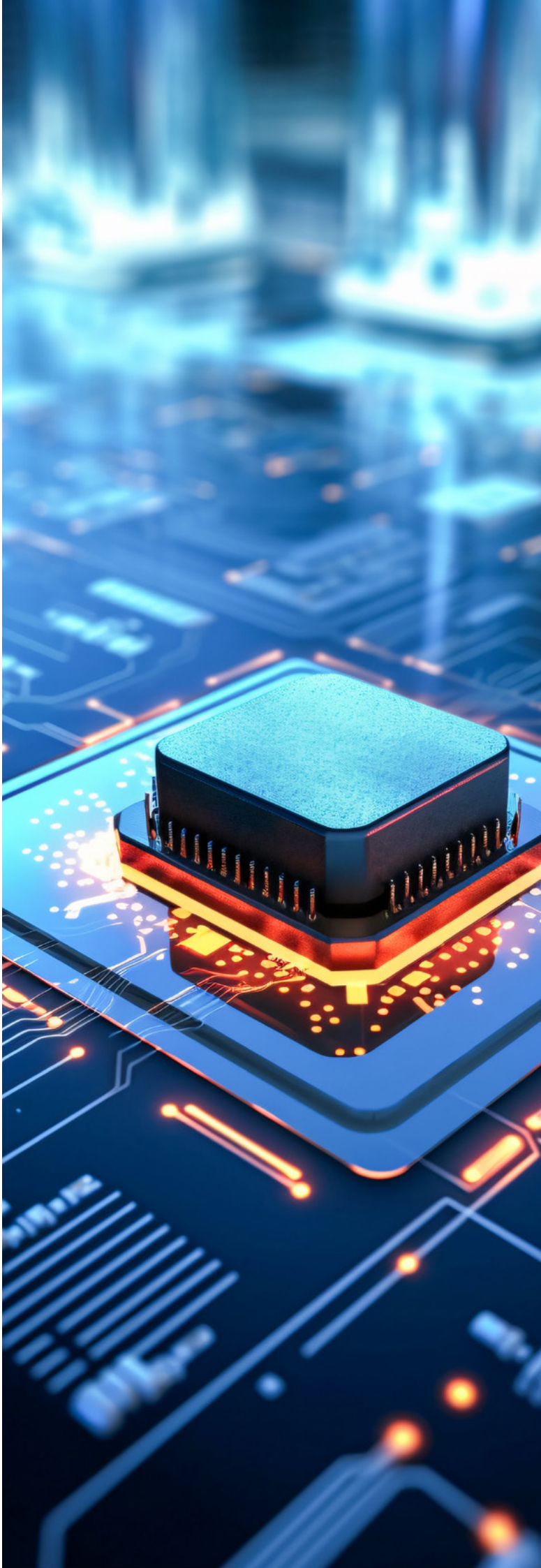
الأمان والسرية: تتحمل المنظمات التي تجمع وتعالج البيانات الشخصية مسؤولية تنفيذ جميع التدابير الأمنية المناسبة لحماية البيانات الشخصية من الضياع أو الاختراق أو الإفصاح أو الإتلاف. وتشمل هذه التدابير تشفير البيانات أو إدارة الوصول إلى قواعد البيانات.

احترام حقوق الأفراد: يتمتع الأفراد بحقوق على بياناتهم الشخصية، بما في ذلك الحق في الوصول إليها وتصحيحها إذا كانت غير دقيقة، وحذفها، والاعتراض على معالجتها، أو طلب نقلها إلى مقدم خدمة آخر.

إن الالتزام بهذه المبادئ الأساسية سيُمكِّن المنظمات من حماية البيانات الشخصية مع احترام حقوق الأفراد وتطلعاتهم بشأن الخصوصية.

يتحمل معالج البيانات، أي الجهة أو الفرد المسؤول عن تحديد أغراض ووسائل معالجة البيانات، مسؤولية ضمان الامتثال لمبادئ حماية البيانات الشخصية وأن معالجة البيانات تتم

[5] اللجنة الوطنية للمعلوماتية والحريات (CNIL)، 23 أغسطس 2019، المبادئ الستة الرئيسية للائحة العامة لحماية البيانات (GDPR)، التي تم اعتمادها في 24 مايو 2016 من قبل البرلمان الأوروبي والمجلس. قانون حماية البيانات لعام 2018، https://www.cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd



وفقًا للقوانيـن واللوائـح السـارية. قـد يكـون معالـج البيانـات شـركة أو منظمـة عامـة أو أي جهـة تجمع أو تسـتخدم أو تخـزن البيانـات الشـخصية. كمـا يتحمـل معالـج البيانـات مسـؤولية سـرية وأمـان البيانـات، فضـلاً عـن احتـرام حقـوق الأفـراد المتعلقـة بحمايـة البيانـات. وفي حالـة عـدم الامتثـال، قـد يتعـرض معالـج البيانـات لعقوبـات وغرامـات.

أحـدث الـذكاء الاصطناعـي تحـولا كبيـرا علـى عمليـات جمـع ومعالجة واسـتخدام البيانات الشـخصية. فبفضله أصبحـت الشـركات قـادرة علـى أتمتـة وتحسـين هـذه العمليـات، وجعلهـا أكثـر مواءمـة للخدمـات المقدمـة مـع توفيـر تحليـلات وإحصائيات معمقـة للبيانـات. ومع ذلـك، فـإن هنـاك مخـاوف متزايـدة بشـأن الخصوصيـة وأمـن البيانـات وهـو مـا يسـتوجب فـرض رقابـة وتأطير هـذه الممارسـة بالقوانيـن اللازمـة.

ج. تطور ممارسات جمع ومعالجة واستخدام البيانات الشخصية

تغيرت ممارسات جمع ومعالجة واستخدام البيانات الشخصية جذريا منذ بداية الألفية الثانية تزامنا مع ظهور الشبكات الاجتماعية والتقنيات الرقمية. كانت البيانات تُجمع حصرا لمعاملات بسيطة، ففي مجال التجارة، كان الغرض منها تسجيل العملاء لتسليمهم منتجاتهم وفواتيرهم. وما كان في السابق مجرد جمع بيانات لغرض معاملات محددة، تحول في عام 2010 إلى عملية أكثر تعقيدا بكثير. فلقد تنوعت مصادر تجميع البيانات لتشمل مواقع التواصل الاجتماعي والأجهزة المتصلة بالشبكات والإنترنيت والتطبيقات المحمولة والتي تشمل معلومات بإمكانها تحليل الخصائص النفسية والسلوكية للأفراد وتصنيفهم حسب شخصياتهم وسلوكياتهم.

تعتمد معالجة هذه البيانات الآن على تقنيات متقدمة مثل البيانات الضخمة (Big Data) والذكاء الاصطناعي. تتيح آلية البيانات الضخمة تحليل كميات هائلة من البيانات آنيا، مما يوفر رؤى قيمة يُسترشد بها لاتخاذ القرارات وجعل الخدمات أكثر مواءمة للمستخدمين. أما من جهته، فيسهل الذكاء الاصطناعي تنفيذ مهام معقدة مثل التعرف على الأنماط وتوقع سلوكيات المستخدمين لتكييف العروض مع احتياجاتهم.

غير أن هذا التقدم التكنولوجي يطرح تحديات كبيرة أمام حماية الخصوصية، ذلك أن التوسع في جمع البيانات وتحليلها يزيد من مخاطر المراقبة والتنميط، أي تحليل الخصائص النفسية والسلوكية للأفراد وتصنيفهم حسب شخصياتهم، وإساءة استخدام المعلومات الشخصية. ومن هنا يبرز دور التربية الرقمية في توعية الناس بكيفية إدارة بياناتهم من أجل الحد من هذا النوع من المخاطر. وبالتالي تبرز الحاجة إلى تشريعات أكثر صرامة لتنظيم استخدام البيانات وضمان اتباع نهج أخلاقي وآمن، من أجل حماية خصوصية المستخدمين.

