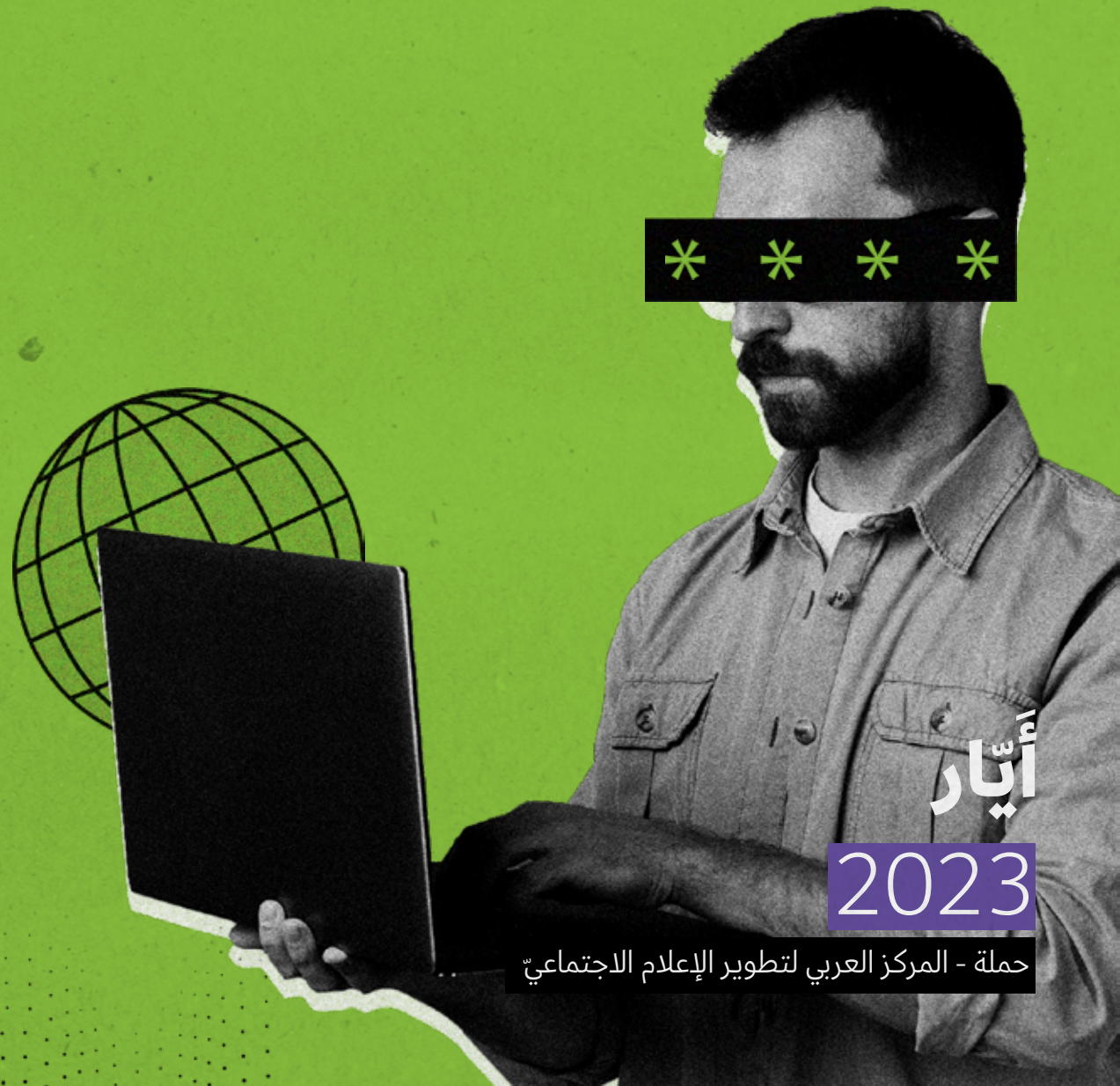
الدّليل الإجرائي لحماية البيانات الشّخصية الفلسطينية في الفضاء الرّقمي



أيّار

2023

حملة - المركز العربي لتطوير الإعلام الاجتماعيّ

حملة – المركز العربي لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for the Advancement of Social Media

الدليل الإجرائي لحماية البيانات الشخصية الفلسطينية في الفضاء الرقمي

إعداد: آندرسن فلسطين
تدقيق ومراجعة: كاثرين أبو عمشا
تدقيق وتحرير لُغويّ: شركة رِتاج للحلول الإداريّة
نقلها إلى الإنجليزيّة: شركة رِتاج للحلول الإداريّة
تحرير اللغة الإنجليزية: ياسمين عراقي

نتطلّع لتواصلكم/ ن معنا عبر القنوات التّالية:

البريد الإلكترونيّ: info@7amleh.org
الموقع الإلكترونيّ: www.7amleh.org
الهاتف: 20670 7740 (0) 972+

تابعونا وتابعننا عبر صفحاتنا على مِنصّات التّواصل الاجتماعيّ: 7amleh

يقدم حملة - المركز العربي لتطوير الإعلام الاجتماعي جزيل الشّكر والتقدير لائتلاف الحقوق الرّقمية الفلسطينيّة على مشاركته الغنيّة في مراجعة ونقاش المسودة الأولى لهذا الدليل.

