إرشادات حماية البيانات الشخصية في إفريقيا

مبادرة مشتركة لجميعة الإنترنت ومفوضية الاتحاد الأفريقي

9 مايو 2018

African Union

Internet Society

مقدمة

في 2014، تبنى أعضاء الاتحاد الأفريقي (AU) اتفاقية الاتحاد الأفريقي حول أمن الفضاء الإلكتروني وحماية البيانات الشخصية ("الاتفاق")[1]. أكّد وزراء الاتحاد الأفريقي المسؤولين عن تكنولوجيا المعلومات والاتصالات (CICT) وخدمات البريد التزامهم بالاتفاق الصادر عن اللجنة الفنية المتخصصة التابعة للاتحاد الأوروبي حول الإعلان الوزاري المعني بتكنولوجيا المعلومات والاتصالات (AU/CCICT-2)[2].

وضع الإعلان هدفًا قويًا للعمل الأفريقي في موضوع أمن الفضاء الإلكتروني، وحماية البيانات الشخصية بغرض تقديم الميزات لأفريقيا. وعلى وجه الخصوص، طالبت مفوضية الاتحاد الأفريقي (AUC) بوضع إرشادات عن حماية البيانات الشخصية (فقرة 31).

لتسهيل تنفيذ الاتفاق، طلبت مفوضية الاتحاد الإفريقي من جمعية الإنترنت (ISOC) الاشتراك في وضع تعليمات الخصوصية وحماية البيانات الشخصية ("التعليمات"). تمت صياغة التعليمات بمساهمات من خبراء خصوصية إقليميين، وعالميين بما في ذلك أخصائي الخصوصية في المجال، والأكاديميين، ومجموعات المجتمع المدني.

تشدد التعليمات على أهمية ضمان الثقة في الخدمات عبر الإنترنت، كعامل أساسي في الحفاظ على اقتصاد رقمي ومثمر، ومفيد. كما أنها توفر أيضًا توجيهات حول كيفية مساعدة الأفراد على أخذ دور أكثر فاعلية في حماية بياناتهم الشخصية، مع التسليم بأن في مناطق كثيرة، تعتمد النتائج الإيجابية للأفراد على العمل الإيجابي الذي يقوم به أصحاب المصالح الآخرين.

لقد حددت التعليمات 18 توصية، مجمّعة في ثلاثة عناوين:

- اثنان من المبادئ الأساسية لتكوين الثقة، والخصوصية، والاستخدام المسؤول للبيانات الشخصية
- ثمانية توصيات لاتخاذ إجراء بشأنها من قبل أصحاب المصالح التاليين:
  - الحكومات وواضعو السياسات
  - سلطات حماية البيانات (DPAs)
  - مراقبو البيانات ومعالجو البيانات
- ثمانية توصيات حول المواضيع التالية:
  - حلول أصحاب المصالح المتعددين
  - سلامة المواطن الملم بالتكنولوجيا الرقمية
  - تدابير التمكين والاستدامة

تُعد الخصوصية وحماية البيانات الشخصية أحد النطاقات الواسعة والمتغيّرة باستمرار؛ فالتعليمات ليست نهاية المطاف – وإنما هي مخطط لعملية مستمرة لتطوير السياسة، والتوجيهات التشغيلية، وأفضل الممارسات، مع ظهور متطلبات، وظروف جديدة.

1 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

2 https://au.int/sites/default/files/newsevents/reports/33025-rp-addis_ababa_declaration_of_the_stc-cict-2_en.pdf (فقرة رقم 31)

جدول المحتويات

ملخص تنفيذي

يلخص هذا الجزء الأدوار الأساسية ومسؤوليات مجموعات أصحاب المصالح الأساسيين فيما يتعلق بحماية البيانات الشخصية.

الحكومات وواضعو السياسات

الدور: تعزيز المواطن الرقمي، والتأكد من أن البيئة عبر الإنترنت موثوق بها، وآمنة، ومفيدة لكل أصحاب المصالح.

المسؤوليات:

- تعزيز فهمهم لميزات وأخطار الاقتصاد القائم على البيانات.
- فهم القوى الاجتماعية، والاقتصادية العاملة ضمن نظام ايكولوجي خاص بالبيانات الشخصية.
- غرس إطار اجتماعي طويل الأجل لتحقيق الثقة في الاقتصاد الرقمي، والتأكد من توزيع الميزات بصورة منصفة.

هذه هي أهداف المبادئ الأساسية، وتدابير التمكين والاستدامة.

سلطات حماية البيانات (DPAs)

الدور: تعزيز التيّقن القانوني، عن طريق تطبيق قوانين حماية البيانات، والتحقيق في انتهاكات الخصوصية المزعومة، وفرض عقوبات متى أمكن، والعمل مع مجموعات أصحاب المصالح، وسلطات حماية البيانات (DPAs).

المسؤوليات:

- توفير إسهامات الخبراء للحكومات حول قوانين وسياسة حماية البيانات.
- إعطاء توجيهات واضحة لمراقبي البيانات، ومصنّعي/مطوّري المنتجات والخدمات.
- مراعاة الإنفاذ الفعّال للوائح حماية البيانات، بما في ذلك عملية التحقيق، والعقوبات.
- تقديم المشورة والمساعدة للأشخاص موضوعي البيانات.
- التنسيق مع سلطات حماية البيانات (DPAs) الأخرى من أجل دعم قواعد حماية بيانات عبر الحدود متسقة وإنفاذها.

مراقبو البيانات وشركائهم

الدور: إنشاء وتطبيق ممارسات مسؤولة ومستدامة لمعالجة البيانات الشخصية التي تعكس اهتمامات الشخص المعني بالبيانات وأيضًا تلك الخاصة بمراقبي البيانات وشركائهم.

المسؤوليات:

- مضاعفة الثقة، كتوقع للمواطن/العميل/المستخدم، وكميزة تقدمها خدماتك، ومنتجاتك، وكأصل اقتصادي لمؤسستك. الثقة تعزز السمعة، وتقوي الموافقة، ويمكن أن تقدّم ميزة تنافسية في أي سياق تجاري.
- معالجة المشاكل العملية لحماية البيانات الشخصية (الموافقة، فترات الاحتفاظ بالبيانات، وأمن البيانات، إلخ)، مع المزيج الصحيح من التدابير الفنية، والإجرائية.
- زيادة استخدام الخصوصية تبعًا للتصميم (PbD)، والتصميم القائم على القيمة[3]، كجزء متكامل من تطور المنتج/الخدمة.

3 تركّز معظم معالجات تصميم المنتجات في الأساس على جوانب مثل الوظيفة، والشكل، والنواحي الجمالية، والتكلفة. يقر كل تصميم يعتمد على القيمة أن كل اختيار من اختيارات التصاميم لديها بعد أخلاقي، وتدمج اعتبارات أخلاقية بطريقة منهجية في التصميم، ونمط الحياة المتطور.

المواطنون والمجتمع المدني

الدور: تشكيل مواطنين ملمين بالتكنولوجيا الرقمية الفعالة؛ ليصبحوا أصحاب مصالح فعّالين يتحكمون في خصوصيتهم وبياناتهم الشخصية.

المسؤوليات:

- فهم المخاطر التي تنطوي عليها الحياة عبر الإنترنت.
- فهم وممارسة الحقوق المرتبطة بالبيانات الشخصية، والخصوصية، والاستقلالية.
- تطوير إمكاناتك في حماية اهتماماتك عبر الإنترنت، سواء بطريقة مباشرة، أو عن طريق استخدام أدوات، وخدمات تساعد في تعزيز خصوصيتك.
- تشكيل صوت موحد (مع العميل، ومنظمات المجتمع المدني) لتحويل السوق الاستهلاكية نحو خصوصية أفضل.

مهام أصحاب المصالح المتعددين

لكل صاحب مصلحة دور في خلق منظومة موثوق بها عبر الإنترنت بصورة جماعية تعمل لصالح الجميع.

تقوم الخصوصية على احترام توقعات الأفراد فيما يتعلق بكيفية معالجة معلوماتهم الشخصية؛ تعتمد الخصوصية على علاقة احترام، بين الفرد، وأصحاب المصالح الذين يقومون بجمع، واستخدام بيانات عنه. تتحقق خصوصية أفضل عبر الإنترنت عندما يكون لكل شخص دور في الحل.

تتطلب الكثير من المشكلات العملية لحماية البيانات عملاً جماعيًا من قِبل أكثر من صاحب مصلحة؛ على سبيل المثال،

- تطوير مدونات قواعد سلوك تتضمن أفضل الممارسات (سلطات حماية البيانات (DPA)، ومراقبي البيانات، والهيئات الصناعية)؛
- إنشاء وتشغيل مخططات التصديق لحماية البيانات (سلطات حماية البيانات (DPA)، ومنظمات المستهلكين، وهيئات التصديق والمعايير)؛ و
- موافقة المستخدم، واحترام سياقات الخصوصية[4] (سلطات حماية البيانات (DPA)، ومراقبي البيانات، وهيئات العملاء).

هذه هي الأعمال الموصى بها تحت عنوان "حلول أصحاب المصالح المتعددين".

4 تعرف الخصوصية في الغالب باحترام السياق الذي كشفت فيه المعلومات، وعدم مشاركتها أو إعادة استخدامها في السياقات الأخرى (على سبيل المثال، عدم أخذ البيانات الطبية الخاصة ونشرها في أي صحيفة).

الإقرارات

نود أن نعرب عن تقديرنا للمساهمات التي لا تقدر بثمن لروبين ويلتون (جمعية الإنترنت)، الذي عمل على المسودة الأولى للتعليمات، وتلقى مسودات متتالية بناءً على مدخلات من خبراء مساهمين. ونود أيضًا أن نعرب عن تقديرنا لمساهمات كل مما يلي، جميعهم شاركوا في ورشة عمل الخبراء لتحديد ومناقشة المواضيع الأساسية لهذه التعليمات وعلّق على نص المسودة:

سهيلة امازوز (مفوضية الاتحاد الأفريقي)
ياوفي عطوحون (آيكان)
داويت بيكيلي (جمعية الإنترنت)
أليباشو برهانو (جامعة بحر دار)
بيتيل هايلو (جمعية الإنترنت)
فيرينجاي مابيكا (جمعية الإنترنت)
إيفلين نامارا (جمعية الإنترنت)
مارسما تاريكو (جمعية الإنترنت)
واكابي وايراغالا (منظمة التعاون لسياسات تكنولوجيا الاتصالات والمعلومات في شرق وجنوب أفريقيا)
أوغست يانكي (مفوضية الاتحاد الأفريقي)
مختار يدلي (مفوضية الاتحاد الأفريقي)
كنف يلما (جامعة ملبورن)

تفضل كل مما يلي بتقديم المساهمات الأخرى، و/أو مراجعات المسودات التالية:

جاك باص (منتدى التنوير الرقمي)
جمال حسين (مفوضية الاتحاد الأفريقي)
أولاف كولكمان (جمعية الإنترنت)
إيف مالر (Forgerock Inc.)
كريستين رانجر (جمعية الإنترنت)
كولين واليس (مبادرة الكنتارا)
بات والش (Privacy Matters Ltd.)
سالي وينتورث (جمعية الإنترنت)

جمعية الإنترنت، أبريل 2018
مستند مرجعي: AUC-PDPG-Apr2018

السياق الأفريقي

هذه التعليمات تأخذ في الحسبان الخصائص التالية للسياق الإفريقي، كما هو محدد عن طريق مجموعة الخبراء:

- التنوع القانوني والثقافي الهام في جميع أرجاء القارة، مع توقعات الخصوصية المختلفة.
- اختلافات في الوصول إلى التكنولوجيا والخدمات عبر الإنترنت، بين الدول الأعضاء.
- النقاط الحساسة المتعلقة بالإثنية، والتنميط غير المرضي للموطنين، في سياق أي دولة وطنية.
- مستويات مختلفة من الإمكانات في مجالات مثل التكنولوجيا والحوكمة والقانون المرتبط بالتكنولوجيا.
- تنشأ المخاطر من الاعتماد الكبير على موفري الخدمات والمصنّعين غير الأفارقة:
  - القدرة المحدودة للدول الأعضاء في الاتحاد الأفريقي في التأثير على سلوك موفري الخدمات الخارجيين.
  - الخطورة المتزايدة المحتملة لإساءة استخدام البيانات حيث يتم توفير المحتوى والخدمات بشكل فردي عن طريق شركات أجنبية (مثل، خدمات "على القمة" أو OTTs) وتطبيق قوانين حماية البيانات المحلية قد تكون بسبب هذه العوامل أكثر صعوبة.