د. قضايا ومخاطر حماية البيانات الشخصية وبناء الثقة الرقمية

يتمحور مفهوم الثقة الرقمية حول خلق فضاء رقمي أكثر أمانا للمستخدمين من خلال تعزيز حماية المعطيات الشخصية وضمان سرية بيانات الأفراد والمؤسسات. كما يشمل أيضا ضمان سرية البيانات وأمنها وسلامتها في العالم الرقمي. ومن الناحية القانونية، فإن الثقة الرقمية هي مجموع القواعد والمعايير التي تضمن هذه الحماية، بما في ذلك تشريعات حماية البيانات والمعايير والتدابير الشاملة للأمن السيبراني [6] [7].

عندما يقدم الأفراد معلوماتهم الشخصية عبر الإنترنت ويوافقون على معالجتها من طرف معالج البيانات، فإنهم يتوقعون أن تُكفل بواجبي الأمانة والسرية وتُستعمل للغرض الذي جُمعت من أجله. إلا أن مخاطر الخصوصية وأمن البيانات يمكن أن تضعضع هذه الثقة.

والحق أن للجرائم السيبرانية والهجمات الإلكترونية واختراق البيانات وإساءة جمعها ومعالجتها عواقب وخيمة على الأفراد، تتراوح بين سرقة الهوية أو الكشف عن المعلومات الحساسة أو تسريبها. هذه الحوادث، أو لنقل الجرائم، لا تنتهك خصوصية المستخدمين فحسب، بل تقوض أيضا الثقة في الشركات والمؤسسات المسؤولة عن حماية هذه البيانات.

ولتعزيز الثقة الرقمية، من الضروري تنفيذ تدابير فعالة لحماية البيانات [8]، مثل تقنيات التشفير وتنظيم تصاريح الولوج إلى قواعد البيانات، بالإضافة إلى توعية المستخدمين بالممارسات الفضلى في الأمن السيبراني وحماية بياناتهم الشخصية.

ويُعَد أمن البيانات الشخصية وسريتها عنصرا أساسيا في تعزيز ثقة الناس في المنظومة الرقمية، وفي توفير فضاء رقمي أكثر أمانا.

[6] القانون رقم 575-2004 الصادر في 21 يونيو 2004 بشأن الثقة في الاقتصاد الرقمي (فرنسا).

[7] قانون حماية المعلومات الشخصية والوثائق الإلكترونية (PIPEDA) (كندا).

[8] القانون رقم 20-43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية (المغرب).

2

دد
تعزيز الإطار المؤسساتي والتنظيمي لحماية المعطيات الشخصية

أ. دور هيئة حماية البيانات ومهمتها؛

ب. السياسات الداخلية للامتثال القانوني في المنظمات؛

ج. تدريب الموظفين المسؤولين عن معالجة وإدارة البيانات الشخصية على أفضل الممارسات؛

د. اعتماد التقنيات الآمنة لمعالجة البيانات الشخصية.


AI
1 10 1001 01010 10
1 0
0 1 1 0010
10

أ. دور هيئة حماية البيانات ومهمتها

تضطلع هيئة حماية البيانات الشخصية، باعتبارها هيئة حكومية مستقلة مكلفة بحماية البيانات الشخصية داخل البلد أو المنطقة، بضمان الامتثال لقوانين حماية البيانات وتشريعاتها من خلال الإشراف على معالجة البيانات وتنظيمها. وعلى هذا فإن هذه الهيئة لها مهام رقابية وتقوم بإنفاذ قوانين حماية البيانات الشخصية وضمان الامتثال لها. كما أن الهيئة مسؤولة عن التحقيق في الانتهاكات ويمكنها فرض عقوبات على عدم الامتثال. بالإضافة إلى ذلك، فهي تقدم الدعم والتوجيه للشركات والأفراد بشأن أفضل الممارسات لحماية البيانات، وتُساهم في رفع مستوى الوعي العام بشأن قضايا الخصوصية وأمن البيانات.

وفي عالم رقمي متشعب ومعقد، تتعاون هيئة حماية البيانات الشخصية مع السلطات المسؤولة عن الأمن الوطني والسيبراني ومع نظيراتها في الدول الأخرى لتعزيز التعاون وتوحيد معايير حماية البيانات.

ب. السياسات الداخلية للامتثال القانوني في المنظمات

لا بد لأي مؤسسة، شركة كانت أو غير ذلك، من اعتماد سياسات داخلية للامتثال للمعايير والضوابط القانونية لحماية البيانات الشخصية. فهذه السياسات هي الضامن للتزامها بمبادئ حماية البيانات، والتي تُعد ركيزة من ركائز بناء الثقة الرقمية واحترام الخصوصية. ومن أمثلة هذه السياسات وضع إجراءات ومبادئ توجيهية واضحة للاسترشاد بها في جميع مراحل حماية البيانات - وهي جمع البيانات ومعالجتها وتخزينها - لضمان امتثالها للقوانين والتشريعات الحالية. لذا، من الضروري تعيين مسؤول حماية البيانات للإشراف على هذه المعايير ومراقبة الامتثال لها.

كما يتعين على جميع الشركات في الدول الأعضاء في الاتحاد الأوروبي، والتي تتعامل مع البيانات الشخصية، تعيين مسؤول حماية البيانات وذلك بموجب مقتضيات اللائحة العامة لحماية البيانات (GDPR).

ومن أجل ضمان الامتثال الكامل لمعايير حماية البيانات ومواكبة التطورات التكنولوجية والقانونية، يجب على المؤسسات إنشاء برامج تدريب مستمرة. تهدف هذه الأخيرة إلى تعزيز مهارات الموظفين المسؤولين وزيادة الوعي بالممارسات الحسنة لحماية البيانات وبالمخاطر المرتبطة بانتهاكات الخصوصية.

يجب على المنظمة أيضا اتخاذ تدابير تقنية وتطوير بنى تحتية رقمية وإرساء الحوكمة المناسبة لضمان أمن البيانات الشخصية وسريتها. ومن بين هذه التدابير نذكر، تقنيات تشفير البيانات، وتنظيم الولوج إلى قواعد البيانات، وتدابير الأمن السيبراني العامة. كما ينبغي إخضاع أنشطة المؤسسة لمراجعة داخلية منتظمة لتقييم امتثالها للمعايير القانونية لحماية البيانات وإجراء التعديلات اللازمة.

ج. تدريب الموظفين المسؤولين عن معالجة وإدارة البيانات الشخصية على أفضل الممارسات

لتعزيز قدرة المؤسسات في مجال حماية البيانات الشخصية، يجب تدريب موظفيها المسؤولين عن معالجة البيانات الشخصية على أفضل الممارسات. كما يجب أن يستفيد من هذا البرنامج التدريبي جميع الموظفين. ذلك أن تحديد المُستهدفين بالتدريب مُسبقا، بناءً على دور كل موظف ومهمته، من الأهمية بمكان.

يجب أن يتضمن البرنامج التدريبي مواد تبرز مبادئ حماية البيانات وأسسها، والالتزامات القانونية والتنظيمية، والمخاطر المرتبطة بانتهاكات الخصوصية، والتدابير الأمنية الواجب اعتمادها. ولضمان التزام الموظفين، يجب أن يكون البرنامج تفاعليا وشاملًا وأن يتضمن ورش عمل تطبيقية ودراسات حالات. كما ينبغي الاستعانة بمدربين أو خبراء مؤهلين وبالموارد والأدوات المناسبة. ومن الضروري أيضا تنظيم دورات توعوية دورية لتعزيز الممارسات الجيدة والتشجيع على الالتزام بحماية البيانات.

كما تقتضي الحكمة تنفيذ آلية لتقييم آثر برنامج التدريب باستمرار وإجراء تعديلات عليه في سبيل ضمان الامتثال لمعايير حماية البيانات.