قائمة المحتويات

05 المقدمة

07 لماذا يجب الالتزام بقواعد الخصوصيّة

07 مفاهيم أساسيّة

09 ما هي العمليات التي تتمّ على البيانات في الفضاء الرّقمي

09 المبادئ الأساسية لجمع ومراجعة البيانات

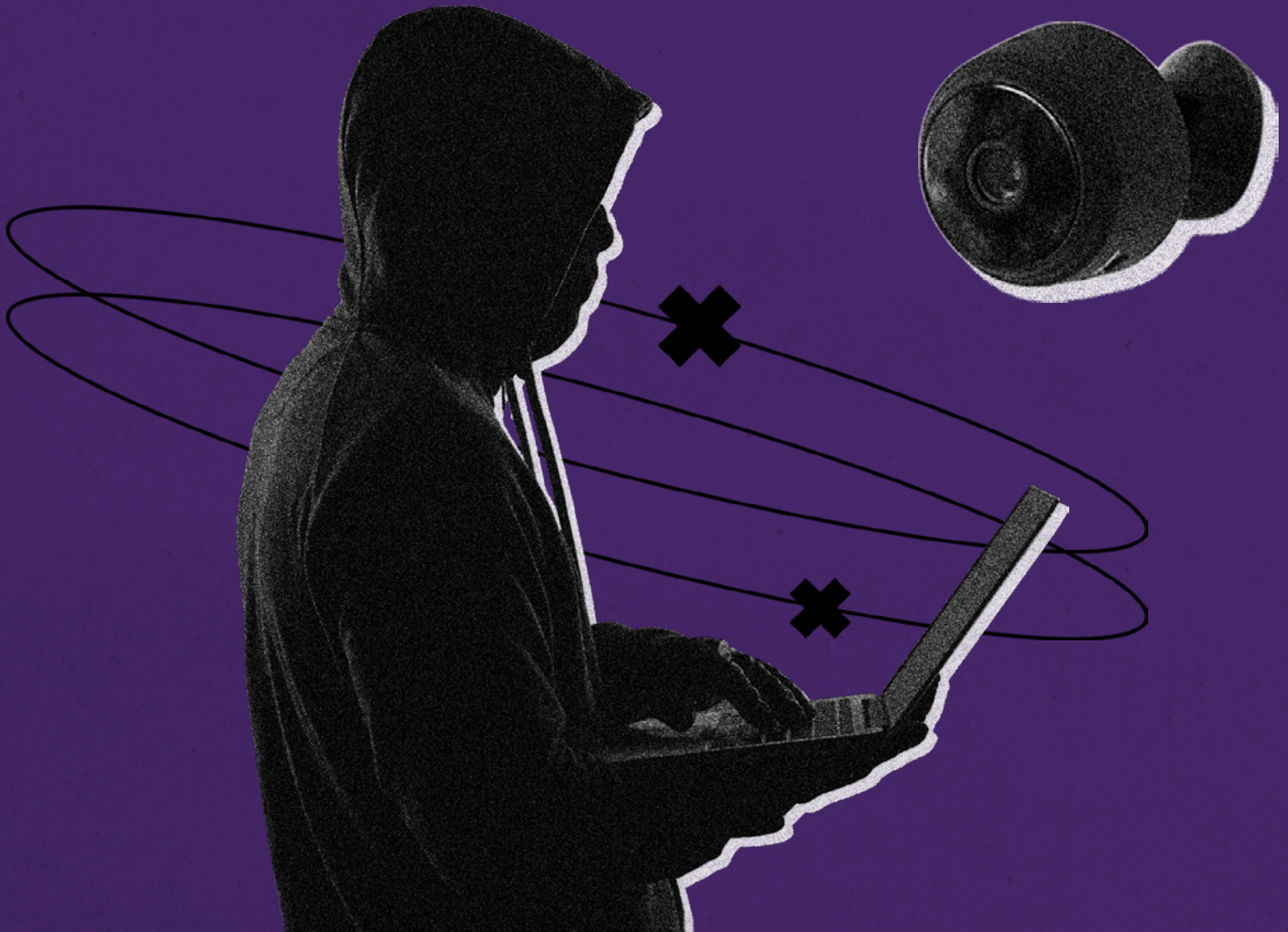
11 الأسس القانونية لجمع ومراجعة البيانات

13 حقوق صاحب البيانات

15 الالتزامات المفروضة على الجهة التي تعالج البيانات

17 ما الذي يختلف عندما تُوكِل الجهة المتحكمة بالبيانات عملية معالجة البيانات إلى جهة أخرى

19 أمثلة عملية



مقدمة

أكد مجلس حقوق الإنسان، التابع للأمم المتحدة منذ عام 2012، على ضرورة حماية حقوق الإنسان في الفضاء الرقمي كما يجدر في أرض الواقع؛ إذ صرّح في أحد قراراته أنّ: «نفس الحقوق التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تحظى بالحماية أيضاً على الإنترنت»،[1] واستمرّ في التأكيد على ذلك بشكل مستمر؛ إذ أصبحت تُعرف هذه الحقوق بـ»الحقوق الرقمية»، التي يجدر أن يتمتع بها جميع الأفراد حول العالم، بمن فيهم الشعب الفلسطيني.

ركّز حملة - المركز العربي لتطوير الإعلام الاجتماعي أهدافه ومجالاته للعمل على الدفاع عن الحقوق الرقمية الفلسطينية؛ سعياً للوصول إلى فضاء رقمي آمن وعادل وحر للفلسطينيين والفلسطينيات. كما وخصّص برامجه لتكفل الرصد والبحث ورفع الوعي والمناصرة لجميع هذه الحقوق؛ لا سيّما الحقُّ في الخصوصية، وحماية البيانات الشخصية الرقمية، التي يركّز هذا الدليل، بإجراءاته المفصّلة، على ضمان حمايتها.

تشكل الفجوة بين حقِّ الخصوصية وحماية البيانات الرقمية، في المواثيق الدولية الأساسية، لحقوق الإنسان والمعايير الدولية الفضلى، وبين الواقع الفلسطيني إشكالاً كبيراً؛ جعل من خصوصية وأمان الفلسطينيين/ات وحقوقهم/ن الأخرى ذات العلاقة عرضة للخطر والاستغلال، الأمر الذي عمل حملة مُطوّلاً لتغييره. فيأتي هذا الدّليل، «الدّليل الإجرائي لحماية البيانات الشخصية الفلسطينية في الفضاء الرقمي»، كإحدى الخطوات، ضمن سلسلة من إصدارات وأعمال حملة، التي تستهدف تحسين واقع الخصوصية، وحماية البيانات الفلسطينية. إذ سبق هذا الدليل عدد من الإصدارات، واستطلاعات الرأي والحملات الرقمية واللقاءات مع أصحاب المصلحة والقرار ذات العلاقة بحق الخصوصية. ولعل من أبرز ما توصّلت إليه حملة حاجةَ الفلسطينيين/ات ودعمَهم لإقرار قانون فلسطيني لحماية البيانات الشخصية؛ الذي وصلت نسبته نحو 69% ممن جرى استطلاعهم/ن بالخصوص.