يمكن أن تزيد هذه العوامل من صعوبة صياغة وتطبيق سياسة متسقة بين – وأحيانًا حتى داخل – الدول الأعضاء.

سياق السياسة

على نحو ما تبيّنه مفوضية الاتحاد الأفريقي حول أمن الفضاء الإلكتروني، وحماية البيانات (2014)، وإعلان أديس أبابا الوزاري (AU/CCICT-2, 2017)، تم تطوير هذه التعليمات في سياق التغيّر السريع في نطاق، ووفرة الخدمات عبر الإنترنت في أفريقيا، وعلى خلفية أهداف السياسة الأفريقية بموجب أجندة 2063.

لقد كرّس الاتحاد الأفريقي تركيز سياسي معقولاً على المواءمة. على سبيل المثال، يُشير القانون التأسيسي للاتحاد الأفريقي[5] (مقالة 3، صفحة 6) بوضوح إلى تنسيق ومواءمة السياسات بين الجماعات الاقتصادية الإقليمية الحالية والمستقبلية، من أجل دعم (من بين أمور أخرى) الأهداف التالية:

- أفريقيا موحدة وقوية
- الإدماج الاجتماعي الاقتصادي، والسياسي المتسارع للقارة
- إيجاد الظروف التي تمكّن أفريقيا من لعب دورها المناسب في الاقتصاد العالمي
- التطور المستدام على المستويات الثقافية، والاجتماعية، والاقتصادية.

تضع أيضًا مفوضية الاتحاد الأفريقي "مبادرة سياسات ولوائح خاصة بأفريقيا الرقمية" (PRIDA)، والتي سيتم خلالها استكشاف أدوات، ومنهجيات لمواءمة، وتنسيق السياسات واللوائح.

كجزء من هدف الإدماج الإقليمي الأكبر، عزم مؤتمر الاتحاد، في جلسته العادي السابعة والعشرين (يوليو 2016، كيغالي، رواندا) على تنفيذ بروتوكول يتعلق بحرية حركة الأشخاص داخل القارة.

5 https://au.int/sites/default/files/pages/32020-file-constitutiveact_en.pdf

- وتترتب على هذا القرار آثار تتعلق بالتبادل القياسي، والآمن، والذي يحترم الخصوصية لبيانات هوية المواطنين، في سياق المعابر الحدودية، والتبادل اللاحق للبيانات الشخصية عبر الحدود، عندما يعمل المواطن أو يقيم صفقات خارج بلده الأصلي. شددت نفس الجلسة على أهمية الحركة الحرة للبضائع والخدمات باعتبارها أحد عناصر الوحدة والتكامل القاري الكبيرة.
- ينعكس أيضًا مبدأ حرية حركة الأشخاص في المادة 43 من المعاهدة التي تؤسس للجماعة الاقتصادية الأفريقية (1991، أبوجا، نيجيريا).

لقد أخذ أيضًا الاتحاد الأفريقي خطوات هامة تجاه تأسيس منطقة تجارة حرة قارية (CFTA) دعمًا لمبادئ حرية حركة الأشخاص، والبضائع، والخدمات، على النحو المنعكس في قرارات، وإعلانات، وقرار جلسته العادية الخامسة والعشرين (يونيو 2015، جوهانسبرغ، جنوب أفريقيا). ولهذه الخطوة آثار على الانتقال المقابل للبيانات الشخصية عبر الحدود، في سياق المعاملات عبر الإنترنت (التجارة)، وعلى الأفراد الذين يعيشون ويعملون في دول أعضاء غير دولهم الأصلية.

وللدول الأعضاء في الاتحاد الأفريقي أيضًا التزامات تتعلق بالحريات الأساسية، وحقوق الإنسان، على نحو المبيّن في إعلانات واتفاقيات الاتحاد الأفريقي والأمم المتحدة. وهذا يشمل الالتزام باحترام، وحماية، وتعزيز الحق في الخصوصية، وحماية البيانات الشخصية. وفي عدد من الحالات، تم بالفعل إقرار الحق بالخصوصية في دساتير الدول الأعضاء (على سبيل المثال تعترف بوتسوانا، جمهورية الكونغو الديمقراطية، ومصر، وغانا، وكينيا، ونيجيريا، وسيراليون، وجنوب أفريقيا، وتنزانيا، وأوغندا، وزامبيا، وزيمبابوي بالحق في خصوصية الأفراد في دساتيرهم الوطنية كحق إنساني أصيل).

لكل هذه السياسات والالتزامات آثار تتعلق بالتبادل الآمن، والشفاف، والقوي والذي يحترم الخصوصية للبيانات الشخصية عبر الحدود، وبين الولايات القضائية. وهذا بدوره، يضع عبئًا على الدول الأعضاء في الاتحاد الأفريقي لضمان عدم إعاقة إحراز تقدم تجاه الإدماج الإقليمي، والتجارة الحرة، والتطور أو إحاطته بالمخاطر عن طريق عدم القدرة على تبادل البيانات الشخصية بطريقة آمنة، وموثوقة، ومع الاحترام اللائق لحقوق الأفراد.

وبالتوازي، يُعتبر الاستخدام الآمن، والقوي، والذي يحترم الخصوصية للبيانات الشخصية عامل تكوين أساسي لقدرة الدول الأعضاء في الاتحاد الأفريقي على القيام بما يلي:

- الحفاظ على تقرير مصيرهم في المجتمع المعلوماتي، والاستمرار في مواكبة التغير السريع
- الاستفادة من الابتكار التكنولوجي
- خلق ثقة في الاقتصاد القائم على البيانات، والحفاظ عليها

للحفاظ على الثقة في الاقتصاد المستند إلى البيانات، ينبغي على أعضاء الاتحاد الأفريقي الاعتراف بالدور الذي تلعبه البيانات الشخصية، والقوى الاقتصادية التي تشكلها. عند نجاحه، يمكن للاقتصاد المستند إلى البيانات خلق نمو اقتصادي، وتقديم خدمات جذابة، وابتكارية، وتحسين جودة الحياة.

ومع ذلك، يمكن أيضًا أن يكون للاقتصاد المستند على البيانات جانب مظلم، حيث تتم معاجلة البيانات الشخصية بطرق استغلالية أو تعسفية، وحيث يتم تدمير اهتمامات الشخص موضوع البيانات. لا تصبح أحيانًا التكلفة، والخطورة المتأصلة في هذه الحالات واضحة إلا عندما تسوء الأمور – عندما يكون هناك خرق للبيانات أو يتم التعرض لحالة من الاحتيال. وقد يكون لذلك أثر عميق على الثقة والاطمئنان في الخدمات عبر الإنترنت، والتأثير المقابل على الاقتصاد المستند إلى البيانات. توصي هذه التعليمات بخطوات للحد من هذه النتائج المذكورة غير المرغوب بها.

اعتبرت مجموعة الخبراء أنه، بالنسبة إلى بعض الدول الأعضاء في الاتحاد الأفريقي، وصنّاع القرار، قد تكون حماية البيانات الشخصية نطاق غير مألوف نسبيًا، والذي يمكن أن يكون حاجزًا أمام وضع سياسة فعّالة. تهدف التعليمات إلى المساعدة على تمكين الدول الأعضاء من تطوير سياسة وقوانين خاصة بحماية البيانات الشخصية. لذا، فإن التوصيات تكون مقترنة بعدد من تدابير التمكين والاستدامة ، مثل البرامج التي تركّز على زيادة الوعي والتعليم، لصانعي السياسات والأفراد.

وفي نهاية المطاف، هناك خطورة حدوث تأثير كبير (على مواطنيهم واقتصادياتهم) إذا لم تقم الدول الأعضاء في الاتحاد الأفريقي بفعل شيء. وبناءً على ذلك، تقترح التعليمات إجراءات تهدف إلى تخفيف هذه الخطورة.

نحو توافق مع مبادئ الخصوصية المطبّقة في المناطق الأخرى

المبادئ المحددة في اتفاق مالابو

تحدد المادة 13 من الميثاق المبادئ الستة التالية المتعلقة بحماية البيانات:

- الموافقة، والمشروعية
- المعالجة المشروعة، والنزيهة
- الغرض، والصلة، والاحتفاظ بالبيانات
- دقة البيانات على مدار فترة من الزمن
- شفافية المعالجة
- سرية وأمان البيانات الشخصية

مجموعات مشابهة من المبادئ من مصادر أخرى

لقد تم تقارب عدد من أُطر عمل الخصوصية الوطنية، والدولية إلى حد كبير لتكوين مجموعة من مبادئ حماية البيانات الأساسية والجوهرية. وتم تطبيقها في أُطر عمل الخصوصية الوطنية في أكثر من 100 دولة. ربما الثلاثة الأكثر أهمية هي تعليمات خصوصية منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) (غير ملزمة، وجرى آخر تعديل في عام 2013)، واتفاقية المجلس الأوروبي 108، والتي هي ملزمة للأطراف الموقعة عليها البالغ عددها 51 توقيعًا[6]، وإطار عمل خصوصية التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) وجرى آخر تعديل في 2015. تعبّر هذه المستندات على مبادئ الخصوصية المشابهة، ويعترف بها على نطاق واسع في توفير أساس قوي للممارسات، وسياسات الخصوصية عبر الإنترنت. ومع تغييرات طفيفة، يمكنها أن تشكّل أساسًا للتعليمات التي تطبقها الجمعية العامة للأمم المتحدة، ودول الكومنولث، وتتم مواءمتها بشكل كبير مع لوائح حماية البيانات العامة التابعة للاتحاد الأوروبي 2016.

هذه هي المناطق التي تركّز عليها مبادئ الخصوصية هذه:

- **قيود الجمع.** ينبغي الحصول على البيانات الشخصية ومعالجتها بطريقة مشروعة، ونزيهة، وشفافة إلى أقصى قدر ممكن.
- **جودة البيانات.** ينبغي أن تكون البيانات الشخصية دقيقة عند جمعها، وينبغي اتخاذ خطوات معقولة للتأكد من الحفاظ على دقتها على مدار فترة الاحتفاظ.
- **مواصفات الغرض.** ينبغي جمع البيانات لأغراض محددة، وصريحة، ومشروعة فقط. لا ينبغي استخدام البيانات الشخصية لأغراض أخرى إلا أن تكون متوافقة مع القوانين المعمول بها، مثل أرشفة البيانات والتي تنصب في صالح المصلحة العامة أو لأغراض البحث العلمي.
- **قيود الاستخدام.** لا ينبغي الكشف عن البيانات الشخصية، أو إتاحتها أو استخدامها لأغراض أخرى بدون موافقة الشخص أو حيثما يخوّل القانون ذلك.
- **الضمانات الأمنية.** ينبغي حماية البيانات الشخصية بضمانات أمنية معقولة للحفاظ على سلامتها وسريتها.
- **الانفتاح.** ينبغي أن تكون هناك سياسة انفتاح عامة على عمليات التطوير، والممارسات، والسياسات فيما يتعلق بالبيانات الشخصية.