وعلى سبيل المثال، أطلقت اللجنة الوطنية لحماية البيانات في فرنسا برنامجا تدريبيا متاح للجميع عبر الإنترنيت لدعم الشركات في الامتثال للائحة العامة لحماية البيانات. يستهدف هذا البرنامج مسؤولي حماية البيانات الحاليين والمستقبليين وكذلك المهنيين الراغبين في التعرف على هذه اللائحة. تتضمن ورش العمل هذه مقاطع فيديو ونصوصًا ورسومًا توضيحية وحالات عملية واختبارات وتقييمات. وتتمحور مضامين الدورة حول الوحدات الأربع التالية:

الوحدة 1: اللائحة العامة لحماية البيانات ومفاهيمها الأساسية؛

الوحدة 2: مبادئ حماية البيانات؛

الوحدة 3: مسؤوليات الجهات المعنية؛

الوحدة 4: مسؤولو حماية البيانات وأدوات الامتثال؛

التدريب مجاني ومتاح للجميع. وفي نهاية كل وحدة، يتسلم المشاركون الذين أكملوا الدورة شهادة تفيد بذلك.

د. اعتماد التقنيات الآمنة لمعالجة البيانات الشخصية

لضمـان أمـن البيانـات الشـخصية، لا سـيما البيانـات الحساسـة، أثنـاء المعالجـة، يجـب اعتمـاد نهـج محـدد وأنظمـة حمايـة متينـة، خاصـة التقنيـات التي تعمـل بخوارزميـات تشـفير معقـدة ومتطـورة. ونذكـر منهـا علـى سـبيل المثـال:

معيـار التشـفير المتقـدم (Advanced Encryption Standard): خوارزميـة تشـفير متماثـل ومـن أكثـر طـرق التشـفير اسـتخداما، وتعتمدهـا الحكومـة الأمريكيـة لحمايـة المعلومـات الحساسـة.

تشفيـــر (Rivest-Shamir-Adleman): خوارزميـة تشـفير غيـر متماثـل تُسـتخدم عـادة لتشـفير الاتصـالات عبـر الإنترنـت. يعتمـد هـذا التشـفير علـى نظـام مفاتيـح ثنـائي (عـام وخـاص) لتشـفير البيانـات وفـك تشـفيرها، وهـو مـا يوفـر حمايـة متطـورة للبيانـات الشـخصية.

تشـفير (Elliptic Curve Cryptography): خوارزميـة تشـفير غيـر متماثلـة ملائمـة لحمايـة البيانـات الشـخصية علـى الأجهـزة المحمولـة وأنظمـة التشـغيل المدمجـة في الأجهـزة.

وتُعـد هـذه التقنيـات وغيرهـا مـن تقنيـات التشـفير ضروريـة لحمايـة البيانـات الشـخصية أثنـاء معالجتهـا ونقلهـا وتخزينهـا. بالإضافـة إلـى ذلـك، فـإن اسـتخدام برنامـج جـدار الحمايـة وبرامـج مكافحـة الفيروسـات كفيـل بمنـع الهجمات الإلكترونيـة والاختراقـات الأمنيـة.

ومـن بيـن إجـراءات الأمـان المعـزز أيضـا نجـد تقنيـة المصادقـة متعـددة العوامـل، والتي تتطلـب اسـتخدام عـدة أرقـام سـرية لتسـجيل الدخـول للحسـابات وإتاحـة الوصـول إلـى البيانـات. كمـا يمكن اسـتخدام أدوات التحقـق مـن الهويـة وتنظيـم الولـوج لإتاحـة البيانـات للأشـخاص الذيـن تخـول لهـم صفتهـم ذلـك أو لـكل مـن يتوفـر علـى تصريـح بذلـك.

3

التربية الرقمية وحماية المعطيات الشخصية

أ. التربية الرقمية والمعطيات الشخصية؛

ب. تنفيذ البرامج التعليمية والتواصلية؛

ج. أفضل الممارسات لاستخدام آمن للتقنيات الرقمية ؛

د. رفع مستوى الوعي والمسؤولية الفردية والجماعية.

أ. التربية الرقمية والبيانات الشخصية

ترتبط التربية الرقمية وحماية البيانات الشخصية ارتباطا وثيقا ببعضهما البعض وهما أمران ضروريان في عالم ما فتئ يزداد تشعبا ورقمنة. وهنا يبرز دور التربية الرقمية في إذكاء الوعي بمشاكل حماية البيانات الشخصية لدى المستخدمين من جميع الأعمار. فهي تساعدهم على فهم مخاطر الكشف عن المعلومات الشخصية على الإنترنت وتزودهم بالمعارف اللازمة لحماية أنفسهم من هذه المخاطر.

بالإضافة إلى ذلك، فإن التربية الرقمية المبنية على أسس متينة ستمكّن الأفراد من تنمية المهارات اللازمة لحماية بياناتهم الشخصية، ذلك أن الإحاطة بالممارسات الجيدة للسرية والخصوصية على المنصات الإلكترونية، والتعرف على مختلف جوانب الجرائم الإلكترونية، وفهم أساليب الهجوم مثل التصيد وسرقة الهوية، سيدفع الناس لتبني ممارسات ناجعة للحفاظ على أمن بياناتهم.

إن إتاحة التربية الرقمية منذ سن مبكرة، مع دمج مفاهيم حماية البيانات وأفضل الممارسات في المناهج التعليمية، له بالغ الأثر في تعزيز ثقافة الخصوصية وأمن البيانات، ومنع انتهاك الخصوصية وتعزيز الثقة في الفضاء الرقمي.

وإن من شأن التربية الرقمية المبنية على أسس متينة أن يذكي الوعي بحقوق الأفراد فيما يتعلق بحماية البيانات والمسؤوليات الملقاة على عاتق معالج البيانات داخل المنظمات، ويساهم في التشجيع على الاستخدام الأخلاقي والمسؤول للتكنولوجيا. ففي النهاية، تعد التربية الرقمية وحماية البيانات عنصرين مكملين لبعضهما البعض، مما يخلق فضاء رقمية أكثر أمانا واحتراما للخصوصية.

ب. تنفيذ البرامج التعليمية والتواصلية

يُعـد تنفيـذ البرامـج التعليميـة والتواصليـة، مثـل "التربيـة الإعلاميـة والمعلوماتيـة"، التي تركـز علـى حمايـة البيانـات الشـخصية حجـر الأسـاس لبنـاء الوعـي الرقمـي وتعزيـز فهـم الأفـراد لمخاطـر الإفصـاح عـن المعلومـات الشـخصية علـى الإنترنـت وخارجـه. وتهـدف هـذه البرامـج إلـى الإحاطـة بالحقـوق والمسـؤوليات وأهميـة حمايـة الخصوصية.

صُممـت هـذه البرامـج لتوعيـة الأفـراد وتثقيفهـم بشـأن حمايـة البيانـات الشـخصية، وتعليمهـم أفضـل الممارسـات لضمـان الأمـان عبـر الإنترنـت. يمكـن تنظيـم هـذه البرامـج، حسـب السـياق والفئـة المسـتهدفة، في شـكل نـدوات تفاعليـة أو دورات تطبيقيـة أو حمـلات توعيـة، سـواء رقميـة أو ميدانيـة، أو دورات أو مـواد تعليميـة.

علـى سـبيل المثـال، اعتمـدت الـدول الإسـكندنافية، وهـي مـن الأنظمـة التعليميـة الرائـدة، برامـج تـروم رفـع الوعـي بحمايـة البيانـات الشـخصية. فالنرويـج مثـلا نفـذت سياسـات تعليميـة لتدريـب المواطنيـن علـى حمايـة بياناتهـم الشـخصية. كمـا تُـدرب النرويج طلابهـا علـى مبـادئ الخصوصيـة عبـر الإنترنـت وأفضـل الممارسـات لحمايتهـا، وكـذا المخاطـر المرتبطـة بمشـاركة المعلومـات الشـخصية. تـروم النرويـج تعريـف طلابهـا علـى حقوقهـم كمسـتخدمين للإنترنـت وتعليميهـم كيفيـة إدارة إعـدادات الخصوصيـة علـى المنصـات الرقميـة، وفهـم شـروط الخدمـة وممارسـة حقوقهـم علـى البيانـات الشـخصية. كمـا أنهـا تـدرب مدرسـيها حـول التوعيـة بحمايـة البيانـات، لنقـل هـذه المعـارف إلـى الطـلاب وتوجيههـم نحـو الاسـتخدام المسـؤول للإنترنـت، كما تشـجع الحكومـة النرويجيـة المـدارسُ علـى إشـراك أوليـاء الأمـور في ورش العمـل والجلسـات التوعويـة.