تبرز أهمية حماية هذا الحق في العصر الرقمي نتيجة لتوسع الممارسات، التي يقوم بها الأفراد والمجتمعات والجهات الحكومية وغير الحكومية، بما فيها القطاع الخاص، حيث تتطلب التعامل مع البيانات والمعلومات الرقمية، ويمكن نسبها لشخص أو جهة معينة، في ظل تطور قدرة الدول والشركات وغيرها من الجهات على الوصول إليها، واستخدامها لأغراض مختلفة قد يشكّل انتهاكاً للحقِّ في الخصوصيّة.

فيما يخص دولة فلسطين، فإن الحق في الخصوصية هو حقٌّ دستوري كفله القانون الأساسي الفلسطيني المعدّل لعام 2003. إضافة لذلك، فإنّ دولة فلسطين هي عضو في العهد الدولي الخاص بالحقوق المدنية والسياسية، الذي يكفل الحقّ في الخصوصية في الفضاء الفعلي والرّقمي. وعليه، فإنّه يجب على الأفراد والجهات الحكومية وغير الحكومية الفلسطينية الالتزامُ باحترام وحماية الحقِّ في الخصوصية في مختلف الفضاءات.

1 قرار مجلس الأمم المتحدة لحقوق الإنسان (A/HRC/RES/20/8)، الدورة 20، 16 تموز 2012. متاح عبر:
https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/23/PDF/G1215323.pdf?OpenElement

التطورات التكنولوجية المرتبطة به من جهة أخرى. وبشكل عام، فإنّ أهم الأدوات القانونية، التي تكفل الحق في الخصوصية، في الفضاء الرقمي، هي النظام الأوروبي لحماية البيانات، الذي يمثل المعايير الفضلى في عملية حماية البيانات في مختلف المراحل، التي تمرّ بها، والذي اعتمدته العديد من الجهات خارج الاتحاد الأوروبي كمعيار مرجعي أمثل، لتطبيق قواعد احترام وحماية الحق في الخصوصية، في الفضاء الرقمي، خاصّة إذا كانت هذه الجهات تدخل في سياق تعاملاتها المعتادة مع أفراد أو جهات أوروبية.

بناءً على ذلك، تمّت صياغة وإعداد هذا الدّليل لإرشاد الأفراد والمؤسسات والشركات في فلسطين، نحو تطبيقٍ أفضل، في حماية الحقِّ في الخصوصية أثناء التّعامل مع البيانات الرّقمية المختلفة، وذلك بالاستناد إلى القوانين الفلسطينية السارية والقانون الدّولي لحقوق الإنسان، مع الاستئناس بالممارسات الفضلى، كما وردت في النّظام الأوروبي لحماية البيانات، [2] وذلك لضمان شمول الدليل على أعلى معايير الحماية، التي يمكن توفيرها للحقّ في الخصوصية بالفضاء الرقميّ.

2 النظام الأوروبي لحماية البيانات 679/2016 ،(GDPR)، متاح عبر: https://gdpr.eu/tag/gdpr/.

لماذا يجب الالتزام بقواعد الخصوصيّة؟

تعدّ خصوصية الأفراد، بما فيها البيانات الشخصية، أمراً بالغ الأهمية؛ تجدر حمايته والالتزام به، وذلك لأسباب عدة أهمها:

- اِمتثالاً لواجب قانوني يحتّم الالتزام باحترام وحماية الحقّ في الخصوصية في الفضاءَين الفعليّ والرقميّ.
- ضماناً لأمان وسلامة التعامل مع البيانات الخصوصية لمستخدمي/ات الإنترنت، وبما يسهم في تحقيق استخدام آمن للشبكة.
- حفاظاً على المصداقية والشفافية وزيادة ثقة المتعاملين مع الجهات الملتزمة سواء كانت حكومية أو تجارية.

مفاهيم أساسية

وفقاً للنظام الأوروبي لحماية البيانات[3] تعد المصطلحات أدناه من أبرز المفاهيم الأساسية الواجبة الفهم، لضمان التعامل مع البيانات الشخصية بشكل سليم:

- البيانات الشخصية: أي معلومة تخصّ شخصًا طبيعيًّا محدّدًا أو غير محدد.
- صاحب البيانات: هو شخص طبيعي معيّن، يمكن التعرف عليه بشكل مباشر أو غير مباشر، من خلال أحد البيانات الشخصية الخاصة به، كالمعلومات الإلكترونية الخاصة، مثل:

3 النظام الأوروبي لحماية البيانات، مادة (1.4)، متاح عبر: https://gdpr.eu/article-4-definitions/.

أو معلومات أخرى مثل: الاسم، رقم البطاقة التعريفية، معلومات لها علاقة بحالة صاحب البيانات، النفسية أو العقلية أو الاجتماعية أو الاقتصادية.

ويمكن التعرف على صاحب البيانات بشكل مباشر، إذا كان التعرّف عليه ممكناً فقط من خلال معلومة واحدة، يمكن الحصول عليها من جهة واحدة، مثل: اسم الشخص. أمّا الطريقة غير المباشرة فتكون عندما يتمّ تجميع بيانات مختلفة من جهات مختلفة، ثم ربطها، بحيث تعطي معلومات محدّدة عن شخص معين، مثل المعلومات المتعلقة بالجنس أو تاريخ الميلاد.