6 بداية من تاريخ نشر هذه التعليمات.

- **مشاركة الشخص.** ينبغي أن لدى الأشخاص الحق في الحصول على معلومات عن معلوماتهم الشخصية التي يحتفظ بها الآخرون. وينبغي تقديم هذه البيانات في غضون فترة معقولة من الوقت، في صيغة قابلة للفهم بسهولة، وبتكلفة غير مبالغ فيها. للأشخاص موضوع البيانات الحق في تغيير بياناتهم وتعديلها إذا كانت غير دقيقة أو محوها إذا كانت غير لائقة.
- **المحاسبة.** ينبغي على من يقوم بجمع، ومعالجة البيانات الشخصية أن يكون قادرًا على إثبات امتثاله لهذه المبادئ.

الاتساق مع المبادئ الستة المعيّنة في المادة 13 من الاتفاق ليس مؤكدًا، ومع ذلك هناك الكثير من الجوانب المشتركة. تظهر منطقتان من مناطق الاختلاف، على النحو التالي:

- تُدرج المادة 13 من اتفاق مالابو "الموافقة" كمبدأ منفصل، بينما في أُطر عمل منظمة التعاون والتنمية في الميدان الاقتصادي (OECD)، والمجلس الأوروبي، يتم تضمين الموافقة كمعيار للمعالجة المشروعة.
- تعبّر المواد 7 و10 من اتفاق المجلس الأوروبي 108، والمبدأ 14 من تعليمات خصوصية منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) والفقرة 32 من إطار عمل خصوصية آبيك عن المتطلبات المرتبطة بمساءلة مراقب البيانات. المساءلة غير صريحة في مبادئ اتفاق مالابو (المادة 13) أو التزامات مراقب البيانات الشخصية (المواد 20 – 23) ومع ذلك، فإن المواد 19-16 تُشير إلى المساءلة في جزء مراقب البيانات، من خلال التعبير عن حقوق معيّنة في الجزء المتعلق بالشخص موضوع البيانات (دقة البيانات، والتصحيح، والحذف وما إلى ذلك).

هذه التغييرات طفيفة نسبيًا، ولا ينبغي أن تخفي حقيقة أن هناك الكثير من أوجه التوافق، والاتساق أكبر من الاختلاف. ومع ذلك، نوصي أن تولي الدول الأعضاء في الاتحاد الأفريقي أهمية خاصة لآليات المساءلة الخاصة بمراقبي البيانات في أُطر عمل حماية البيانات ذات الصلة الخاصة بها حتى لا يتم التغافل عن معالجة موضوع بهذه الأهمية.

أُطر العمل الإقليمية والوطنية الحالية في أفريقيا

لقد حدد البحث الذي أجرته منظمة التعاون لسياسات تكنولوجيا الاتصالات والمعلومات في شرق وجنوب أفريقيا (CIPESA) أُطر العمل الأفريقية التالية التي تعكس مبادئ حماية البيانات والخصوصية المشابهة لما ذكر أعلاه:

- قانون نموذج SADC المعني بحماية البيانات (2010)
- القانون المكمل ECOWAS رقم A/SA.1/01/10 المعني بحماية البيانات الشخصية (2010)
- إطار عمل EAC المتعلق بقوانين الفضاء الإلكتروني (2008)

بحسب نفس البحث، فإن الدول التالية لديها تشريعات مقترحة أو حالية (في وقت كتابة هذه التعليمات) تتضمن مبادئ مشابهة تتعلق بحقوق الأشخاص موضوع البيانات وتُعنى بتأسيس سلطات لحماية البيانات: أنجولا (2016)، وغينيا الاستوائية (2016)، وموريتانيا (2017)، وجنوب أفريقيا (2013)، وبوركينا فاسو (2004)، ومالي (2013)، والجابون (2011)، وبينين (2009)، وغانا (2012)، وساحل العاج (2013)، وليسوتو (2012)، ومدغشقر (2014)، والمغرب (2009)، والسينغال (2008)، وتونس (2004)، وزيمبابوي (2003). مشاريع قوانين لحماية وخصوصية البيانات في كينيا، والنيجير، ونيجيريا، وتنزانيا، وأوغندا تتضمن أيضًا شروط مشابهة.

مواضيع يثيرها مجموعة أصحاب المصالح

يعكس هذا الجزء من التعليمات المواضيع والمساءل التي أثيرت أثناء عملية التشاور وورشة عمل الخبراء.

يتم تجميعها حسب نوع صاحب المصلحة، وفي كل جزء خاص بصاحب المصلحة، ويتم ترتيب المواضيع حسب بنود الاتفاق المقابلة.
يهدف هذا الجزء إلى توفير سياق ومعلومات أساسية للتوصيات المتوفرة في الجزء اللاحق.

الحكومات وصنّاع القرار

الموضوع	الملاحظات
أُطر عمل وتدفقات البيانات عبر الحدود	اللائحة التي تتماشى مع ما هو مضمّن في الاختصاصات القضائية الأخرى تساهم في تعزيز الثقة المتبادلة، وتضع أساسًا للتبادل الموثوق به للبيانات بما في ذلك على سبيل المثال لا الحصر البيانات الشخصية. ولهذا فإن حماية البيانات الشخصية تعتبر أحد عوامل تمكين الثقة المحسنة في حركة الأشخاص، والبضائع، والخدمات عبر الحدود.
المواءمة (اتفاق مالابو، ديباجة، فقرة 20)	تُشير ديباجة الاتفاق إلى استحسان تشريعات الفضاء الإلكتروني المتوائمة. في نفس المبدأ، ستساعد خطوات لزيادة الاتساق في تشريعات حماية البيانات بين الدول الأعضاء في الاتحاد الأفريقي في تقليل أو تخفيف الاختلاف في حماية الخصوصية. ينبغي أن تسعى استراتيجيات حماية البيانات الشخصية، والسياسات، والقوانين إلى استيعاب المناطق التالية: • زيادة الوعي بحقوق والتزامات حماية البيانات الشخصية • أُطر عمل وأهداف السياسة • القوانين، وسلطات حماية البيانات؛ إنفاذ وعقوبات سيتعين على الدول الأعضاء في الاتحاد الأفريقي التعاون لتحقيق مثل هذا النوع من الاتساق. يتوقع أن تكون مبادرة سياسات ولوائح خاصة بأفريقيا الرقمية (PRIDA) الخاصة بمفوضية الاتحاد الأفريقي عامل تمكين هام لمثل هذه الجهود.
حقوق المواطنين، وامتيازات الدولة (اتفاق مالابو، الديباجة والمادة 8)	يؤكد الاتفاق مجددًا على التزام الدول الأعضاء في الاتحاد الأفريقي باحترام الحريات الأساسية وحقوق الإنسان، والتزامها بالميثاق الأفريقي المعني بحقوق الإنسان والشعوب. ومن المبادئ الهامة التأكد من أن الأشخاص يتمتعون بحقوق متساوية على الإنترنت وخارجه. ومع ذلك، يُشير الاتفاق أيضًا إلى امتيازات الدولة، والذي يُفهم منها أن الحق في الخصوصية هو حق مشروط، ويُتغاض عنه بصورة مشروعة، في بعض الحالات، لمصلحة الأمن الوطني، في مجال إنفاذ القانون والسلامة العامة. وهذا يُشكّل تحدي حوكمة فيما يتعلق بالآتي: • وضع شروط متسقة، وقابلة للحل يسمح بموجبها بمثل هذه الاستثناءات من قانون حماية البيانات؛ • بناء نظام مراقبة قوي وموثوق به لمراقبة استخدام مثل هذه الاستثناءات، وخاصة في سياقات الأمن الوطني، حيث يتم تقييد الوصول إلى معلومات الحوكمة ذات الصلة (لأسباب يمكن فهمها).

عدم الاتساق والتبادلية بين مستويات الحماية التي توفرها الدول الأعضاء في الاتحاد الأفريقي، وبين أعضاء الاتحاد الأفريقي والكيانات الأخرى (اتفاق مالابو، مادة 10.6.k)	ومن المحتمل أنه ستكون هناك أوجه من عدم التماثل في مستوي حماية البيانات الذي يوفره أعضاء الاتحاد الأفريقي، ومع ذلك يمكن التخفيف من تأثيراتها و/ أو الحد منها، من خلال إعطاء الحوكمة عناية مناسبة، ومن خلال التدابير التنظيمية والتنفيذية، والعوامل الاقتصادية. تُشير المادة 10.6.k من الاتفاق إلى ترتيب التبادلية المتعلقة بعمليات نقل البيانات خارج الاتحاد الأفريقي. التبادلية هي العنصر الأساسي في الحد من عدم التماثل في حماية البيانات الشخصية. تعتبر معايير الكفاية المتسقة (بين الدول الأعضاء) المتعلقة بمعالجة البيانات الشخصية آلية مهمة للتأكيد على التبادلية العملية في تدابير القانونية والإنفاذية. (ومع ذلك، هذا ليس نهجًا واحدًا. في منطقة آسيا والمحيط الهادئ، على سبيل المثال، بدلاً من اتّباع قرارات الكفاية كأساس لعمليات الانتقال عبر الحدود، طوّرت رابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (أبيك) آلية تطوعية تعتمد على المساءلة، تعرف باسم نظام "قواعد الخصوصية عبر الحدود" من ابيك (نظام CBPR)، وإقرار الخصوصية للمعالجين من ابيك (نظام PRP).

مراقبو البيانات

الموضوع	الملاحظات
الأدوار والالتزامات	يُدفع سلوك مراقبي البيانات بعوامل مختلفة (الربحية أو الكفاءة أو الفوائد الاجتماعية أو المجتمعية) ويعتمد في الغالب بصورة أساسية على ما إذا كان مراقب البيانات يعمل على سبيل المثال في القطاع التجاري أو العام أو غير الربحي أم لا. سيتم تقييد سلوكهم، من ناحية المبدأ، بموجب القانون المطبّق – ولكن بشرط أن يتم تنفيذ ذلك القانون على نحو فعّال. في هذا السياق، لا يحدد القانون في لإعادة إلا الحد الأدنى للسلوك المقبول لمراقب البيانات. و يحتمل أن تتطلب الحماية الفعّالة بشدة للخصوصية أن يقوم مراقبو البيانات بمدّ الحد القانوني البحت وأن يتبنوا أفضل الممارسات لمعالجة البيانات، مثل المشاركة في مخطط مصادقة لحماية البيانات الشخصية. وقد يُنظر إلى هذا الإجراء، بموجب الاتفاق، على أنه حماية بيانات مماثلة للطلب (الوارد في المادة 32) لتطوير قواعد سلوك متوائمة لنطاق أمن الفضاء الإلكتروني.
علاقة مراقبي البيانات ومعالجي البيانات	فيما يتعلق بالبيانات الشخصية: • مراقب البيانات شخص يقرر الأغراض التي من أجلها، والطريقة التي بها تُعالج أو ينبغي أن تعالج أي بيانات شخصية. • معالج البيانات يعني أي شخص (بخلاف الموظف القائم بدور مراقب البيانات) يُعالج البيانات نيابة عن مراقب البيانات. كمبدأ عام، لا يفقد مراقب البيانات أي التزامات عندما يقوم بتمرير البيانات الشخصية إلى معالج البيانات للمعالجة بدلاً منه. "يرث" معالج البيانات مسؤوليات مراقب البيانات فيما يتعلق بحماية البيانات التي مررت إليه، وخصوصية الشخص موضوع البيانات. ومع ذلك، على سبيل المثال، لن يكون معالج البيانات مسؤولاً عن الاستجابة لطلبات وصول الشخص موضوع البيانات (SAR) فيما يتعلق بالبيانات الشخصية التي مررت إليه: يمكن لمعالج البيانات أن يحيل بطريقة مشروعة أي طلب كهذا إلى مراقب البيانات. سيتم الإتيان على نقطة (SARs) طلب وصول الشخص موضوع البيانات بتفصيل أكبر أدناه، من وجهات نظر مراقب البيانات، وسلطة حماية البيانات).