يجـب تكييـف البرامـج التعليميـة مـع عمـر الطـلاب واحتياجاتهـم بمـا يُمكنهـا مـن تقديـم إرشـادات عمليـة وواضحـة حـول كيفيـة حمايـة البيانـات الشـخصية والتطـرق لمختلـف الجوانـب التقنيـة والقانونيـة لتطويـر مهـارات إدارة الخصوصيـة، وتأميـن كلمـات المـرور، وإفشـال محـاولات التصيـد، والحمايـة مـن البرمجيـات الضـارة، والإحاطـة بقوانيـن حمايـة البيانـات. وفي هـذا الصـدد، يجـب إذكاء الوعـي بالحقـوق المتعلقـة بالخصوصيـة، كالموافقـة علـى معالجـة البيانـات أو رفـض ذلـك، والولـوج إلـى المعلومـات الشـخصية والحـق في تصحيـح المعلومـات الشـخصية.

إن نَهـج طـرق تواصـل ناجعـة كفيـل بنشـر الوعـي الرقمـي الـذي يركـز علـى الحـق في الخصوصيـة وحمايـة البيانـات الشـخصية، ممـا يشـجع علـى زيادة الوعـي الجماعـي والاسـتخدام المسـؤول للتكنولوجيـا.

ج. أفضل الممارسات لاستخدام آمن للتقنيات الرقمية

إن تعزيز حماية البيانات الشخصية في الفضاء الرقمي رهين بوعي مستخدمي الإنترنيت والتكنولوجيا بسلوكياتهم وتوخي الحذر أثناء استخدامهم لها. وهو ما ستعينهم عليه البرامج التدريبية بالإضافة إلى تعليمهم الممارسات التالية:

- استخدام كلمات مرور قوية ومختلفة لكل حساب على الإنترنت: استخدام كلمات مرور تجمع بين الأحرف والأرقام والرموز؛
- تفعيل التحقق الثنائي عند الإمكان: وهو ما سيعزز من أمان حسابات مواقع التواصل الاجتماعي، والبريد الإلكتروني، أو الألعاب الإلكترونية؛
- تقليل المعلومات الشخصية المنشورة عبر الإنترنت: الحرص على تقديم البيانات الشخصية عند الضرورة فقط، مع التأكد من أن المواقع موثوقة وآمنة، وتعديل إعدادات الخصوصية في المواقع الإلكترونية؛
- تثبيت برامج الحماية ومكافحة الفيروسات : وذلك لحماية الأجهزة من البرمجيات الضارة وبرامج التجسس والتهديدات الإلكترونية؛
- تحديث البرامج والتطبيقات وأنظمة التشغيل بانتظام: وذلك للاستفادة من آخر التحديثات الأمنية ومعالجة الثغرات المحتملة.
- تفادي الروابط غير الآمنة أو المرفقات مجهولة أو غير موثوقة المصدر: وذلك للوقاية ضد هجمات التصيد الاحتيالي التي تستهدف البيانات الشخصية أو الحساسة للمستخد مين .
- توخي الحذر عند الاتصال بشبكات الواي فاي العمومية وغير المؤمنة برقم سري: تجنب إجراء معاملات حساسة أو الولوج إلى الحسابات الشخصية.
- الحذر من محاولات الاحتيال أو سرقة الهوية: التحقق من مصدر الرسائل أو البريد والإبلاغ عن أي سلوك مشبوه.

زاد التطور السريع للتقنيات الرقمية من مخاطر البيانات الشخصية، لا سيما مع انتشار الأجهزة الذكية وتزايد استخدام الذكاء الاصطناعي وظهور الميتافيرس. وفي هذا السياق، يتعين علينا تعزيز مستوى اليقظة لضمان الاستخدام الآمن، وذلك من خلال تبني الممارسات التالية:

- التعـرف أكثـر علـى مجـال الأجهـزة الذكيـة (مثـل السـاعات الذكيـة وأتمتـة المنـازل والكاميـرات): وذلـك بفهـم خصائصهـا ووظائفهـا وتفاعلاتهـا مـع الأجهـزة الإلكترونيـة الأخـرى. والحـق أن الأجهـزة الذكيـة تحتـوي علـى ثغـرات في أمـن البيانـات الشـخصية.

- حمايـة البيانـات الشـخصية الحساسـة التي تسـتخدمها أنظمـة الـذكاء الاصطناعـي: مـن خلال اعتمـاد بروتوكـولات أمـان قويـة مثـل التشـفير، وإخفـاء الهويـة مـن خـلال أسـماء مسـتعارة، وإدارة صلاحيـات الولـوج. ولذلـك، يجـب الحـرص علـى أن البيانـات الحساسـة التي تعالجهـا أنظمـة الـذكاء الاصطناعـي آمنـة ومتوافقـة مـع القوانين المعمـول بهـا.

- إنشـاء آليـات مراقبـة مسـتمرة: رصد الاختـلالات والسـلوكيات غيـر الطبيعيـة أثنـاء تطويـر أنظمـة الـذكاء الاصطناعـي، والاسـتجابة السـريعة للمشـاكل التي تـم تحديدهـا درءا لمفاسـده.

- التفطـن لأسـاليب التصيـد الجديـدة بواسـطة الـذكاء الاصطناعـي: يمكـن لهـذه الهجمـات المتطـورة أن تسـتخدم خوارزميـات الـذكاء الاصطناعـي لانتحـال هويـة جهـة مـا وإرسـال الرسـائل باسـمها متجـاوزة بذلـك طـرق الحمايـة التقليديـة، وهـو مـا يسـتدعي اليقظـة والتفطـن لإبطـال هـذه الحيـل.

د. رفع مستوى الوعي والمسؤولية الفردية والجماعية

يُعد رفع الوعي بأهمية حماية البيانات الشخصية والخصوصية في الفضاء الرقمية ضرورة ملحة، خاصة مع تعرض المعلومات الشخصية لمخاطر متنامية نتيجة تطور التقنيات الرقمية، ومنها تطبيقات الذكاء الاصطناعي. فإذكاء الوعي كفيل بإفهام الناس بمخاطر الكشف عن المعلومات الشخصية عبر الإنترنت.

إن حماية البيانات الشخصية مسؤولية مشتركة بين الأفراد ومختلف الجهات الفاعلة، بما في ذلك المجتمع. وفي سبيل ذلك، يتعين على الأفراد اتخاذ التدابير اللازمة لحماية بياناتهم الشخصية من خلال تبني ممارسات آمنة عبر الإنترنت وفهم الجوانب القانونية والتنظيمية. يجب أن يتظافر المجتمع ككل لتعزيز ثقافة حماية البيانات الشخصية، مع التركيز على التوعية بحقوق نشر الصور الشخصية على المنصات الرقمية والشبكات الاجتماعية. بل ويجب أن تُعمم هذه الجهود لتشمل قطاع التعليم، من خلال الآباء والأوصياء والمدرسين لما لهم من دور في هذا المسعى.

4

حماية المعطيات الشخصية في الدول الأعضاء للإيسيسكو

أ. القوانين الوطنية والدولية لحماية البيانات الشخصية؛

ب. تحليل مقارن للتشريعات الوطنية في الدول الأعضاء في الإيسيسكو؛

ج. تحديات توحيد القوانين والممارسات ؛

د. تحديات تنفيذ استراتيجيات التوعية وبناء القدرات.

أ. القوانين الوطنية والدولية لحماية البيانات الشخصية

تؤدي القوانين الوطنية والدولية حول حماية البيانات الشخصية دورا هاما في الحفاظ على خصوصية وأمن الأفراد في فضاء رقمية سريع ودائم التغير. وقد ظهرت المخاوف الدولية الأولى بشأن حماية البيانات والخصوصية في سبعينيات القرن الماضي وكانت سببا في سن التشريعات الحالية استجابة للتقدم التكنولوجي.