- البيانات الشّخصية الحسّاسة: تلك البيانات التي تعدّ أشد حساسية من البيانات الشخصية العادية، التي تسبب ضرراً أكبر لصاحبها في حال حدوث أيّ اختراق لها، مثل المعلومات التي تصف أصول الشخص وعرقه أو توجّهاته السياسية أو الدينية أو الفلسفية أو الجنسية، أو اشتراكات الشخص في الاتحادات التجارية، المعلومات الجينية أو البيومترية، التي يتم استخدامها للتعرف على الشّخص، أو المعلومات الصحية المتعلقة بشخص معيّن.
- الجهة المتحكّمة في البيانات: الجهة التي تقوم بجمع ومعالجة البيانات، وتعني الشخص الطبيعي أو المعنوي، الذي يقوم بنفسه أو بالاشتراك مع جهة أخرى بتحديد الهدف من جمع البيانات وحيثيات هذا الجمع.

1. الحكومة: تقوم الحكومة بجمع ومعالجة بيانات المواطنين لعدة أسباب، منها: لغايات إدارة القطاع الحكومي وتقديم الخدمات للجمهور، الأرشفة، غايات إحصائية، وغيرها.
2. الشركات: تقوم الشركات بجمع ومعالجة البيانات الأفراد لعدة أسباب، منها: تحسين تجربة العميل على الموقع أو التطبيق، تقديم خدمة معينة، التسويق وغيرها.
3. المؤسسات: تقوم بجمع ومعالجة بيانات الأفراد لعدة أسباب، منها: إضافة المتعاملين مع موقعها الإلكتروني لقوائمها البريدية، تحسين تجربة المتعامل مع الموقع، وغيرها.

- الجهة التي تقوم بمعالجة البيانات: هي الشخص الطبيعي أو المعنوي الذي يحلل ويعالج البيانات بالنيابة عن الجهة المتحكمة في البيانات.
- التصنيف: (Profiling) أي شكل من أشكال معالجة البيانات الشخصية، بصورة آلية بهدف تقييم حالة صاحب البيانات، بالتحديد لمعالجة أو توقّع أداء شخص معين في العمل أو حالته الاقتصادية أو اهتماماته أو سلوكه.
- اختراق البيانات الشخصية: يعني أيّ خرق لأمن المعلومات، الذي يؤدي إلى ضياع أو تغيير البيانات أو أي دخول أو اطّلاع على المعلومات بشكل غير قانوني.

ما هي العمليات التي تتمّ على البيانات في الفضاء الرقمي؟

هنالك العديد من العمليات التي تخضع لها البيانات الرقمية، ويمكن اختزالها بما يلي:

- الحصول على البيانات من صاحب البيانات: هي الحالة التي يقوم بها صاحب البيانات بتقديم بياناته طوعاً للجهة التي تتحكّم بها. مثال ذلك: عند قيام المستخدم بتزويد موقع إلكتروني معين باسمه الشخصيّ وعنوان بريده الإلكتروني بهدف الاشتراك بالقائمة البريدية الخاصة بالموقع.
- جمع البيانات: هي آلية الحصول على بيانات شخص أو جهة معينة إمّا من خلال طلب تلك البيانات من صاحبها، أو من خلال جمعها بشكل آلي وتلقائي.
- معالجة البيانات: هي عملية أو عمليات تتم على المعلومات الشخصية سواء تمّت بطرق آليّة أو بطرق عادية، وتشمل عمليات: جمع، تسجيل، تنظيم، هيكلة، تخزين، تغيير، استخدام، محو أو تعديل البيانات.

في أغلب الأحيان تكون الجهة المتحكمة بالبيانات هي ذاتها التي تعالج هذه البيانات، وفي أحيان أخرى تقوم الجهة المتحكمة بالبيانات بتعيين جهة لتقوم بالمعالجة. ويمكن أيضاً أن تكون ذات الجهة هي (الجهة المتحكمة) عند تعاملها مع بيانات محددة، والجهة المعالجة عند تعاملها مع بيانات أخرى.