الموافقة (المادة 13، المبدأ 1)	يطرح الحصول على موافقة لمعالجة البيانات الشخصية تحديات أخلاقية، وقانونية، وعملية. يمكن أن تعطي التشريعات حسنة النيّة لمراقبي البيانات حافزًا سلبيًا لحلول من شأنها أن تقوّض الثقة بدلاً من تعزيزها. على سبيل المثال، قدّم الاتحاد الأوروبي "قانون ملفات تعريف الارتباط" الذي كان يهدف إلى منع مواقع الويب من تعقب المستخدمين بدون معرفتهم أو موافقتهم، باستخدام أجزاء صغيرة من البيانات المحددة للهوية (ملفات تعريف الارتباط) المخزّنة في متصفح المستخدم. استجابت بعض مواقع الويب عن طريق إعادة عرض خيار الموافقة "اوافق أو ارفض" والذي يُعطي المستخدمين اختيارًا ذا مغزى. وقد يكون ذلك تطبيقًا لنص القانون ولكنه يبعد عن تنفيذ روحه. وبوجه عام، لم يحصل المستخدمون نتيجة لذلك على نتائج خصوصية أفضل. يحتمل أن يتطلب حلّ مشكلة الموافقة الصعبة مزيجًا من التدابير القوانين القانونية والفنية وفي بعض الحالات، قد يضطر عدد من موفري خدمات الحوافز الاقتصادية القوية إلى "الالتفاف" على القانون. ينبغي تطوير قوانين حماية البيانات الشخصية من خلال عملية تحقق الموازنة بين ما هو مطلوب من الناحية القانونية، وما هو ممكن من الناحية الفنية، وما يُمثل على نحو أفضل مصالح الشخص الذي يُطلب منه إبداء الموافقة. في بعض لوائح حماية البيانات، مثل اتفاق المجلس الأوروبي 108، يتم إضافة إلى ذلك تقييد المتطلب الخاص بالموافقة (على سبيل المثال، ويشترط أن تكون الموافقة مستنيرة، ومحددة، وقابلة للإبطال، وما إلى ذلك)، وسيكون لكل شرط من هذه الشروط آثار تتطلب تدابير قانونية، وفنية، وإجرائية يتم تنفيذها من قِبل مراقب البيانات. لا تزال تفتقد هذه المشكلة بشكل كبير إلى حلول قاطعة، وتُشجّع الدول الأعضاء على تحفيز التحقيق متعدد التخصصات لمعالجتها بطرق أفضل.
تتدفق البيانات الشخصية بين السياقات، وتأثيرها على الخصوصية (المادة 13، المبدأ 2 - نزاهة المعالجة)	السلامة السياقية مهمة.[7] تنتهك البيانات الشخصية، التي يتم جمعها في سياق واحد محدد، واستخدامها لاحقًا في سياق آخر بدون وعي أو موافقة الشخص، خصوصية المستخدم (على سبيل المثال، البيانات الشخصية التي تتم مشاركتها من قِبل مستخدم لاستكمال معاملة بيع بالتجزئة عبر الإنترنت، ولكن يتم بيعها إلى جهة إعلانية بدون معرفة الشخص). تنطوي فكرة السلامة السياقية على أن يكون مراقب البيانات على دراية بالسياق الذي جمعت فيه البيانات، وأن يحترم سلامة ذلك السياق. وهذا يرتبط بمبدأ خصوصية "الغرض من الجمع". ونظرًا لأن هناك في الغالب حوافز قوية تدفع مراقبي البيانات إلى نقل البيانات من سياق إلى آخر (على سبيل المثال، أخذ بيانات معاملات العملاء وبيعها ومن ثمّ، استخدامها في إعلانات مستهدفة)، ينبغي على سياسات حماية البيانات التأكيد على أن هذا الإجراء لن يضر بأي حال الشخص موضوع البيانات أو التأكيد على أن الشخص موضوع البيانات لديه فرصة الإعراب عن والإنفاذ لتفضيلاته حول ما إذا أو متى أو كيف يجب أن يحدث ذلك. يعد نقل البيانات بين السياقات المختلفة مشكلة على وجه الخصوص عندما لا يكون المستخدمون على دراية بما يحدث. على سبيل المثال، قد لا يعي الطفل الذي يُعطى دمية "متصلة" أن هذه الدمية تربط سياق "المنزل" الخاص بسياق تجاري لجهة خارجية. وقد لا يبدو أن مستخدمي متتبع اللياقة Strava أدركوا أن الجهاز يتيح نقل بيانات الموقع من سياق (مثلا قاعدة عسكرية) ويجعلها عامة في (خرائط عبر الإنترنت يمكن البحث فيها) كسياق آخر. ونظرًا لأن المستخدمين يتحكمون بمقدار بسيط في الاستخدام اللاحق للبيانات التي يكشفون عنها، فإن جزء كبير من مسؤولية الاستخدام المناسب للبيانات ينبغي أن يقع على مراقب البيانات. ينبغي على الحكومات أن تشجّع على ثقافة التصميم الأخلاقي والمستند إلى قيم[8]، حتى تضمن أن موفري الخدمات على دراية باختيارات التصميمات التي تشدد على تحقيق الخصوصية والمبادئ الأخلاقية الأخرى في المنتجات والخدمات التي تعالج بيانات شخصية.
طلبات وصول الشخص موضوع البيانات (اتفاق مالابو، المواد 19-16)، وعلاقتها بالمساءلة والشفافية	تتضمن معظم قوانين حماية البيانات الحالية مبدأ المساءلة، كما هو محدد، على سبيل المثال، في تعليمات خصوصية منظمة التعاون والتنمية في الميدان الاقتصادي (OECD). تُشير تعليمات منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) إلى الشفافية كعنصر أساسي في المساءلة. بالنسبة إلى مراقبي البيانات، يتضمن ذلك (من بين جملة أمور أخرى) الالتزام بالرد على طلبات الشخص موضوع البيانات حول ما هي طبيعة البيانات المحتجزة عنه. وهذا بدوره، يتضمن رفع مطلب إلى واضعي السياسات للتأكيد على معالجة طلبات وصول الشخص موضوع البيانات في إطار قانوني يضمن النظر في تلك الطلبات بطريقة تخدم المصالح المشروعة للشخص موضوع البيانات، ولا تضع عراقيل أمامه أو تحمل مراقب البيانات أعباء غير مبررة.

7 "الخصوصية باعتبارها من عناصر السلامة السياقية" (هيلين نيسينباوم، مراجعة قانون واشنطن، 2004)
8 راجع، على سبيل المثال، "الابتكار الأخلاقي في مجال تكنولوجيا المعلومات" (سارة سبايكمان، 2016)

سرية معالجة البيانات، والتدابير المناسبة لتأمين البيانات (المواد 21-20، و المادة 15 المتعلقة بقابلية الربط)	يلزم هذا الاتفاق أن يتخذ مراقبو البيانات التدابير المناسبة لتأمين البيانات الشخصية، والتأكيد على سريتها وسلامتها. ستشمل "التدابير اللازمة" مجموعة من الخيارات الفنية، والإجرائية، والمادية. على سبيل المثال، حماية السجلات الورقية المؤمنة في خزانة ملفات بشكل واحد من أشكال التحكم في الوصول؛ للسجلات الرقمية بخلاف تدابير المصادقة والتصريح[9] القوية شكلاً آخر من أشكال الحماية؛ تتم تشفير الملفات بطريقة ما، وهكذا. ينبغي تشجيع مراقبي البيانات على تطبيق معايير الممارسات الأفضل المقبولة في المجال على أمن البيانات. في هذا الصدد، لقد تبنت الكثير من الدول نهجًا يستند على المخاطرة، حيث يجري تقييم التدابير التي تعتبر مناسبة من ناحية الخطورة، والسجلات، والتأثير المحتمل لأي فشل لحماية البيانات الشخصية المعنية. عوامل الأمن الثلاثة "الكلاسيكية" كلها وثيقة الصلة في هذا السياق: السرية، والسلامة، والتوفّر. ينبغي حماية البيانات من الكشف غير المرغوب فيه، والتعديل غير المطلوب، والتدمير/عدم إمكانية الوصول غير المرغوب فيه. ينبغي على الدول الأعضاء الرجوع إلى توجيهات أمن الفضاء الإلكتروني ذات الصلة المتعلقة بهذا المواضيع. أيضًا تحت بند أمن الفضاء الإلكتروني، ينبغي على مراقبي البيانات، وعند الضرورة، سلطات حماية البيانات التماس توجيهات تتعلق بآليات الأمن الموثوقة (الخوارزميات، والأطوال الأساسية، وأنظمة الإدارة الرئيسية)، على المستوى الوطني والدولي. من أمثلة مصادر مثل هذه التوجيهات، في مناطق أخرى، ما يلي: • ENISA (وكالة الاتحاد الأوروبي المعنية بأمن الشبكات والمعلومات) • NIST (الولايات المتحدة، ولكن يُشار إليها على نطاق واسع من قبل البلدان الأخرى) • CESG (التوجيهات الخاصة بالمملكة المتحدة، على سبيل المثال، تلك المتعلقة بصناعة المملكة المتحدة) ستساعد مثل هذه التوجيهات السلطات الوطنية على قياس، على سبيل المثال، الفترة التي ينبغي أن يعتبر فيها شكل معين من أشكال التشفير آلية حماية موثوقة لأغراض المواد 21-20. وبالمثل، عند استخدام أساليب الاستعارة و/أو حجب الهوية كوسائل لحماية البيانات الشخصية من الاستخدام أو الكشف غير المرغوب فيه، فينبغي مراقبة فاعليتها في ضوء التطورات في الأساليب الخاصة "بإعادة تحديد هوية" البيانات التي يفترض أنها مستعارة أو محجوبة الهوية. وإضافة إلى إعادة تحديد الهوية، ينبغي مراعاة اثنين من التهديدات الأخرى للخصوصية في هذا السياق: الاستدلالية، وقابلية الربط. • تشير الاستدلالية إلى إمكانية أخذ البيانات غير الشخصية أو استخدامها لاستخلاص الافتراضات أو التوقعات الشخصية أو أخذ البيانات الشخصية واستخدامها لاستخلاص البيانات الشخصية الحساسة حول شخص ما. • بمعنى آخر، البيانات التي قد لا تبدو شخصية قد تكون في الحقيقة شخصية أو ربما استنباط البيانات الشخصية. وبالمثل، قد تكون البيانات الشخصية "العادية" نقطة البداية لاستخلاص البيانات الشخصية الحساسة. ينبغي على الدول الأعضاء مراجعة تشريعات حماية البيانات للتحقق من حماية الأفراد أو المجموعات من الإقصاء أو التمييز، من خلال استخدام مثل هذه البيانات المستخلصة أو المستنتجة. • تُشير قابلية الربط إلى قدرة مراقبي البيانات أو الأطراف الخارجية لإثبات أن البيانات الشخصية المستخلصة من مصادر مختلفة ترتبط بنفس الشخص. على سبيل المثال، تكون سجلات المكالمات لرقم الهاتف هذا مرتبطة بنفس الشخص كما هو الحال بالنسبة إلى المنشورات الموجودة على موقع الوسائط الاجتماعية. يمكن أن يقوّض ربط بيانات من هذا النوع خصوصية واستقلالية الفرد بشكل خطير، عن طريق منعه من الاحتفاظ بسياقات منفصلة في حياته عبر الإنترنت. هذه مناطق صعبة ينبغي سنّ تشريعات بخصوصها بنجاح، خاصة عندما تتطور التكنولوجيا المرتبطة بالاستدلالية (الذكاء الاصطناعي، واتخاذ القرار القائم على الخوارزميات، والتعلم الآلي) بشكل سريع، وعندما يكون من السهل تعدين البيانات لأنواع الربط الموضحة أعلاه. وبحسب ذلك، نوصي بتبني نهج متعدد الأطراف عند التعامل مع المشكلة، والبحث عن حلول تستند إلى القدرة على دمج التدابير التنظيمية، والإجرائية، والفنية، والتعليمية على النحو المطلوب. يحتمل أن يقدم النهج القائم على المخاطر أفضل النتائج.