وعلى مر العقود، توالت المحطات البارزة في هذا المسار، بما في ذلك اعتماد قوانين هامة مثل قانون الخصوصية في الولايات المتحدة (الثمانينيات)، واتفاقية مجلس أوروبا رقم 108 (1981)، واللائحة العامة لحماية البيانات في الاتحاد الأوروبي (2016) (GDPR). وتهدف هذه القوانين إلى حماية الحقوق الأساسية للأفراد في ظل التطور المتسارع للعالم الرقمي.

كما صاغت منظمات دولية عديدة، مثل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية ومجلس أوروبا، اتفاقيات وتوصيات لتعزيز حماية البيانات الشخصية دوليا. ومن بين أهم هذه الاتفاقيات الإعلان العالمي لحقوق الإنسان (1948)، واتفاقية مجلس أوروبا رقم 108 (1981)، والتوجيه الصادر عن الاتحاد الأوروبي بشأن حماية البيانات (1995) واللائحة العامة لحماية البيانات في الاتحاد الأوروبي (2018).

أما على المستوى الوطني، فقد اعتمدت العديد من الدول قوانين لحماية البيانات، مثل قانون حماية البيانات الشخصية (PDPL) في كوريا الجنوبية، وقانون خصوصية المستهلك في كاليفورنيا (CCPA) في الولايات المتحدة. تُلزم هذه القوانين بوضع معايير ومتطلبات صارمة لجمع ومعالجة وتخزين البيانات الشخصية، بالإضافة إلى آليات لتطبيق هذه القواعد وفرض العقوبات على المخالفات.

والحـق أن هـذه القوانيـن الوطنيـة والدولية تشـكل إطـارًا قانونيًـا متينا يضمــن معالجــة المعطيــات ذات الطابـع الشـخصي بطريقـة أخلاقيـة وآمنــة ومتوافقــة مــع الحقــوق الأساسـية، كمـا أنهـا تشـجع علـى التعــاون بيــن الــدول لمواجهــة التحديــات المتعلقــة بحمايــة المعطيـات العابـرة للحـدود، مثـل عمليــات نقــل البيانــات الدوليــة ومكافحــة الجرائــم الإلكترونيــة. كمـا أنهـا مـن تُعـزز الثقـة الرقميـة وتجعـل مـن الخصوصيـة حقـا مـن الحقــوق الأساســية.

ب. تحليل مقارن للتشريعات الوطنية في الدول الأعضاء في الإيسيسكو

تبنّت بعض الدول الأعضاء في الإيسيسكو مقاربات متنوعة فيما يتعلق بحماية المعطيات ذات الطابع الشخصي، مما يعكس الخصوصيات الثقافية والسياسية والقانونية لكل دولة. فبينما سنَّت معظم الدول قوانين متطورة وصارمة ، لا تزال بعض الدول الأخرى في مرحلة صياغة أطرها القانونية.

وفي هذا السياق، سنسلط الضوء في هذا التحليل المقارن على التقدم المحرز وعلى أوجه التشابه والاختلاف بين القوانين الوطنية فيما يخص تعريفها للمعطيات ذات الطابع الشخصي ومقتضياتها بشأن حقوق الأفراد ومسؤوليات المنظمات وآليات المراقبة والعقوبات في حالة عدم الامتثال. على سبيل المثال، تركز بعض الدول على حماية المعطيات الحساسة مثل البيانات البيومترية أو الطبية، بينما يولي البعض الآخر اهتماماً أكبر بتأمين المعلومات المالية أو التجارية.

كما سنتطرق في هذا التحليل لقوانين الدول الأعضاء في الإيسيسكو بشأن الذكاء الاصطناعي والإنترنت وكيف تعاملت معها. ومن بين القضايا المهمة التي يجب دراستها إدارة البيانات البيومترية، والحماية من الهجمات الإلكترونية، وشفافية المعلومات بخصوص الخوارزميات على أن ذلك سيبين الاستراتيجيات المتبعة لضمان الأمن والسرية في الفضاء الرقمي.

والمتأمل في الأطر القانونية والتنظيمية للدول الأعضاء في الإيسيسكو سيجد تنوعاً في الاستراتيجيات والمقاربات المعتمدة، ومنه تبرز أهمية التعاون الإقليمي والدولي لمواجهة التحديات المشتركة في مجال حماية البيانات.

إن هذا التحليل المقارن والشامل وسيلة لتحديد أوجه الاختلاف في قوانين حماية المعطيات. وهي اختلافات ستقف حجر عثرة أمام تعزيز التعاون وتعيق توحيد الأطر التنظيمية الوطنية. والحق أن وضع معايير مشتركة سيعزز من نجاعة التعاون بين الدول الأعضاء في هذا المجال.

نستعرض في الجدول التالي نظرة شاملة على القوانين الوطنية المتعلقة بحماية البيانات ذات الطابع الشخصي في بعض الدول الأعضاء في الإيسيسكو:

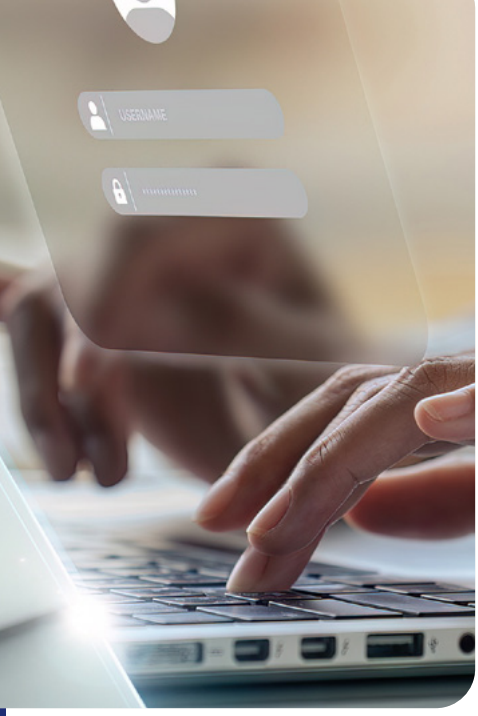
	الدولة العضو	المرجع القانوني	الهيئة المختصة
1	المملكة المغربية	القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع	اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي
2	الجمهورية الإسلامية الموريتانية	القانون رقم 020-2017 الصادر في 22 يوليو 2017، بشأن حماية البيانات ذات الطابع الشخصي.	سلطة حماية البيانات ذات الطابع الشخصي (APDCP)
3	جمهورية النيجر	القانون رقم 31-2023 المؤرخ في 4 يوليو 2023، والمعَدِّل للقانون رقم 59-2022 الصادر في 16 ديسمبر 2022 بشأن حماية البيانات ذات الطابع الشخصي، وكذا القانون رقم 59-2022 المؤرخ في 16 ديسمبر 2022، بشأن حماية البيانات ذات الطابع الشخصي.	الهيئة العليا لحماية المعطيات ذات الطابع الشخصي (HAPDP)
4	جمهورية نيجيريا الاتحادية	قانون نيجيريا بشأن حماية المعطيات (الصادر في 2023)	لجنة نيجيريا لحماية البيانات (NDPC)
5	الجمهورية اليمنية	لا يوجد	لا توجد
6	جمهورية البنين	يخضع بروتوكول حماية البيانات في بنين لنصين تشريعيين: قانون رقم 20-2017 المؤرخ في 20 أبريل 2018، بشأن الإنترنت والقانون رقم -2009 09 المؤرخ في 22 مايو 2009 بشأن حماية البيانات ذات الطابع الشخصي.	هيئة حماية المعطيات ذات الطابع الشخصي (APDP)
7	جمهورية كوت ديفوار	قانون 450-2013 بشأن حماية المعطيات ذات الطابع الشخصي.	هيئة تنظيم الاتصالات وتكنولوجيا المعلومات والاتصالات بكوت ديفوار
8	دولة الكويت	قرار رقم 42 لسنة 2021 بشأن تنظيم حماية سرية البيانات	الهيئة العامة للاتصالات وتقنية المعلومات