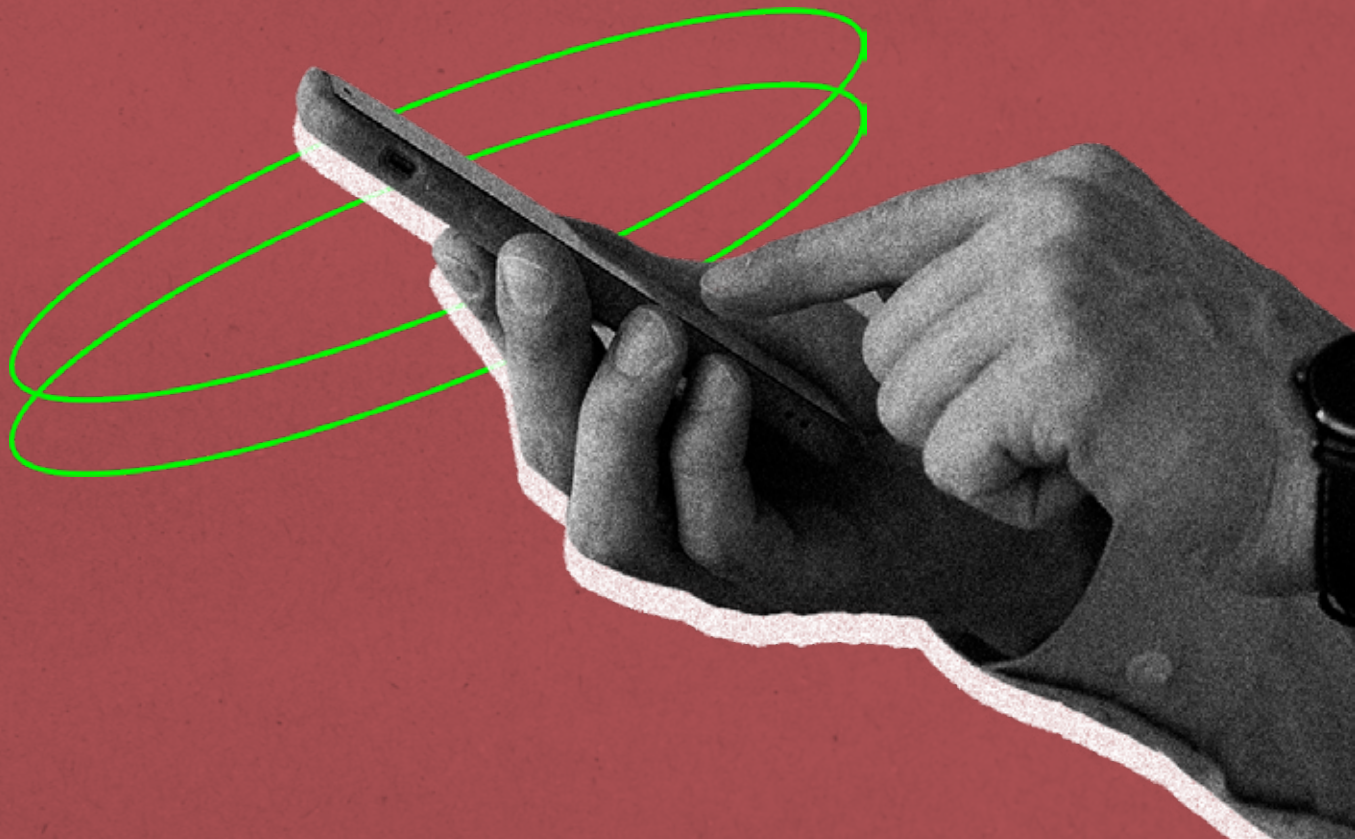
المبادئ الأساسية لجمع ومعالجة البيانات

وفقاً للمرجعيات المحلية والدولية يجدر بالعمليات التي تخضع لها البيانات أن تجري ضمن مجموعة من المبادئ الأساسية، وهي كالتالي:

- المشروعية والشّفافية والإنصاف: أي أن يتم جمع ومعالجة البيانات بطريقة مشروعة وعادلة وشفّافة لصالح صاحب البيانات.
بحيث يجب أن يكون صاحب البيانات على علم مؤكّد بأنّه يتمّ جمع معلوماته واستخدامها أو معالجتها. ويشمل الالتزام بهذا المبدأ أيضاً:

1. أن تكون جميع المعلومات المتعلّقة بعملية جمع البيانات معروضة بشكل يسهل الوصول إليها من قبل صاحب البيانات، ومكتوبة بشكل واضح باستخدام لغة بسيطة يفهمها الشخص العادي.
2. أن يتم إعلام صاحب البيانات بتداعيات ومخاطر عملية جمع البيانات وبحقوقه المتعلقة بهذه العملية.
3. أن تكون المعلومات الموجهة للعامة أو لصاحب البيانات مختصرة، ويسهل الوصول إليها ويسهل فهمها وتتمّ صياغتها بلغة مبسّطة وواضحة، وأن يتمَّ استخدام الصّور أو الرسومات عندما يكون هناك حاجة لها، خاصّة في الحالات التي يكون فيها أكثر من جهة وأكثر من تقنية، وبصورة يصعب على صاحب البيانات معرفة الجهة التي ستقوم بجمع البيانات، والغاية من ذلك الجمع (في حالة الإعلانات مثلاً).

- توضيح الهدف من عملية جمع ومعالجة البيانات: توضيح الهدف المحدّد والمشروع من جمع ومعالجة البيانات، وعدم استخدام هذه البيانات بشكل لا يتوافق مع ذلك الهدف. هذا، ولا تعدّ أرشفة البيانات، التي تهدف لتحقيق مصلحة عامة محددة وواضحة، أو الأهداف البحثية أو العلمية أو الاحصائية المحددة متعارضة مع هذا المبدأ شريطة عدم التعسف في استخدام السلطة تحت مسوّغ المصلحة العامة.
- جمع و معالجة الحد الأدنى من البيانات: أي جمع ومعالجة البيانات بالحدّ الأدنى الضروري واللازم لتحقيق الهدف المشروع والمحدّد مسبقاً، كما ويجب أن يتمّ اللجوء لعملية جمع البيانات فقط في حال لم يكن تحقيق الهدف ممكناً بطرق أخرى، دون جمع البيانات. أيضاً يجب التأكد من أن مدة حفظ البيانات هي مدة معقولة لتحقيق الهدف الموضح مسبقاً لصاحب البيانات، وألّا تتجاوز مدة حفظ البيانات الفترة اللازمة لتحقيق الهدف.
- تحرّي الدّقة عند التعامل مع البيانات: ويشمل ذلك وضع خطوات وحلول تقنية تضمن حفظ البيانات وتحديثها، ووضع معايير تضمن محو وتعديل أيّ معلومة غير دقيقة. كذلك التأكّد من اتخاذ الخطوات التي تضمن حماية هذه البيانات وسرّيتها، ومنع أيّ اختراق أو استعمال غير قانوني لها.



الأسس القانونية لعملية جمع ومعالجة البيانات

تعدّ النّقاط التالية أبرز الأسس التي يجدر تضمينها في أيّة تشريعات، تنظّم عملية جمع ومعالجة البيانات:

- وجود نص قانوني يسمح أو يفرض عملية جمع ومعالجة البيانات، بحيث يتمّ:
  1. جمع ومعالجة البيانات بناءً على نص قانوني يسمح بجمعها، على شرط أن يكون النص واضحاً ودقيقاً، وأن يكون تطبيقه واضحاً للأشخاص الخاضعين له.
  2. جمع ومعالجة البيانات عند وجود التزام قانوني مفروض على الجهة المتحكمة في البيانات، بحيث تتعلّق عملية جمع البيانات بالمصلحة العامّة أو بتنفيذ السلطات العامة لأعمالها، شريطة ألا تستخدم المصلحة العامة مسوّغاً لإساءة استخدام السلطة[4] .

- معالجة البيانات في الحالات الخطيرة، التي يمكن أن تؤثّر على حياة الإنسان.