9 المصادقة هي عملية التحقق من صحة هوية الشخص، في اللحظة التي يحاول فيها الوصول إلى خدمة أو مورد. المصادقة هي عملية تنص على أن أي شخص مخوّل له الحق في الوصول إلى الخدمة أو المورد المعني. التحكم في الوصول هي عملية إنفاذ الحق.

فترات الاحتفاظ (اتفاق مالابو، المادة 22)	تتضمن معظم قوانين حماية البيانات الحالية مبدأ وضع قيود على الاحتفاظ بالبيانات. ومع ذلك، يُطبق عدد قليل من مراقبي البيانات هذا المبدأ، ومن ثمّ يتم الاحتفاظ بالكثير من البيانات لفترة أطول من المطلوب أحيانًا إلى أجل غير مسمى، مما يضع مراقبي البيانات في خطر متزايد من حدوث خرق للبيانات الشخصية، وعليه يتعرض الأشخاص موضوعي البيانات لمخاطر انتهاك الخصوصية. ينبغي ألا يستند النظام التنظيمي والرقابي على افتراض أن البيانات سيتم حذفها بشكل افتراضي ومن ثمّ، ينبغي أن تتضمن تدابير للتشجيع على تقليل البيانات إلى الحد الأدنى وحذفها، والتأكد من صلتها بذلك المبدأ.
استدامة الوصول إلى البيانات (اتفاق مالابو، المادة 23)	يلزم مراقب البيانات، بموجب الاتفاق، بالتأكيد على بقاء إمكانية الوصول إلى البيانات الشخصية من الناحية الفنية. من ناحية الخصوصية، سيكون لهذا الإجراء تأثير على قدرة مراقب البيانات على الامتثال لمختلف متطلبات المواد 19-16 من الاتفاق (الحقوق في الإعلام، والوصول، والتصحيح، والمحو، إلخ). قد يكون أيضًا عاملاً في الامتثال لطلبات وصول الشخص موضوع البيانات (المادة 17): ستفشل المادة 17 في خدمة الشخص موضوع البيانات إذا تمكن مراقبو البيانات من الاستجابة لطلبات وصول الشخص موضوع البيانات بطريقة أو تنسيق لا يمكن للشخص موضوع البيانات استخدمه.

سلطات حماية البيانات

الموضوع	الملاحظات
عناصر نظام الحوكمة (المواد 12-10)	بينما يضطلع أصحاب المصالح بأدوار قانونية بموجب قوانين الخصوصية وحماية البيانات الشخصية، فإن الامتثال للمتطلبات القانونية ينبغي أن يكون خاضعًا للرقابة، والإنفاذ؛ وهذا يرتبط ارتباطًا مباشرًا بمبدأ حماية البيانات "المساءلة". بينما يكون لدى أصحاب المصالح التزامات تعاقدية أو قائمة على المعايير، ينبغي أن تكون هناك إمكانية لمراجعة امتثالهم، وهو ما يتطلب وجود مقيمين ومراجعين قادرين ومؤهلين. ولهذا ينبغي إضافة هذه الكيانات إلى قائمة أصحاب المصالح، كما يلي: • الأشخاص موضوعي البيانات، • مراقبو البيانات لمختلف الأنواع (موفر الهوية، وموفر السمة، وموفر الخدمة)، • سلطات حماية البيانات، • مقيمو الحوكمة، • مراجعو الامتثال، و • هيئات الاعتماد للمقيمين، والمراجعين. وهذا يتضمن أيضًا أن يكون لدى سلطات حماية البيانات السلطة للتحقيق في الإجراءات الخاصة بالاعتماد، والتقييم، والمراجعة، وفرض عقوبة على حالات الفشل. يمكن لنظام كهذا أن يُشكل أساسًا لنظام الاعتماد، لتوحيد وتنفيذ مبادئ حماية البيانات. يمكن لنظام الاعتماد أيضًا تغطية المهام ذات الصلة، مثل مبادئ أمن المعلومات، والتي تعتبر ضرورية لتحديد ما يُشكل "التدابير المناسبة" تحت البنود 21-20 (والمرتبطة بالبنود 15 و23). في سياق كل دولة عضو، سيتيح كل نظام اعتماد معني بهذه المبادئ وضع لوائح وتوجيهات لما يلي: • خدمات السرية، والسلامة، والتوفر المتعلقة بمعالجة البيانات. • تقييم وتحديد التشفيرات الخوارزمية، والأطوال الأساسية، وإجراءات الإدارة الرئيسية. • قياس نقاط القوى ذات الصلة لآليات التصديق المختلفة. • حماية البيانات الشخصية من خلال حجب الهوية، والتزييف. • معايير تقييم المخاطرة لإعادة تحديد هوية البيانات التي تم حجب هويتها/تزييفها. • معايير تقييم المخاطرة المرتبطة بالبيانات الاستدلالية وقابلية الربط. بعد ذلك يمكن أن يشكل الاعتماد الأساس لمنح علامة ثقة لأصحاب المصالح الذين يلبون المعايير المحددة، والذي يساعد بدوره على تنوير وتوجيه الأفراد بشأن القرارات الموثوق بها التي يتخذونها عبر الإنترنت.

دور واستقلالية سلطات حماية البيانات (DPA) (المادة 11)	قد تخفق سلطة حماية البيانات (DPA) في تلبية غرضها المقصود إذا خاضعة لضغط سياسي أو إداري أو تجاري غير مبرر. على سبيل المثال، إذا كان موظفيهم خاضعين لتعيين اعتباطي/فصل تعسفي، إذا كانوا مفتقرين إلى سلطات الإنفاذ المناسبة أو الموارد أو إذا كانوا خاضعين لحشد تأييدي (لوبي) تجاري أو تشريعات كيدية.
قرارات الكفاية (المادة 12.2.k)	تعتبر سلطات حماية البيانات (DPA) الفعّالة عنصرًا أساسيًا للتأكيد على حدوث عمليات نقل البيانات عبر الحدود في إطار من الثقة المتبادلة والمعايير المتسقة (راجع أيضًا "الملاحظات" المذكورة أعلاه، تحت "الحكومات وواضعي السياسات" فيما يتعلق بالتبادلية).
حقوق الأشخاص موضوعي البيانات (المواد 13، 16-19)	سيضطلع سلطات حماية البيانات (DPA) بدور أساسي يلعبونه في توضيح، وتوصيل، ومراقبة، وتعزيز حقوق الأشخاص موضوعي البيانات، كما هو محدد في العديد من مواد/شروط الاتفاق. المادة 18: الحق في الاعتراض على المعالجة. ستتحمل سلطات حماية البيانات (DPA) قدرًا من المسؤولية عن الاتفاق حول الأسس المشروعة لمثل هذه الاعتراضات، وأيضًا تتحمل مسؤولية كبيرة عن تقرير متى يكون من العملي أو المعقول ممارسة حق كهذا (على سبيل المثال، في أي مرحلة يمكن افتراض أن الشخص موضوع البيانات قد وافق صراحة على المعالجة، وتحت أي ظروف ينبغي التماس طلب صريح للموافقة؟). المادة 19: الحق في التنقيح/المحو. قد تطالب سلطات حماية البيانات (DPA) بتقديم توجيهات، على سبيل المثال، حول الظروف التي يمكن/يجوز/ينبغي فيها حذف البيانات الشخصية تبعًا لطلب الشخص موضوع البيانات، حتى إذا كانت البيانات المقصودة صحيحة ودقيقة. على سبيل المثال، في أي مرحلة يمكن للشخص موضوع البيانات طلب حذف البيانات الشخصية على أساس أن مراقب البيانات لم يعد بحاجة إليها – وإذا لم يتفق الشخص موضوع البيانات، ومراقب البيانات على هذه النقطة، فم يحل الخلاف؟ ينبغي تمييز الحق في المحو من الحق في إلغاء الفهرسة (يُشار إليه أحيانًا بصورة مضللة باسم "الحق في النسيان"[10]). إلغاء فهرسة محتوى الويب، في سياق الخصوصية، هي طريقة لجعل إمكانية الوصول إلى بيانات محددة عبر الإنترنت أقل سهولة. بموجب قانون الاتحاد الأوروبي[11]، تم استخدام هذه الخاصية لإلزام محركات البحث بطمس نتائج عمليات بحث محددة مفهرسة باسم موضوع بحث البيانات. ولا يمنع هذا الإجراء نشر المعلومات على الويب، ولا يضمن عدم العثور على تلك المعلومات. ومن جملة القوانين الأخرى، يحتوي القانون التكميلي الصادر عن الجماعة الاقتصادية لدول غرب أفريقيا[12] (ECOWAS) على أحكام واسعة، والتي يمكن التعويل عليها لتقديم أي حق مشابه.

10 "Hiding In Plain Sight" (Garstka, Erdos, University of Cambridge 2017) توفر لك شرحًا وافيًا لإلغاء الفهرسة مقابل "right to be forgotten": https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043870

11 حكم "جوجل ضد أسبانيا". http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 2014

12 القانون التكميلي رقم A/SA.1/01/10 المعني بحماية البيانات الشخصية داخل ECOWAS (2010)

المواطنون والمجتمع المدني (المواد 8.1, 8.2)