9	الجمهورية اللبنانية	قانون رقم 81 لسنة 2018 بشأن المعاملات الإلكترونية والبيانات ذات الطابع الشخصي	وزارة الاقتصاد والتجارة
10	دولة ليبيا	المادتان 12 و13 من دستور 2011	لا توجد
11	جمهورية المالديف	لا يوجد قانون محدد	لا توجد
12	جمهورية مالي	قانون رقم 015-2013	هيئة حماية المعطيات ذات الطابع الشخصي
13	ماليزيا	قانون حماية المعطيات ذات الطابع الشخصي 2010 (PDPA)	إدارة حماية المعطيات ذات الطابع الشخصي
14	جمهورية مصر العربية	قانون حماية البيانات الشخصية رقم 151 لسنة 2020	مركز حماية البيانات الشخصية
15	جمهورية غينيا	قانون رقم 37/2016 بشأن الأمن السيبراني وحماية البيانات الشخصية	الهيئة المكلفة بالأمن السيبراني ANSSI
16	دولة فلسطين	لا يوجد	لا توجد
17	جمهورية كازاخستان	القانون رقم V-94 المؤرخ في 21 مايو 2013	وزارة التنمية الرقمية والابتكار والفضاء
18	دولة قطر	القانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية	شؤون الحوكمة والضمان السيبراني الوطني NCGAA
19	اتحاد جزر القمر	لا يوجد	لا توجد
20	جمهورية قيرغيزستان	القانون رقم 58 الصادر في 14 أبريل 2008	الوكالة الوطنية لحماية المعطيات ذات الطابع الشخصي

21	جمهورية الكاميرون	قانون رقم 2010/013 المؤرخ في 21 ديسمبر 2010، المعدل والمكمل للقانون رقم 2015/06 المؤرخ في 20 أبريل 2015، بشأن تنظيم الاتصالات الإلكترونية	هيئة الكاميرون لحماية المعطيات الشخصية
22	جمهورية سيراليون	لا يوجد	لا توجد
23	جمهورية السنغال	القانون رقم 12-2008 الصادر في 25 يناير 2008	لجنة حماية المعطيات ذات الطابع الشخصي
24	جمهورية الصومال الفيدرالية	القانون رقم 005 لسنة 2023	هيئة حماية المعطيات
25	جمهورية العراق	لا يوجد	لا توجد
26	سلطنة عمان	المرسوم السلطاني رقم 6 لسنة 2022 بشأن إصدار قانون حماية البيانات الشخصية	لا توجد
27	جمهورية الغابون	القانون رقم 025/2023 المؤرخ في 9 يوليو 2023، المعدل للقانون رقم 001/2011 المؤرخ في 25 سبتمبر 2011	هيئة حماية المعطيات ذات الطابع الشخصي والخصوصية (APDPVP)
28	جمهورية غامبيا	مشروع قانون قيد التشريع	لا توجد
29	جمهورية غيانا التعاونية	القانون رقم 18 لسنة 2023 بشأن حماية المعطيات ذات الطابع الشخصي	هيئة حماية البيانات
30	الجمهورية التونسية	القانون رقم 014-2019 المؤرخ في 29 أكتوبر 2019	الهيئة الوطنية لحماية المعطيات الشخصية
31	الجمهورية الجزائرية الديمقراطية الشعبية	القانون التنظيمي رقم 63469 – 2004، مرسوم رقم 3003470 – 2007	الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي

32	جمهورية جيبوتي	مشروع قانون قيد التشريع	لا توجد
33	المملكة العربية السعودية	مرسوم ملكي رقم م/19 المؤرخ في 9/2/1443هـ (الموافق 16 سبتمبر 2021م)، المعدل للمرسوم الملكي رقم م/148 المؤرخ في 5/9/1444هـ (الموافق 27 مارس 2023م)	الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)
34	جمهورية السودان	لا يوجد	لا توجد
35	جمهورية سورينام	مشروع قانون قيد التشريع	لا توجد
36	الجمهورية العربية السورية	لا يوجد	لا توجد
37	جمهورية باكستان الإسلامية	مشروع قانون قيد الدرس	لا توجد
38	مملكة البحرين	القانون رقم 30 لسنة 2018، الذي دخل حيز التنفيذ بتاريخ 1 أغسطس 2019، والمتعلق بحماية البيانات ذات الطابع الشخصي	وزارة العدل والشؤون الإسلامية والأوقاف
39	بروناي دار السلام	مشروع قانون حماية المعطيات ذات الطابع الشخصي لعام 2021	هيئة قطاع تكنولوجيا المعلومات والاتصالات
40	جمهورية بنغلاديش الشعبية	لا يوجد قانون محدد قانون الأمن السيبراني لعام 2023	وكالة الأمن السيبراني
41	بوركينا فاسو	القانون رقم AN/010-2004	هيئة تكنولوجيا المعلومات والحريات
42	جمهورية طاجيكستان	القانون رقم 1537 المؤرخ في 3 أغسطس 2018، والقانون رقم 631 المؤرخ في 15 مايو 2002 بشأن حماية البيانات	مصلحة خدمات الاتصالات في حكومة جمهورية طاجيكستان

43	جمهورية تشاد	القانون رقم PR/2015/007 بشأن حماية البيانات	الوكالة الوطنية لأمن الحاسوب والشهادات الإلكترونية
44	الجمهورية الإسلامية الإيرانية	لا يوجد قانون محدد	لا توجد
45	جمهورية أوغندا	القانون رقم 9 لسنة 2019 بشأن حماية البيانات والخصوصية	مكتب حماية المعطيات ذات الطابع الشخصي التابع للهيئة الوطنية لتكنولوجيا المعلومات
46	المملكة الأردنية الهاشمية	القانون رقم 24/2023 بشأن حماية البيانات الشخصية	لا توجد
47	جمهورية أوزبكستان	القانون رقم ZRU-547 بشأن البيانات الشخصية	وكالة التخصيص التابعة لوزارة العدل
48	جمهورية إندونيسيا	مشروع قانون قيد التشريع	لا توجد
49	الإمارات العربية المتحدة	مرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية	مكتب الإمارات للبيانات
50	جمهورية أفغانستان الإسلامية	لا يوجد	لا توجد
51	جمهورية أذربيجان	رقم IIIQ-998 بتاريخ 11 مايو 2010 بشأن البيانات الشخصية	وزارة النقل والاتصالات والتكنولوجيا العالية



ج. تحديات توحيد القوانين والممارسات

إن توحيد القوانين الدولية والممارسات الفضلى في مجال حماية البيانات الشخصية من الأهمية بمكان وذلك لأثره في اتساق الأطر القانونية على المستوى الدولي، وهو ما يعين الشركات والمنظمات الدولية على الامتثال. كما أن توحيد البيانات كفيل بإرساء ركائز الشفافية والأمان للبيانات المتداولة عالميًا وتسهيل التعاون الدولي في مكافحة التهديدات العابرة للحدود ومنها الجرائم الإلكترونية. غير أن الاختلافات الثقافية والسياسية والقانونية بين الدول تقف حجر عثرة في سبيل توحيد القوانين، و تزيد من صعوبة وضع معايير وقواعد إقليمية أو عالمية. والحق أن لكل دولة سماتها الخاصة ونهجها في حماية البيانات ونظامها القانوني، مما يعقد مهمة توحيد المعايير والقوانين.

كما أن التطور التكنولوجي المتسارع يعيق هذا المسعى، ذلك أن بعض التقنيات، على غرار الذكاء الاصطناعي وإنترنت الأشياء وسلسلة الكتل (blockchain)، تُحدِث خللا على مستوى جمع البيانات الشخصية ومعالجتها والتعامل معها وهو ما يستدعي تطويع القوانين وجعلها أكثر مرونة. فيما تواجه الشركات والمنظمات الدولية صعوبات في الامتثال بسبب اختلاف القوانين بين الدول.