تعدّ معالجة البيانات مبررة عندما يتم ذلك بهدف حماية حياة صاحب البيانات أو أي شخص آخر. ويتم اللجوء إلى هذا المبرر في حالات ضيّقة جداً، وحصراً عندما لا يكون اللجوء لمبرر آخر خياراً ممكناً. على سبيل المثال، عندما تكون عملية جمع البيانات مهمة لأغراض إنسانية، مثل تتبع الأوبئة وانتشارها، أو في الحالات الإنسانية الطارئة، خاصة في حالات الكوارث البيئية، أو التي صنعها الإنسان، ويرتبط هذا المبرر بالجهات الحكومية، التي يصب اختصاصها في حماية الأمن العام والمصلحة العامة، شريطة ألّا يتم الاعتماد على هذا المبرر كمسوّغ للتّعسف في استخدام الحق في جمع ومعالجة البيانات.

- معالجة البيانات عند وجود مصلحة مشروعة (legitimate interest).

يمكن اللجوء لمعالجة البيانات لتحقيق هدف قانوني ومبرر من قبل الجهة المتحكمة في البيانات، أو أي جهة أخرى، بشرط ألا يتضارب جمع البيانات هذا مع أيٍّ من حقوق الإنسان وحرياته الأساسية والأسس القانونية النافذة، وبشرط حماية هذه البيانات، ومثال ذلك:

1. في حالات منع الفساد.
2. لحماية أمن الشبكة.
3. لتحديد أفعال جرمية أو تهديد جرمي يهدّد الأمن العام، وفي هذه الحالة يجب أن يصدر قرار المعالجة عن جهة محايدة.

- معالجة البيانات لغاية تنفيذ عقد.

تعدّ عملية معالجة البيانات قانونية في الحالات الضرورية التي تتعلق بتنفيذ عقد، يكون صاحب البيانات أحد أطرافه، أو من أجل الدخول في عقد تمّت الموافقة عليه من قبل صاحب البيانات.

- معالجة البيانات بناء على موافقة صاحب البيانات على عملية جمع المعلومات

وتعدّ هذه الحالة هي الأكثر شيوعاً، ويتم في الغالب اللجوء إليها عند معالجة بيانات الأفراد.

4 في القانون الفلسطيني وبموجب المادة (31) قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية يتوجب على مزود الخدمة، الذي يعرف على أنه أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أي خدمة إلكترونية أو مستخدمي هذه الخدمة، أن يزود الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة. كذلك يجب عليه الاحتفاظ بكافة المعلومات المتعلقة بالمشترك لمدة لا تقل عن ثلاث سنوات. تشمل هذه المعلومات: المعلومات الموجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات حول نوع خدمة الاتصالات المستخدمة، والشروط الفنية، وفترة الخدمة، وهوية المشترك، وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة، وأي معلومات آخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة. كذلك وبنص الفقرة الأولى من المادة (33) يحق للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعمليها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية.

تعريف الموافقة

تعني الإشارة الصريحة الطوعية والمحددة والمبنية على معلومات واضحة وصادرة عن صاحب البيانات، وتتمثل في بيان صريح أو أي إجراء إيجابي ومؤكد، يؤدي إلى الدخول في اتفاقية جمع ومعالجة البيانات الشخصية الخاصة بصاحب البيانات.

شروط الموافقة الصّحيحة

1 **أن تتمثّل الموافقة بتصرّف إيجابي صريح: يعني ذلك أنّه لا يجوز افتراض الموافقة الضمنية، ويجب أن يقوم صاحب البيانات باتّخاذ خطوة إيجابية، تؤكد على موافقته على جمع ومعالجة بياناته، مثال ذلك:**

- إقرار الموافقة ببيان مكتوب بما يشمل الكتابة الإلكترونية.
- أو الموافقة الشفوية.
- أو وضع إشارة تأكيد عند دخول موقع إلكتروني معين أو اختيار (الموافقة على) تقنيات معينة تسمح بجمع البيانات أو أي تصرف أو بيان آخر يدلّ على الموافقة على خيار جمع ومعالجة البيانات المقترح.
- يجب أن تتمثل الموافقة دائماً بالقيام بفعل أو حركة معينة، ولا يعتدّ بالموافقة الصامتة، أو الّتي لا تتطلّب أيّ فعل (مثل الصناديق الموافق عليها أصلاً من قبل الموقع) (pre-ticked boxes) موافقة صحيحة.
- بالنسبة للأطفال تحت سن السادسة عشرة، فتتطلب عملية جمع البيانات موافقة إضافية أخرى من قبل الوصيّ عليهم، ويستثنى من هذا الالتزام الشركات التي تقدّم الخدمات للكبار فقط، وغير موجهة للأطفال بأي شكل من الأشكال.
- ليس هناك شكل محدد للموافقة، لكن يفضل دائماً أن تكون الموافقة مكتوبة لكي تتمكن الجهة التي تجمع وتتحكم في البيانات من الرجوع إليها وإثبات وجودها.

2. **أن تكون الموافقة طوعية: وتعني أن صاحب البيانات اتّخذ قرار السماح بمعالجة بياناته عن اقتناع وبناء على رغبته، مع عدم وجود أي عنصر ضغط أو تأثير غير مناسب قد يؤثر على قراره.**

- عند تقييم طوعية قرار الموافقة على جمع ومعالجة البيانات، فإنه يتم النظر إلى ما إذا كان تنفيذ عقد معين أو تقديم خدمة معينة، مشروطاً بالموافقة على عملية معالجة معلومات شخصية غير ضرورية لتنفيذ ذلك العقد. (وفي هذه الحالة تعدّ الموافقة غير طوعيّة).
- في حال تم طلب الموافقة على عملية جمع البيانات، في سياق كتابي (أي وثيقة مكتوبة غير متعلقة بجمع البيانات بشكل مباشر) يجب طلب الموافقة على جمع البيانات بشكل واضح ومنفصل عن المسائل الأخرى، وبلغة بسيطة يسهل على صاحب البيانات فهمها.
- إذا تم طلب الموافقة على عملية جمع البيانات بشكل إلكتروني، فيجب أن يكون الطلب واضحاً ومختصراً ولا يؤثر بشكل غير ضروري على الحصول على الخدمة المقدمة.
- لا يعتدّ بالموافقة إذا لم يكن لصاحب البيانات الخيار الحرّ أو في حال لم يكن قادراً على رفض أو سحب موافقته دون التّعرّض لضرر.