الموضوع	الملاحظات
الحقوق والمسؤوليات ذات الصلة التي ينبغي معرفتها والاطّلاع عليها	يتضح أن الجزء الكبير من المسؤولية العملية لحماية الخصوصية يقع على عاتق مراقبي البيانات، وسلطات حماية البيانات. وهذا يعكس عدم الاتساق الكامن في العلاقة بين الأشخاص موضوعي البيانات، والشركات، وهيئات القطاع العام التي تعالج بياناتهم. يتمتع الأشخاص موضوعي البيانات بإمكانات عملية أو تقنية بسيطة جدًا على حماية البيانات الشخصية بمجرد جمعها. ومع ذلك، يعتبر الأشخاص أصحاب مصالح أيضًا، وليس من ناحية إنجاز الأشياء لهم أو لبياناتهم الشخصية. لا يمكن للأفراد ممارسة الحقوق التي هم على غير دراية بها، ولا يمكن للمستهلكين التأثير على السوق من خلال سلوكياتهم إذا كانوا غير مطلعين بما يكفي على اختيارات المستهلك التي يحددونها. ينبغي تمكين الأشخاص ليكونوا مستهلكين/مواطنين على دراية بالنواحي التقنية، وأن يكونوا على دراية، على سبيل المثال، بالصفقة التي يدخلون فيها عند التسجيل في الخدمات "المجانية" أو المشاركة في أنظمة وسائط التواصل الاجتماعي التي تتماشى مع بياناتهم. ومع ذلك، لدى المواطنين أيضًا توقع مشروع مفاده أنه يمكنهم تتبع أعمالهم العادية عبر الإنترنت – ومن ثمّ، يقع على المشرعين، والسلطات الإشرافية واجب مقابل ألا وهو التأكيد على أن المواطنين غير معرضين بطريقة غير مبررة لخطر الإصابة بأي أضرار جراء استخدام تكنولوجيا المعلومات والاتصال والاقتصاد الرقمي. يمكن أن تمثل أوجه التفاوت في السلطة والمعلومات حاجزًا كبيرًا في هذا الشأن، حيث يمكنها: • منع سلوك المستهلك من إحداث تأثير حتمي على السوق. • إخفاء آثار نماذج العمل الاستغلالية أو الشرهة. • تقويض الثقة في التجارة الإلكترونية، وخدمات الإنترنت الأخرى. • إعاقة أفريقيا من جني ثمار التحول الرقمي. يمكن أيضًا لنفس أنواع أوجه التفاوت أن تقوّض الثقة في العلاقة بين المواطن، والخدمات العامة. عندما تتخذ حالات تقويض الثقة تلك شكلاً نظاميًا، سواء في القطاعات التجارية أو العامة، فلا يمكن تحقيق الميزات المرجوة من الاقتصاد الرقمي. أنواع علامة الثقة، ونظام الاعتماد الموصوف أعلاه، ضمن "عناصر نظام الحوكمة"، تعتبر جزءًا مهمًا في إنشاء علاقة ثقة بين الأشخاص وخدمات الإنترنت والحفاظ عليها.
نصائح مستقلة وبناء المقدرة	يحتاج الأشخاص إلى المساعدة والتشجيع عند قيامهم بمجهودات لزيادة معرفتهم بحماية البيانات الشخصية، وصلتها بالخصوصية. وللمجتمع المدني دور يلعبه في المساعدة في التأكيد على توافر البحوث المستقلة، والتحليل، والتقارير، والمناصرة، وفي تحفيز هؤلاء الأشخاص لمعرفة المزيد عن وحماية خصوصيتهم عبر الإنترنت.
تمثيل مصالح أصحاب المصالح	لمنظمات المجتمع المدني (CSO)، والمجتمع الأكاديمي دور مهم يؤدونه، في السياق الأفريقي، يتمثل في المساعدة في ضمان عدم إعاقة جهود حماية البيانات والخصوصية بسبب تنوع القارة وحجمها. وفي هذا الصدد، نوصي منظمات المجتمع المدني أن تجتمع على المستوى الوطني والإقليمي، وأن تستفيد من المجموعات الإقليمية الحالية في الاتحاد الأفريقي. قد يكون للمجموعات الأخرى أيضًا قيمة، فيما يخص تمثيل مصالح مجموعات محددة من أصحاب المصالح بطريقة أكثر فاعلية مثل النساء والأطفال، والأشخاص ذوي الإعاقة، والمعرضين على وجه الخصوص لخطر التنمر عبر الإنترنت وما إلى ذلك.

المناصرة المستقلة	يمكن لمنظمات المجتمع المدني تنفيذ خدمة قيمة من خلال توفير تقييمات مستقلة للوضع الحالي الخاص بخصوصية، وقوانين حماية البيانات، بما في ذلك التحليل المقارن مع الدول الأعضاء الأخرى، والمناطق/ القارات الأخرى. ولها أيضًا دور محتمل في توفير مدخلات لتعزيز العمليات القائمة، مثل الاستعراض الشامل للاقران التابع للأمم المتحدة. وحتى يقوم المجتمع المدني بدور فعّال، ينبغي على الحكومات أيضًا أن تقوم بدورها لضمان تمتع منظمات المجتمع المدني ببيئة عمل بناءة وآمنة، مع وجود حماية مناسبة من المضايقة والتدخل.

التوصيات

الأساسيات: الخصوصية، والثقة، والاستخدام المسؤول

الخصوصية كأساس للثقة في البيئة الرقمية

التوصية: نحث الدول الأعضاء في الاتحاد الأفريقي على التصديق على أحكام اتفاق مالابو الواردة في التدابير السياسية الخاصة بهم وتنفيذها للتشديد على أن حماية الخصوصية عبر الإنترنت، والبيانات الشخصية ليست مجرد حق أصلي بل أيضًا عملية ضرورية طويلة المدى تهدف إلى غرس الثقة في استخدام تكنولوجيا المعلومات والاتصال والحفاظ عليها، على اعتبارها شرطًا مسبقًا للتطور المستمر للمجتمع المعلوماتي في أفريقيا. وهذا الإجراء له أهمية خاصة بالنظر إلى عوامل اجتماعية، مثل العرق، وسرعة التأثر، والإعاقة، والحرمان.

الاستخدام المستدام، والمسؤول للبيانات الشخصية في الاقتصاد المدعوم بالبيانات

التوصية: ينبغي على الحكومات وسلطات حماية البيانات مراقبة الاقتصاد المدعوم بالبيانات للتعرّف على الممارسات التي يحتمل أن تكون ضارة بالنظر إلى البيانات الشخصية، مثل التالي:

- ممارسات التسييل، وجمع البيانات التي تشوّه السوق، وتؤدي إلى صعوبة في اختيار المستهلك.
- تثير ممارسات استخدام البيانات حدوث مخاطرات جزافية (على سبيل المثال، شركة مشاريع صغيرة التي تراكم بيانات أكثر بكثير من الموارد أو المهارات التي تديرها؛ أو الشركات الكبيرة التي تدمج كميات كبيرة من البيانات في هدف واحد لا يمكن مقاومته).
- نماذج العمل الاستغلالية أو الضارية التي تفتقر إلى الشفافية والمساءلة حول تجميع واستخدام البيانات الشخصية.

كلما كان ذلك ممكنًا، ينبغي على الحكومات، وسلطات جمع البيانات العمل على تصحيح ممارسات مثل تلك الموصوفة، وتراعي في الوقت نفسه ميزات التجديد المستدام، والمنافسة، ونماذج العمل. يحتمل أن يتطلب الإنفاذ الفعّال للتدابير الوقائية مجموعة من المبادئ والقواعد المتفق عليها بين الجانبين لتنظيم عمليات نقل البيانات الشخصية عبر الحدود.

أصحاب المصالح: الحكومات، وواضعي السياسات

اتساق كبير في حماية البيانات الشخصية داخل أفريقيا

التوصية:

- وضع نهج متسق تجاه: قانون، وسياسة جمع البيانات الشخصية؛ إنشاء سلطات تنظيمية؛ وتدابير إنفاذية (يتم توضيح هذا الجزء فيما يلي، تحت جزء "سلطات حماية البيانات").
- وضع معايير متسقة ومشتركة لتقييم حد الكفاية في مستوى حماية البيانات الشخصية لتمكين عمليات نقل البيانات عبر الحدود في الاتحاد الأفريقي.

هذه عوامل مهمة لضمان التبادلية بين الدول الأعضاء في:

- البنود والشروط التي يعمل وفقها مراقبو البيانات.
- الحقوق والشروط التي يتمتع بها الأفراد فيما يتعلق بجمع واستخدام البيانات الشخصية.
- تدابير الإنفاذ، ووسائل الانتصاف القانونية المتاحة للأشخاص موضوعي البيانات.

ينبغي على الدول الأعضاء أن تراعي بشكل خاصة مبادرة سياسيات ولوائح خاصة بأفريقيا الرقمية (PRIDA) الخاصة بمفوضية الاتحاد الأفريقي في تطورها، للتأكد من قدرتها على الاستفادة من الفرص التي تقدمها لتعزيز العمل التعاوني لتنسيق السياسات واللوائح في هذه المنطقة. [MC - ديباجة p.3، والمادة 10.6]

احترام الخصوصية عبر الإنترنت وخارجه

التوصية: ينبغي على الدول الأعضاء احترام، وحماية حقوق الأفراد في الخصوصية عبر الإنترنت وخارجه. ينبغي عليهم مراجعة قوانينهم، والإجراءات، والممارسات بما في ذلك تلك المرتبطة بمراقبة الاتصالات أو التنصت للتأكد من التنفيذ الفعّال لهذه الالتزامات.

استثناءات خاصة بحماية البيانات، وقوانين الخصوصية

التوصية: ينبغي على الدول الأعضاء عدم السماح إلا باستثناءات في تطبيق قوانين حماية البيانات الشخصية والخصوصية إلا فيما يخص الشؤون المتعلقة بالسيادة الوطنية أو الأمن الوطني أو السلامة العامة، حيث تلبي هدفًا مشروعًا، وضروريًا، ومناسبًا، وليس تعسفيًا. ينبغي على الأعضاء التأكد من أي سلطات مستثناة من تطبيق قوانين حماية البيانات الشخصية، والخصوصية خاضعة لنظام إشرافي قوي، وموثوق، وقضائي مستقل يوفر الشفافية والمساءلة. [MC - ديباجة p.2، p.3]

أصحاب المصالح: مراقبو البيانات ومعالجوها

طلبات وصول الشخص موضوع البيانات (SARs) – وجهة نظر مراقب البيانات

التوصية: ينبغي إلزام مراقبي البيانات بالرد على طلبات وصول الشخص موضوع البيانات بطريقة أو تنسيق يمكن للشخص موضوع البيانات معالجتها. وغير ذلك ستكون هناك خطورة تتمثل في أن المادة 17 لن تخدم مصالح الشخص موضوع البيانات.

المساهمة في حلول متعددة الأطراف

التوصية: بينما تتطلب مشكلات حماية البيانات حلولاً متعددة الأطراف أو منسّقة، ينبغي على مراقبي البيانات أن يؤدوا دورًا في عمليات تحديد المشكلة، والتوافق في الآراء بشأن الخيارات المتاحة، وتنفيذ الحلول. وهذا ينطبق على وجه الخصوص على المناطق الموضحة بالتفصيل في الجزء الواردة أدناه، حول الحلول متعددة أصحاب المصالح:

- أفضل ممارسة، مدونات قواعد السلوك، والاعتماد،
- الموافقة،
- احترام السلامة السياقية،
- ردود طلبات وصول الشخص موضوع البيانات (SARs)،
- سرية وسلامة البيانات الشخصية، و
- فترات الاحتجاز.

ينبغي على مراقبي البيانات إيلاء اهتمام خاص لعمليات التطوير لوضع أفضل الممارسات – مثل الخصوصية حسب التصميم، والخصوصية بشكل افتراضي. يوجد، من بين جملة أمور أخرى، عوامل مهمة لتحديد متى لا يجب جمع أو الاحتفاظ بالبيانات.

إن قرارات جمع أو معالجة أو الاحتفاظ بالبيانات تتبع عادة مجموعة من اختيارات التصميم، والتنفيذ الأخرى، والتي أدخلت خلال عملية تطوير المنتجات. ينبغي على مراقبي البيانات الاستفادة من زيادة حجم التوجيهات في تصميم النظام القائم على القيمة أو الأخلاقي لدمج المبادئ التي تعزز الخصوصية في منتجاتها من المراحل المبكرة. وسيقلل هذا الإجراء من التكلفة اللاحقة لتحقيق الامتثال لمتطلبات حماية البيانات، ويبعث على الثقة كمردود ناجم عن الآخرين.

أصحاب المصالح: سلطات حماية البيانات

دور واستقلالية سلطات حماية البيانات

تعتبر سلطة حماية بيانات وطنية مستقلة (DPA) عنصرًا حيويًا لإطار قانوني، ومؤسسي من أجل بناء الثقة عبر الإنترنت كما هو متوخى في اتفاق مالابو (المواد 12-10).