تُظهر المخاطر المتزايدة لخرق البيانات الشخصية وانتهاكات الخصوصية بجلاء الحاجة إلى مزيد من القواعد القانونية الموحدة بين البلدان. فعلى سبيل المثال، اعتمدت دول الاتحاد الأوروبي اللائحة العامة لحماية البيانات لتوحيد القوانين وتسهيل تبادل البيانات داخل الاتحاد.

ولمواجهة التحديات المذكورة، فلا مندوحة عن توحيد القوانين وتعميم الممارسات الناجحة في مجال حماية البيانات. فهي الضامن للحقوق الأساسية للأفراد، والمُعزز لعملية تبادل البيانات دوليا دونما قيود. كما أن توحيدها سيسهل التجارة والتعاون الدولي. والحق أن تحقيق هذا الهدف رهين بالتعاون وتظافر الجهود بين الحكومات والمنظمات الدولية والشركات والمجتمع المدني لوضع معايير ومبادئ مشتركة واستعادة الثقة والشفافية في التعامل مع البيانات الشخصية على المستويين الإقليمي والدولي، خاصةً بين الدول ذات الثقافات أو المرجعيات المشتركة.

د. تحديات تنفيذ استراتيجيات التوعية وبناء القدرات

يواجـه تنفيـذ اسـتراتيجية التوعيـة والتدريـب في مجـال حمايـة البيانـات العديـد مـن التحديـات العمليـة، علـى رأسـها صعوبـة إذكاء وعـي العامـة، حيـث لا يـدرك معظمهـم مخاطـر الكشـف عـن بياناتهـم الشـخصية. بالإضافـة إلـى ذلـك، يجـب تصميـم برامـج التوعيـة وبنـاء القـدرات بمـا يـلبي احتياجـات مختلـف الفئـات ومداركهـم، ومنهـم المهنيـون ومسـتخدمي الإنترنيـت الشـباب والأطفـال. وهـذا يسـتلزم وضـع اسـتراتيجيات ناجعـة مصممـة لتلبيـة احتياجـات كل فئـة مسـتهدفة.

ولمواكبـة التغيـرات التكنولوجيـة وتطـور ممارسـات حمايـة البيانـات الشـخصية، وَجَـبَ تنقيـح محتويـات مناهـج التدريـس باسـتمرار. ومـن ناحيـة أخـرى، فـإن إقصـاء فئـات بعينهـا مـن برامـج التوعيـة يضعـف تأثيـر ونجاعـة التدريـب علـى المـدى الطويـل. فتنفيـذ اسـتراتيجيات التوعيـة والتدريـب يتطلـب مـوارد ماليـة وبشـرية مدربـة ، الأمـر الـذي يمكـن أن يعيـق تنفيـذ برامـج توعيـة وتدريـب مفيـدة وشـاملة وطويلـة الأجـل.

كمـا أن وضـع آليـات لتقييـم اسـتراتيجيات التوعيـة أو التدريـب خطـوة لا محيـد عنهـا لقيـاس أثـر البرامـج ونجاعتهـا وإجـراء التعديـلات اللازمـة لتحسـين اسـتراتيجية حمايـة البيانـات الشـخصية علـى الإنترنـت.

5 دد

تعزيز التعاون بين الدول الأعضاء في الإيسيسكو

"

أ. نماذج لآليات التعاون الناجحة؛

ب. تطوير المعايير الأساسية والالتزام بها؛

ج. آليات التعاون وبناء القدرات في الدول الأعضاء في الإيسيسكو ؛

أ. نماذج لآليات التعاون الناجحة

لا محيد عن التعاون الدولي في مجال حماية البيانات الشخصية لضمان حماية أكبر وأكثر موثوقية للبيانات دوليا، وبالتالي تعزيز ثقة الأفراد في استخدام التقنيات الرقمية. كما أنه سيسهّل تبادل المعلومات وأفضل الممارسات بين هيئات حماية البيانات وتعزيز قدرتها على الاستجابة للتحديات الجديدة في مجال حماية البيانات. وعلاوة على ذلك، فإن التعاون الدولي سبيل لتوحيد معايير وقوانين حماية البيانات والتقليل من المشاكل التي تعترض التنمية الدولية وتسهيل نقل البيانات عبر الحدود في احترام تام لحقوق الخصوصية.

وإدراكاً منها لمختلف مزايا التعاون الدولي، اختارت عدة دول سن نصوص واتفاقيات دولية وإقليمية. وتعد اتفاقية مجلس أوروبا رقم 108 و+108 أول نص قانوني مُلزم في مجال حماية البيانات على المستوى الدولي. وفرت الاتفاقية إطارا للتعاون بين الدول الأعضاء في مجلس أوروبا لحماية البيانات الشخصية ومهدت الطريق لباقي دول العالم لاعتماد معايير مشتركة.

بالإضافة إلى ذلك، تهدف اتفاقية التعاون بين الاتحاد الأوروبي واليابان في مجال حماية البيانات الشخصية إلى تسهيل نقل هذه الأخيرة بين الاتحاد الأوروبي واليابان من خلال إقرار كلا الطرفين بكِفَايَة أنظمة حماية البيانات بينهما وتمكين الشركات العاملة داخل طرفي هذه الاتفاقية من نقل البيانات بشكل آمن ودون الحاجة إلى آليات ضمان إضافية.

مـن جانبهـا، يضـم فريـق العمـل المـعني بحوكمـة البيانـات والخصوصيـة في الاقتصاد الرقمـي (DGP)، التابـع لمنظمـة التعـاون الاقتصـادي والتنميـة، ممثليـن عـن الحكومـات والمنظمـات الدوليـة لمناقشـة التحديـات الأخيـرة في مجـال حمايـة البيانـات ووضـع مبـادئ توجيهيـة وتوصيـات للسياسـات الوطنيـة.

كمـا أنشـأت بعـض الـدول شـبكات إقليميـة لحمايـة البيانـات، وهـي آليـات لتيسـير التعـاون وتبـادل المعلومـات بيـن هيئـات حمايـة البيانـات إقليميـا وخلـق أرضيـة لتبـادل أفضـل الممارسـات وتنسـيق عمليـات التحقيـق العابـرة للحـدود وتعزيـز التقـارب في معاييـر حمايـة البيانـات. ومـن أمثلـة ذلـك، نذكـر الشـبكة الإفريقيـة لهيئـات حمايـة المعطيـات الشـخصية (NAD-PA/RAPDP)، ورابطـة دول جنـوب شـرق آسـيا (ASEAN) والشـبكة الأيبيريـة الأمريكيـة لحمايـة البيانـات (IDPN).

يُمكـن إجـراء تحليـل مقـارن بسـيط للاطـلاع علـى مبـادرات التعـاون وجهـود توحيـد القوانيـن الوطنيـة بيـن الـدول الأعضـاء في الإيسيسـكو بهـدف تعزيـز حمايـة البيانـات الشـخصية علـى المسـتويين الإقليمـي والدولـي. ويمكـن أن يشـمل هـذا اتفاقيـات تبـادل المعلومـات وبرامـج المسـاعدة التقنيـة وآليـات التعـاون.

ب. تطوير المعايير الأساسية والالتزام بها

في ظل انتشار الخدمات الرقمية وزيادة تبادل البيانات عبر الحدود، بات من الضروري وضع معايير مشتركة وإنشاء إطار عمل رصين وموحد لحماية البيانات. إن وضع هذه المعايير الأساسية المشتركة وضمان الامتثال لقوانين حماية البيانات لمن الأهمية بمكان نظرا لمنافعه الجمة.

كما أن المعايير المشتركة تُبسط من فهم المنظمات والشركات والهيئات المختصة لقواعد حماية البيانات وتطبيقها. كما أنها تعزز ثقة الأفراد في طرق معالجة بياناتهم الشخصية، مما يضمن مستوى عالٍ وموحد من الحماية بغض النظر عن معالج البيانات. وعلاوة على ذلك، فإن الالتزام بمعايير حماية البيانات الشخصية يعزز من مصداقية وسمعة المنظمات والشركات ويحسن علاقاتها مع الأفراد ويُنمي موثوقية الخدمات الرقمية.