3. **أن تكون الموافقة مبنية على معلومات واضحة:**

يجب أن تجيب البيانات المقدمة لصاحب البيانات عن الأسئلة التالية:

- **(من)،** هوية الجهة التي ستقوم بجمع البيانات.
- **(ماذا)،** ما هي البيانات التي سيتم جمعها.
- **(لماذا)،** أي لأي غرض سيتم استعمال البيانات.

4. **أن تكون الموافقة محددة لأهداف مشروعة معينة:**

- يجب أن تكون الموافقة محددة، وتشمل أهدافًا معينة وواضحة ومشروحة بشكل كافٍ لصاحب البيانات، و تنحصر صلاحية الجهة التي تقوم بالجمع والتحكم بالبيانات في حدود الأهداف التي تم منح الموافقة عليها.
- عندما تتمّ عملية جمع البيانات لأكثر من هدف، فيجب الحصول على موافقة صاحب البيانات عن كل هدف بحد ذاته.

أما بالنسبة لعبء إثبات قانونية الموافقة فعندما تكون عملية معالجة البيانات مبنية على موافقة صاحب البيانات، فإنه يجب على الجهة التي تقوم بهذه العملية أن تكون قادرة على إثبات صحة موافقة صاحب البيانات، ويجب على الجهة أن تقوم بإثبات ذلك بطريقة مكتوبة بما يشمل:

- أن صاحب البيانات كان يعلم بكافة الحيثيات المرتبطة بموافقته.
- الموافقة الصريحة لصاحب البيانات على وثيقة سياسة خصوصية واضحة ومفهومة، بحيث يجب أن تكون صياغة هذه الوثيقة واضحة ذات لغة بسيطة ويسهل الوصول إليها، بالإضافة إلى عدم احتوائها على أي بنود مجحفة.

حقوق صاحب البيانات

يتمتّع صاحب البيانات بزمرة من الحقوق التي نتطرّق إليها أدناه:

1. **حق الوصول إلى البيانات الخاصة به.**

يحق لصاحب البيانات أن يطلب تأكيدًا من الجهة المتحكِّمة بالبيانات عمّا إذا كان هناك أي عملية معالجة لبياناته، وفي حال كانت تتم معالجة بياناته، فإنه يحق له الوصول إليها والحصول على نسخة منها، بالإضافة إلى معرفة المعلومات التالية:

- الهدف من معالجة البيانات.
- فئات البيانات التي تتم معالجتها.
- الجهات أو الفئات التي سيتم تمكينها من الاطلاع على البيانات أو التي اطلعت عليها.
- الفترة المتوقعة لحفظ البيانات، وفي حال لم يكن ذلك ممكناً، فيجب تحديد المعايير التي سيتم تحديد المدة بناء عليها.
- طلب تعديل أو حذف البيانات، وكذلك الحق في تقييد معالجة البيانات والحق في الاعتراض على تلك المعالجة.
- الحق في تقديم شكوى لدى الجهات الرسمية المختصة.
- عند جمع المعلومات من مصدر آخر غير صاحب البيانات، يجب إضافة معلومات حول مصدر هذه البيانات.
- وجود إجراءات آلية لمعالجة البيانات.

2. **حق تصحيح وتعديل بياناته.**

لصاحب البيانات الحق في تصحيح وتعديل البيانات الخاصة به. كما ويحق له إكمال تلك البيانات، ويشمل ذلك حقه بتقديم بيان تكميلي يحتوي على البيانات الناقصة وذلك مع الأخذ بعين الاعتبار الهدف من معالجة البيانات.

3. **حق حذف البيانات الخاصة به. (أو الحق في النسيان)**

- يحق لصاحب البيانات حذف جميع البيانات المتعلقة به من دون أي تأخير، ويجب على الجهة التي تتحكم بالبيانات أن تقوم بحذف تلك البيانات عند وجود أحد المبررات التالية:

- قيام صاحب البيانات بسحب موافقته، مع عدم وجود أي سبب قانوني آخر لمعالجة هذه البيانات.
- لم تعد البيانات الشخصية المجمعة ضرورية لتحقيق الهدف، الذي جمعت أو حللت أو عولجت من أجل تحقيقه.
- قيام صاحب البيانات بسحب موافقته، مع عدم وجود أي سبب قانوني آخر لمعالجة هذه البيانات.
- اعتراض صاحب البيانات على عملية معالجة بياناته.
- عند معالجة البيانات بطريقة غير قانونية.
- تنفيذاً لنص قانوني ملزم.

* في حال تمت إتاحة البيانات الشخصية لصاحب بيانات معين للعامة، وقام صاحب البيانات بتقديم طلب حذف البيانات، فإنه يجب على الجهة التي قامت بمعالجة البيانات أن تتخذ كافة الخطوات المعقولة، التي تشمل أي إجراءات تقنية لإعلام أي جهة تحكم أو معالجة أخرى تتحكم في تلك البيانات، بوجود طلب لحذف هذه البيانات، وأنه بناء عليه يجب مسح أي روابط أو نسخ أو تكرار لتلك البيانات الشخصية.

* لا يمكن تطبيق هذا الحق وحذف البيانات في حال كانت معالجتها ضرورية للأسباب التالية:
  - ممارسة الحق في حرية الرأي والحصول على المعلومات.
  - لأغراض تتعلق بالصحة العامة، مثلًا لأغراض منع انتشار الأوبئة.
  - لأغراض الأرشفة لصالح المصلحة العامة أو الأبحاث العلمية أو التاريخية.
  - لصياغة الادعاءات القانونية و/أو ممارسة الحق في الدفاع القانوني.