التوصيات: ينبغي شغل منصب مفوّض سلطة حماية البيانات (DPA) بالتعيين، وأن يكون التعيين لمدة محددة، وأن يخضع لإشراف المجلس الاستشاري الذي يمثل أصحاب المصالح، بما في ذلك ممثلي المواطنين (المجتمع المدني)، والمستهلكين (المنظمات الاستهلاكية)، ومراقبي البيانات التجارية (الغرف التجارية)، والمؤسسات الأكاديمية، والحكومية، ومتى كان ذلك ممكنًا، مشغلو أنظمة اعتماد حماية البيانات الشخصية (راجع التوصية 9، أدناه).

ينبغي للدول الأعضاء تأسيس سلطة حماية بيانات للتأكيد على مراعاة قوانين حماية البيانات الشخصية والخصوصية الوطنية. ينبغي على سلطة حماية البيانات أن يكون لديها تفويض واضح، وسلطات، وموارد لتتمكّن من القيام بالآتي:

- مراقبة الامتثال للقانون المعمول به حول الخصوصية، وحماية البيانات وتعزيزه.
- تسهيل تطوير مدونات السلوك الصناعية الطوعية.
- تلقي ومعالجات المطالبات، والالتماسات، والشكاوى المتعلقة بمعالجة البيانات الشخصية، وإبلاغ أصحاب البلاغات بالنتائج.
- فرض عقوبات وسبل انتصاف لمخالفات القانون.
- توفير تفسيرات، وعند الضرورة، اتخاذ قرارات إدارية مختصة تتعلق بتطبيق القوانين.
- الوصول إلى حد الكفاية في حماية عمليات نقل البيانات عبر الحدود.
- التعاون في وتبادل المعلومات، والتوجيهات، وتجربة أفضل الممارسات مع نظراء سلطة حماية البيانات (DPA).
- الاشتراك مع أصحاب المصالح الآخرين (مثل الحكومات، ومراقبي البيانات، والمجتمع المدني) لوضع توجيهات تنظيمية، وإطارات الثقة، وتدابير تمكين مثل تعليم أصحاب المصالح.
- إبلاغ الأشخاص، ومراقبي البيانات حول حقوقهم، والتزاماتهم.
- وضع مقترحات لتحسين الإطار التشريعي والتنظيمي لمعالجة البيانات الشخصية.

لمصلحة الثقة، والشفافية، ينبغي على الدول الأعضاء تشجيع أو الطلب من سلطات حماية البيانات (DPA)، والكيانات الأخرى التي تتحمل مسؤولية مراقبة الخصوصية، وحماية البيانات الشخصية، الإبلاغ بصورة علنية عن أنشطتها عند الاقتضاء.

طلبات الوصول إلى الشخص موضوع البيانات (SARs) - وجهة نظر سلطة حماية البيانات

التوصية: ينبغي على الدول الأعضاء التأكد من أن سلطات حماية البيانات تمتلك السلطات المناسبة المرتبطة بطلبات وصول الشخص موضوع البحث (SARs) لاستكمال الالتزامات الموضحة في المادة 12(2) من الاتفاق.

- بينما يمتلك الأشخاص موضوعي البيانات الحق في طلب نسخ من البيانات الشخصية من مراقب بيانات، فينبغي على سلطات حماية البيانات (DPA) أن تتمكّن من مراقبة النتائج المرتبطة بالتشريع ذي الصلة. ينبغي أن تمتلك سلطات حماية البيانات السلطات للتأكيد على معالجة طلبات وصول الشخص موضوع البيانات بطريقة تخدم المصالح الشرعية للشخص موضوع البيانات، ولا تفرض عقبات على الشخص موضع البيانات (مثل، رسوم مفرطة، وإجراءات معقدة، إلخ)، ولا تتسبب في تحميل مراقب البيانات بأعباء غير مبررة.

الموضوع: حلول أصحاب المصالح المتعددين

يوفر هذا الجزء "التوصيات" في مناطق متعددة حيث ستعتمد النتائج الناجحة على الجهود المنسقة بين أصحاب المصالح.

أفضل ممارسة، مدونات قواعد السلوك، وأنظمة الاعتماد

التوصيات:

- سعيًا لتحقيق الأهداف متعددة الأطراف الواردة في هذا الجزء، ينبغي على الدول الأعضاء إقامة منتديات أصحاب المصالح المتعددين، بما في ذلك سلطات حماية البيانات، ومراقبي البيانات، وأصحاب المصالح الأخرى، لاستكمال القاعدة القانونية بمدونات قواعد السلوك الطوعية التي تنفذ أفضل الممارسات في حماية بيانات الشخصية، والخصوصية.
- ينبغي على الحكومات، والهيئات الصناعية، والاستهلاكية مراعاة إدخال أنظمة الاعتماد للإشارة إلى أن المنتج أو الخدمة يلبي معايير حماية البيانات. على سبيل المثال، قد يدل الاعتماد على أن مراقب البيانات قد خضع للمراجعة في ضوء أفضل معايير الممارسات المتعلقة بالخصوصية حسب التصميم أو أمن البيانات أو الشفافية فيما يتعلق بالبنود والشروط.

تشكيل لجنة حماية البيانات الشخصية على مستوى أفريقيا

التوصية: تأسيس لجنة على مستوى أفريقيا، تركّز بشكل خاص على موضوع الخصوصية، وحماية البيانات الشخصية، لتسهيل تنسيق، ومشاركة المعلومات بين أصحاب المصالح للمساعدة في تحديد مناطق الخصوصية التي تحتاج إلى موارد، وتقديم المشورة لواضعي السياسات في الاتحاد الأفريقي بشأن الاستراتيجيات الإقليمية، وبناء القدرة.

ستكون اللجنة عبارة عن شبكة متطورة، وصغيرة وموثوقة من الخبراء تشكلها مفوضية الاتحاد الأفريقي بالتعاون مع مجتمع الإنترنت الأفريقي. قيادة اللجنة ينبغي أن تكون من أصحاب المصالح المتعددين. ينبغي أن تجذب خبرات من منظمات على المستوى الوطني وعلى مستوى أفريقيا، ومؤسسات، مثل الجامعات الاقتصادية الإقليمية (RECs)، وتتضمن سلطات حماية البيانات (DPA)، وشركات الأعمال، وممثلين من المؤسسات الأكاديمية، والمجتمع الفني، والمجتمع المدني. عن طريق هيكلة نفسها كشبكة أصحاب مصالح متعددين مرنة، يمكن أن تضمن اللجنة اتخاذها موقعًا أفضل لمعالجة تحديات الخصوصية الناشئة، والمستقبلية التي تواجه أفريقيا.

يمكن أن يُطلب من اللجنة تقديم المشورة والدعم لمفوضية الاتحاد الأفريقي في نشاطات الخصوصية الخاصة بها عن طريق:

- تقديم المشورة لمفوضية الاتحاد الأفريقي حول سياسات ومشكلات حماية البيانات الشخصية، والخصوصية، مثل نشاطات بناء القدرة؛
- تطبيق تبادلية طويلة المدى لتوصيات أفضل الممارسات المتعلقة بحماية البيانات الشخصية، والخصوصية؛
- تحديد المناطق البحثية المرتبطة بوضع تعليمات، وسياسات عامة أو خاصة بالقطاع، مع ظهور ظروف ومتطلبات جديدة؛
- تحديد طرق لدعم سلطات حماية البيانات (DPA) لبناء القدرة ومشاركة معلومات على المستوى الإقليمي وعلى مستوى الاتحاد الأفريقي؛
- إقامة منتدى أصحاب مصالح موثوق بهم للكشف المسؤول، والمنسق عن انتهاكات البيانات؛
- تقديم طرق لزيادة مهارات متخصصي الخصوصية (على سبيل المثال، كجزء من برنامج الاعتماد)؛
- مساعدة مفوضية الاتحاد الأفريقي على صياغة استراتيجيات تعاونية عبر الحدود للخصوصية، وبناء القدرة.

ينبغي تنسيق عمل اللجنة مع اللجنة الفنية المتخصصة التابعة لتكنولوجيا الاتصالات والمعلومات (ICT) في الاتحاد الأفريقي، تحت إشراف مفوضية الاتحاد الأفريقي. يمكن تطوير التفاصيل المتعلقة بالاسم والمهمة والرؤية والأهداف والأنشطة المفصلة عن طريق مفوضية الاتحاد الأفريقي بالتعاون مع لجنة الإنترنت الأفريقية.

بوجه خاص، نوصي بهذا الإجراء كطريق لبناء الثقة في نظام الاعتماد الخاص بحماية البيانات الشخصية، بناءً على المفاهيم الموضحة أعلاه، ضمن "عناصر نظام الحوكمة". أحد الأهداف المحدد لهذه اللجنة هو إنشاء إطار عمل موثوق به لوضع نظام الحكومة موضع التنفيذ. سيحدد الإطار الأدوار الخاصة بقيمي التوافق، ومراجعي الامتثال، وهيئات الاعتماد. ستكون هذه الهيئات، بدورها، مسؤولة عن تدوين المعايير المقابلة لكل دور في نظام الحوكمة.

- فيما يتعلق بمراقبي البيانات، وسلطات حماية البيانات، سيكون قدرًا كبيرًا من التدوين مقترحًا بالفعل عن طريق التشريعات السارية.
- بالنسبة إلى هيئات الاعتماد أو التوجيهات المرتبطة بآليات أمن المعلومات، قد يكون من الضروري تحديد أو تطوير معايير التقييم ذات الصلة.
- بالنسبة إلى أنظمة أمن المعلومات، ينبغي على الدول الأعضاء البحث عن مصادر توجيهات مؤهلة، وطنيًا، وإقليميًا، ودوليًا إذا لزم الأمر.

الموافقة

التوصيات:

- ينبغي على سلطات حماية البيانات العمل مع مراقبي البيانات (على سبيل المثال، من خلال الهيئات الصناعية) من أجل تكوين نهج تعاوني، ومتعدد أصحاب المصالح لمعالجة مشكلة الموافقة، بهدف إحداث توازن بين التدابير الفنية (مثل، إيصالات الموافقة)، والتدابير التنظيمية (مثل، إشعارات ملفات تعريف الارتباط)، وتدابير تصميم المنتج (مثل، عناصر تحكم، وتجربة المستخدم).
- بينما تكون الموافقة مؤهلة من الناحية القانونية (على سبيل المثال، قيود قانونية تحدد أن الموافقة ينبغي أن تكون مستنيرة، ومحددة، وبدون ضغوط، وقابلة للإلغاء، إلخ)، وينبغي على سلطات حماية البيانات تشكيل مجموعة أصحاب مصالح متعددين، بما في ذلك موفري الخدمات، والمحامين، والمجتمع المدني، والمصممين، والهيئات الأكاديمية، لتقرير ما إذا كانت المتطلبات القانونية تمت تلبيتها على أكمل وجه عن طريق التدابير الفنية أو التنظيمية أو الموجهة نحو المستخدمين أو مزيج منها.

الغرض من الاعتماد

التوصيات:

- ينبغي أن يكون لدى سلطات حماية البيانات الصلاحيات والموارد اللازمة لتعزيز مبدأ الخصوصية "الغرض من الجمع"، على النحو المنصوص عليه في المادة 13 من الاتفاق. يتطلب التنفيذ الفعّال للمبدا حلاً تعاونيًا ومن ثمّ يتم وضع نهج متعدد الأطراف. يمكن وينبغي أن يجذب هذا النهج متعدد الأطراف المبادئ المقررة للخصوصية حسب التصميم، والخصوصية بشكل افتراضي – خاصة في مواضيع مثل نزاهة قرارات التصميم، وتقليل البيانات إلى الحد الأدنى، واحترام السلامة السياقية.
- ينبغي على الحكومات التأكد على أن سلطات حماية البيانات تمتلك الموارد لمراقبة وتعزيز مبدأ "الغرض من الجمع". ينبغي على سلطات حماية البيانات إصدار توجيهات إلى الموردين، وموفري الخدمات حول الحاجة إلى الشفافية، والمساءلة فيما يتعلق بهذا المبدأ، كأساس لثقة المستهلكين. وإذا لزم الأمر، ينبغي أن تتم الاستعانة بتشريعات حماية العملاء لتعزيز حقوق الشخص موضوع البيانات في البيئة الرقمية.