وأخيرًا، تعمل آلية التعاون الدولي لحماية البيانات الشخصية على تيسير نقل البيانات عبر الحدود من خلال تقليل العوائق التنظيمية والقانونية، لا سيما في قطاع التجارة الإلكترونية، وبالتالي تعزيز المنافسة العادلة في السوق العالمية.

ج. آليات التعاون وبناء القدرات في الدول الأعضاء في الإيسيسكو

وإدراكاً منا بمزايا التعاون الدولي في مجال حماية البيانات الشخصية، أصبح من الضروري وضع آليات وإطار مؤسسي لتعزيز التعاون بين الدول الأعضاء في الإيسيسكو. كما ينبغي النظر في المبادئ التوجيهية والمقاربات التالية:

- إنشاء شبكات إقليمية للدول الأعضاء في الإيسيسكو وتدارس قضايا حماية البيانات الشخصية مع الدول الأخرى. ستعزز هذه المبادرة التعاون بين هيئات حماية البيانات والحكومات والشركات ومنظمات المجتمع المدني لتبادل الخبرات وأفضل الممارسات والموارد. وستُصمَّم هذه الشبكات على نحو يُراعي ويستفيد من أوجه التشابه الثقافي واللغوي والجغرافي بين الدول الأعضاء في الإيسيسكو.
- عقد اتفاقيات ثنائية أو متعددة الأطراف للتعاون بين هيئات حماية البيانات على المستوى الإقليمي لتسهيل تبادل المعلومات وحل المشكلات الطارئة، والتحقيق في حوادث أمن البيانات لاتخاذ التدابير المناسبة. علاوة على ذلك، سيُرسي هذا التعاون أسس وضع معايير مشتركة وممارسات فضلى، بما يعزز التقارب بين القوانين ويوجه المنظمات والشركات نحو الالتزام بها.
- إنشاء مجلس للشبكات الإقليمية أو مركز أو منتدى ذو بعد عالمي واستراتيجي لتوحيد القوانين بين مختلف المناطق والدول واعتماد معايير وممارسات مشتركة في جميع الدول الأعضاء في الإيسيسكو مع مراعاة انتماءها السابق أو الحالي للشبكات والتجمعات العالمية الأخرى.

إن إنشاء آلية مؤسسية للتعاون بين الدول الأعضاء في الإيسيسكو سيكون معينا على بناء قدرات الهيئات المعنية بحماية البيانات الشخصية من خلال توفير إطار لتنفيذ التدريب المتخصص ودعم الموارد البشرية ومساعدتها على مواجهة التحديات الناشئة في مجال حماية البيانات، ومن ذلك أمن البيانات الرقمية وحماية الخصوصية والامتثال للأنظمة. كما أن آليات التعاون ستذكي الوعي العام بشأن قضايا حماية البيانات الشخصية وحقوق الأفراد في الخصوصية لبناء وتعزيز الثقة في استخدام التقنيات الرقمية

6

خـــــاتمة

أضحت حماية البيانات الشخصية ركيزة من ركائز حقوق الإنسان في عالم رقمي ما فتئ يتطور. قدمنا في هذا الدليل نبذة عامة عن المبادئ والممارسات الفضلى والقوانين المعمول بها في مجال حماية البيانات الشخصية، كما استعرضنا الوضع الحالي لمجال حماية البيانات الشخصية في الدول الأعضاء في الإيسيسكو وخارجها.

وإذ وضَّحنا أهمية التربية الرقمية في حماية البيانات الشخصية والخصوصية وعرضنا أفضل الممارسات والتوصيات، رُمنا تذكير الأفراد بضرورة الامتثال لمعايير ومتطلبات حماية البيانات. ذلك أن الدليل يتوخى بناء فضاء رقمي سليم وآمن وشامل ومراعي لخصوصيات جميع الفئات، وذلك من خلال زيادة الوعي بالمخاطر المحتملة والتشجيع على اتخاذ تدابير استباقية. كما أكَّدنا على أهمية وضع آليات للتعاون الدولي بين الدول الأعضاء في الإيسيسكو وضرورة التركيز على التعلم مدى الحياة لمواجهة تحديات حماية البيانات. ويعتبر هذا الدليل بمثابة مصدر أولي لتطوير أدوات وصياغة مواد تعليمية تُنمي قدرات صانعي القرار والمستخدمين والمهنيين على حد سواء.

7

مسرد المصطلحات

البيانات الشخصية: المعلومات التي تحدد هوية الفرد بشكل مباشر أو غير مباشر.

معالجة البيانات: عملية جمع البيانات وتسجيلها وتنظيمها وتخزينها وتكييفها وتعديلها واستخراجها والبحث فيها واستخدامها وإبلاغها ونشرها وتقييدها وإتلافها وما إلى ذلك، بموجب القانون.

هيئة حماية البيانات: هيئة حكومية مستقلة مسؤولة عن مراقبة الالتزام بالقوانين والأنظمة الخاصة بحماية البيانات الشخصية.

قابلية نقل البيانات: حق الشخص في استرداد بياناته الشخصية ونقلها من مزود خدمة إلى آخر.

الموافقة: موافقة الفرد الصريحة أو الضمنية على معالجة بياناته الشخصية.

الموافقة المستنيرة: الموافقة التي يمنحها الفرد بعد اطلاعه كاملا على مقتضيات وتبعات عملية معالجة بياناته.

معالج البيانات: الشخص أو المؤسسة التي تحدد مقاصد معالجة البيانات الشخصية ووسائل معالجتها.

مقاولات المناولة: الشخص أو المؤسسة التي تعالج البيانات الشخصية نيابةً عن معالج البيانات.

الحق في محو الأثر: حق الأفراد في طلب حذف بياناتهم الشخصية، خاصةً إذا انتفت الحاجة التي جُمعت أو عولجت من أجلها.

حقوق الصورة: حق الأفراد في التحكم في كيفية استخدام صورهم وتوزيعها.

التنميط: استخدام البيانات الشخصية لتقييم جوانب معينة من الشخص، مثل تفضيلاته واهتماماته وصحته ووضعه الاقتصادي وموثوقيته أو لتوقع سلوكه.

مسرد المصطلحات

نقل البيانات إلى الخارج: نقل البيانات الشخصية من بلد إلى آخر أو إلى منظمة دولية.

خرق البيانات: الوصول غير المصرح به إلى البيانات الشخصية أو الإفصاح عنها أو تغييرها أو إتلافها.

إخفاء الهوية: محو أثر كل المعلومات الشخصية، المباشرة وغير المباشرة، التي قد تؤدي إلى تحديد هوية الفرد.

تشفير البيانات: استخدام برنامج كمبيوتر لتحويل البيانات إلى صيغة غير مقروءة من قبل أطراف ثالثة، باستثناء أولئك الذين يمتلكون مفتاح فك التشفير.

الذكاء الاصطناعي: الخوارزميات والنماذج الرياضية المستخدمة لإنشاء أنظمة يمكنها التعلم والتفكير واتخاذ القرارات بالاستناد على البيانات.

جهاز متصل بالإنترنت: جهاز مزود بتقنيات الاتصال بالشبكة، مما يسمح له بإرسال واستقبال البيانات والرسائل عبر الإنترنت.

الميتافيرس: عالم افتراضي يُمكّن المستخدمين من التفاعل والتواصل مع بعضهم البعض ومع الفضاء الافتراضي آنيا.

8

روابط هامة

https://www.dataguidance.com/laws

https://cybersecuritymag.africa/etats-des-lieux-des-legislations-sur-protection-donnees-personnelles-afrique

https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-French.pdf

https://www.dlapiperdataprotection.com/index.html?t=law&c=SA

https://paradigmhq.org/wp- content/uploads/2023/07/Londa-2022-Gambia-Eng.pdf

https://www.dataguidance.com/opinion/brunei-darussalam-new-data-protection-regime-focus

https://help.openai.com/en/

JOIN US ! انضموا إلينا REJOIGNEZ-NOUS