فترات الاحتفاظ بالبيانات

التوصيات:

- ينبغي أن تعمل سلطات حماية البيانات مع مراقبي البيانات (على سبيل المثال، من خلال الهيئات الصناعية) للتوصل إلى اتفاق بشأن كيفية وضع مبدأ فترات الاحتفاظ موضع التنفيذ. وهذا يحتمل أن يتطلب مزيجًا من التدابير الفنية (مثل، تعريف بيانات التعريف لتسجيل متى تم جمع البيانات الشخصية، والفترة التي ينبغي حذفها فيها)، والتدابير التنظيمية، مثل تدقيق ممارسة مراقبي البيانات. [MC - المادة 22]
- يتضمن أيضًا مثل هذا النوع من تدابير التدقيق وجود هيئة قادرة ومدعومة بالموارد تكون مسؤولة عن تنفيذ عمليات التدقيق. يدعو هذا الاتفاق إلى تعيين هذه الهيئة كسلطة حماية البيانات. يجب على الحكومات أن تقرر، في سياق الدولة القومية، سواء تم تنفيذ مثل هذا النوع من عمليات المراجعة على أساس قانوني أو النهج القائم على إدارة المخاطر أو بحسب مدونات قواعد السلوك في قطاعات معينة خاضعة للتنظيم (مثل، الرعاية الصحية، والخدمات المالية، وإلخ). [MC - المادة 12(2)(g)] [MC - المادة 17]

الموضوع: سلامة المواطن الممكّن رقميًا

توقعات المواطنين، وواجب رعاية الحكومات

التوصيات:

- كما تمت الإشارة إليه أعلاه، ضمن "المواطنون والمجتمع المدني"، ينبغي على الأفراد التنازل عن قدر كبير من التحكم في بياناتهم الشخصية بمجرد إفشائها. يتحمل لذلك مراقبو البيانات قدرًا من المسؤولية عن ضمان تحقيق ممارسات جيدة ونتائج تحافظ على الخصوصية.
- ومع ذلك، ينبغي على المواطنين الاستفادة من الإنترنت والمصادر الأخرى للتوجيهات للتأكد من أنهم على بينة كافية بمخاطر وميزات أنشطتهم في الاقتصاد الرقمي، والبيئة المتصلة، سواء في مساحات المنزل أو العمل أو المساحات العامة.
- هناك دور مقابل للحكومات، سواء كان مباشرًا أم غير مباشرًا، تؤديه لتعزيز ممارسة الأفراد لحقوقهم في الخصوصية، عن طريق المساعدة للتأكد من أن المواطنين على دراية وعلم بكيفية ممارسة حقوقهم بحسب قانون حماية البيانات الشخصية، والخصوصية.
- ينبغي على السلطات الإشرافية والحكومات اتخاذ خطوات للتأكد من أن موفري الخدمات عبر الإنترنت وموردي المنتجات يتمتعون بالشفافية الكافية حول نماذج الأعمال، وإمكانات المنتجات ومن أن الأشخاص في المكان المناسب الذي يؤهلهم للقيام باختيار مستنير حول الآثار المترتبة على خصوصية المنتجات، والخدمات المعروضة عليهم.

منظمات المجتمع المدني (CSO)

التوصيات:

- ينبغي على الدول الأعضاء الاعتراف بدور منظمات المجتمع المدني، ودعمها في:
  - تطوير بحوث تثقيفية، وتحاليل، وتقارير، وبرامج تعليمية، ومواد توعية حول حماية البيانات الشخصية، والخصوصية لمساعدة المواطنين على فهم وممارسة حقوقهم؛
  - البحث في ميزات أمان البيانات، والخصوصية الخاصة بالتطبيقات عبر الإنترنت، والخدمات للوقوف على الممارسات الجيدة والسيئة؛
  - تقديم مراجعات مستقلة، وموضوعية، وتستند إلى الأدلة لـ "حالة الخصوصية، وحماية البيانات"، باعتبارها مهمة مراقبة لحماية وتقديم مصالح الأفراد.
- يتم تشجيع الدول الأعضاء على التعامل مع منظمات المجتمع المدني (CSO) كشركاء في تشكيل قطاع آمن، وعلى دراية وقادر من "المواطنين الممكنين رقميًا" وينبغي على تلك الدول أن تحرص على أن يكون لمنظمات المجتمع المدني (CSO) الإطار المناسب، وآليات الحماية القانونية والتي تساهم من خلالها في هذه الشراكة.

الموضوع: تدابير الاستدامة والتمكين

تطالب المادة 31 من الإعلان الوزاري (آديس أبابا، نوفمبر 2017) من مفوضية الاتحاد الأفريقي "التأكد من متابعة توقيع وتنقيح الدول الأعضاء" لـ "اتفاق مالابو".

وبناءً على ذلك، نشجّع الدول الأعضاء على تبني النهج التالي، بغية زيادة السرعة والثقة التي يمكن للأعضاء من خلالها تطبيق وتنفيذ التدابير التي ينص عليها الاتفاق.

التوصيات: ينبغي على واضعي السياسات الاشتراك بشكل تعاوني مع المجتمع المدني، والمناصرين للخصوصية، وشركات الأعمال، والهيئات الأكاديمية، وأصحاب المصالح الآخرين لإنتاج مجموعة من المواد التدريبية والشارحة التي يسهل الوصول إليها والمعنية بالمواضيع التالية. سيكون هدف هذه المواد هو التغلب على العقبات المتمثلة في قلة الوعي، والمعرفة، والفهم.

- أساسيات الخصوصية الرقمية، ومخاطرها، وميزاتها
- نماذج العمل الشائعة و/أو السائدة للخدمات عبر الإنترنت
- الإعلان، وتقليل البيانات إلى أقل حد في الاقتصاد المدعوم بالبيانات

- الوعي بالثقافات المختلفة، وتوقعات الخصوصية، داخل وخارج السياق الأفريقي
- الخصوصية حسب التصميم، وإمكانات التقنيات التي تعزز الخصوصية
- التضمين/الاستبعاد الرقمي وأصحاب المصالح المهمشين
- المخاطر والمضار التي قد تنشأ من النشاطات عبر الإنترنت، ونماذج العمل المدعومة بالبيانات
- الآثار المترتبة على التقنيات الناشئة (تعدين البيانات، والتعليم الآلي، والذكاء الاصطناعي؛ الأنظمة المستقلة؛ وإنترنت الأشياء، إلخ)
- ... ومثل هذه المواضيع أصبحت ذات أهمية من وقت لآخر.

ينبغي أن تشكّل هذه المواد أساسًا لبرنامج اجتماعات المائدة المستديرة لأصحاب المصالح – بما في ذلك مشاركة واضعي السياسات – والتي يكون الهدف منها استغلال المعرفة والوعي المكتسب، ووضعه موضع الاستخدام العملي الفوري في شكل إشراك صاحب مصلحة جديد. ينبغي أن يكون للبرنامج الأهداف التالية:

- تبادل المعلومات وبناء الثقة بين أصحاب المصالح المهتمين بأمور السياسات، والأمور الفنية، القانونية، والتجارية، والأكاديمية، وأصحاب المصالح في المجتمع المدني؛
- زيادة معرفة، ووعي، وثقة واضعي السياسات في المواضيع الجديدة؛
- التأكد من أن واضعي السياسات لديهم فرصة تطبيق تلك المعرفة مع الأوساط المعنية؛
- إعطاء أصحاب المصالح المهتمين، والمطلعين صوتًا لصياغة مستقبل الإنترنت لدولهم، ومناطقهم، وقارتهم.

ربما يود الأعضاء مراعاة تشكيل النماذج مثل تشكيل برنامج حول النهج المرتبط بأمن الفضاء الإلكتروني المنصوص عليه في المادة 31 من إعلان أديس أبابا (AU/CCICT-2)، والذي يتوخى مؤتمر أمن الفضاء الإلكتروني السنوي، وشهر أمن الفضاء الإلكتروني على مستوى القارة.

على سبيل المثال، قد يكون من المفيد وضع جدول منتظم للآتي:

- نشر واحد من مواد التدريب المدرجة أعلاه،
- فترة للقراءة، والتدبير،
- ورشة عمل طاولة مستديرة لأصحاب المصالح لمناقشة الموضوع والموافقة على الإجراءات المنبثقة.

يمكن أن تبلغ هذه الأنشطة ذروتها في أي مؤتمر سنوي وشهر من التركيز على حماية البيانات والخصوصية عبر الإنترنت.

نبذة عن جمعية الإنترنت

تدعم جمعية الإنترنت (ISOC) وتعزز تطور الإنترنت باعتباره بنية تحتية فنية عالمية، ومواردًا لحياة الناس الأغنياء، وقوة من أجل الخير في المجتمع. بالعمل خلال مجتمع عالمي يتألف من فروع وأعضاء، فإن جمعية الإنترنت تتعاون مع عدد كبير من المجموعات لتعزيز التكنولوجيات التي تُحافظ على أمان الإنترنت وأمنه، وتناصر السياسات التي تمكّن وصول الجميع إلى الإنترنت.

معًا، يمكننا التركيز على:

- بناء ودعم المجتمعات التي تجعل الإنترنت يعمل بنجاح؛
- النهوض بتطوير وتطبيق بنية الإنترنت، والتكنولوجيات، والمعايير المفتوحة؛
- تعزيز السياسة المتوافقة مع رؤيتنا للإنترنت.

نبذة عن مفوضية الاتحاد الأفريقي

أُطلق الاتحاد الأفريقي (AU) رسميًا في يوليو من عام 2002 عقب القرار الصادر في عام 1999 من قِبل المؤسسة السابقة، منظمة الوحدة الأفريقية (OAU)، والتي تأسست في 1963 لإنشاء مؤسسة قارية جديدة للاستفادة مما قامت به من أعمال. بلغ إجمالي الدول المنضمة إلى المنظمة الجديدة 54، وظلت مقراتها في أديس أبابا بإثيوبيا.

مفوضية الاتحاد الأفريقي (AUC) هي الأمانة العامة للاتحاد الأفريقي والمكلفة بمهام تنفيذية. وهي تتألف من عشرة مسؤولين، الرئيس، ونائبه، وثمانية مفوضين. يمثل هذا الهيكل الاتحاد الأفريقي ويحمي مصالحه تحت رعاية مجلس رؤساء الدول والحكومات وأيضًا اللجنة التنفيذية.

يقع على عاتق مفوضية الاتحاد الأفريقي الحقائب الوزارية التالية: السلام والأمن، والشؤون السياسية، والتجارة، والصناعة، والبنية التحتية، والطاقة، والشؤون الاجتماعية، والاقتصاد الريفي، والزراعة، والموارد البشرية، والعلم والتكنولوجيا، والشؤون الاقتصادية.

الرؤية التوجيهية لجدول أعمال 2063 هي رؤية الاتحاد الأفريقي: "أفريقيا متكاملة، ومزدهرة، وآمنة، تدفعها سواعد مواطنيها أنفسهم إلى الأمام، وتتبوأ موقعها في الساحة العالمية كقوة نشطة". مهمة مفوضية الاتحاد الأفريقي هي "أن تصبح مؤسسة فاعلة، وتضيف قيمة، وتدفع التكامل الأفريقي، وعملية التطور إلى الأمام بالتعاون الوثيق مع دول الاتحاد الأفريقي، والمجتمعات الاقتصادية الإقليمية، ومواطني أفريقيا".