4. حق تقييد معالجة البيانات

* يحق لصاحب البيانات تقييد عملية معالجة البيانات، في الحالات التالية:
  - في حالة الاعتراض على مدى دقة البيانات من قبل صاحبها، خلال فترة تسمح للجهة التي تتحكم بها بالتأكد من صحتها.
  - عندما تكون عملية معالجة البيانات غير قانونية، ويطلب صاحب البيانات وقف استخدامها بدل محوها.
  - عدم حاجة الجهة التي تتحكم بالبيانات لها.
  - قيام صاحب البيانات بالاعتراض على معالجتها، ومع الأخذ بعين الاعتبار أن الأسباب التي يقدمها صاحب البيانات تطغى على أي مبرر قانوني آخر لدى الجهة التي قامت بجمع ومعالجة البيانات.

* عندما يتم وقف معالجة البيانات، يمنع استخدام هذه البيانات، ولا يسمح بمعالجتها إلا بموافقة صاحبها أو لأغراض صياغة ادعاءات قانونية و/أو ممارسة الحق في الدفاع القانوني، أو لحماية حقوق أشخاص آخرين طبيعيين أو معنويين أو لأسباب متعلقة بالمصلحة العامة.

* يجب إبلاغ صاحب البيانات، التي تم وقف معالجة بياناته، باستئناف عملية المعالجة من قبل الجهة المتحكمة قبل رفع هذا التقييد.

5. حق نقل البيانات من جهة تحكم إلى أخرى

* لصاحب البيانات الحق في الحصول على البيانات المتعلقة به، بطريقة وبشكل منظم يلائم الاستخدام الشائع، الذي تسهل قراءته بشكل آلي، ولديه الحق في نقل هذه البيانات لجهة أخرى، تقوم بالتحكم في البيانات، ودون أي تعطيل في حال استيفاء الشروط التالية:
  - تمت معالجة البيانات بناءً على موافقة المستخدم، أو بناءً على عقد معين.
  - تتم معالجة البيانات بشكل آلي من قبل الجهة التي قامت بجمعها.

* عند استخدام صاحب البيانات لهذا الحق، فله أن يطلب من الجهة التي تتحكم بالبيانات أن تقوم بإرسالها بشكل مباشر إلى الجهة المتحكمة الأخرى، في حال كان ذلك ممكنًا تقنيًا.

* لا يمكن استخدام هذا الحق إذا كانت عملية معالجة البيانات ضرورية لإتمام مهمة ضرورية لصالح المصلحة العامة، أو عند قيام الجهة المتحكمة بالبيانات بمعالجتها، بالنيابة عن السلطات المختصة.

6. **الحق في الاعتراض**

* يحق لصاحب البيانات الاعتراض على معالجة بياناته في أي وقت، عندما يكون أساس عملية جمع تلك البيانات مبنيًّا على:
  - جمع البيانات ضروري لإتمام مهمة تنفذ لصالح المصلحة العامة، أو من قبل السلطات العامة.
  - أو إذا كانت المعالجة تستند على هدف مشروع ومثبت، تسعى لتحقيقه الجهة المتحكمة بالبيانات أو جهة ثالثة.
* في هذه الحالة، وعند تلقي الاعتراض يجب أن تتوقف الجهة المتحكمة عن معالجة هذه البيانات، إلا في حال أثبتت أنّ هناك سببًا قانونيًّا، يعلو على الحقوق والحريات الخاصة بصاحب البيانات، أو لممارسة الحق في الدفاع القانوني.
* عندما تتم معالجة البيانات لأسباب تتعلق بالتسويق بشكل مباشر، يحق لصاحب البيانات الاعتراض في أي وقت على معالجة بياناته.

7. **الحقّ في اتخاذ إجراءات قضائية ضد الجهة التي تقوم بجمع أو معالجة بياناته، وعلى حكومات المعنية بحسن حماية الحق بالخصوصية، تبني عقوبات رادعة، تتناسب مع حجم الضرر في حال تم انتهاك الحق في الخصوصية، في الفضاء الرقمي و/أو الفعلي.**

8. **الحق في الحصول على تعويض عند الضرر.**

ما هي الالتزامات المفروضة على الجهة المتحكّمة في البيانات ؟

فيما يلي أبرز الالتزامات الواجبة على الجهة المتحكّمة بالبيانات، التي يجدر الاستناد إليها، في التعامل مع البيانات الشخصية:

أولاً: تمكين صاحب البيانات من ممارسة حقوقه.

* يشمل ذلك أن تكون عملية الوصول للمعلومات بسيطة وسهلة، ولا تتطلب أي مجهود غير معقول من قبل صاحب البيانات، وعند تقديم صاحب البيانات طلبًا لممارسة أيّ حقّ من حقوقه:
  - يتوجب على الجهة المتحكّمة بالبيانات أن تطلعه على الإجراءات المتخذة، بناءً على طلبه، كما ويجب أن تقوم بالرّد على الطلب بالطريقة ذاتها، التي تم تقديم الطلب بها. فمثلا إذا قام صاحب البيانات بالطلب بطريقة إلكترونية يتوجب الرد عليه بذات الطريقة إلا إذا طلب صاحب البيانات غير ذلك.
  - إذا لم تتخذ الجهة المتحكمة في البيانات أي إجراء، بخصوص الطلب المقدم من قبل صاحب البيانات، يجب أن تعلمه بذلك خلال فترة معقولة.
  - يجب تقديم كل البيانات المتعلقة بالطلبات بشكل مجاني، إلا أنه يجوز للجهة المتحكمة في البيانات، وبعد إثبات تكرار الطلب بشكل مفرط (لأكثر من ثلاث مرات للطلب ذاته) طلب رسوم مقابل الرّد على تلك الطلبات أو رفض التعامل معها.
  - يمكن للجهة المتحكمة في البيانات أن تطلب من صاحب البيانات عند طلبه لممارسة أحد حقوقه، معلومات إضافية للتأكد من هويته كشخص طبيعي، في حال كان لها أي شكوك مبررة بخصوص هوية ذلك الشخص.

ثانياً: إبلاغ صاحب البيانات بالمعلومات اللازمة، حول عملية معالجة البيانات.

* عند القيام بعملية جمع البيانات، يجب على الجهة المتحكمة في البيانات، وفي الوقت الذي تجمع فيه البيانات أن تزود صاحب البيانات بالمعلومات التالية:
  - هوية الجهة التي تجمع المعلومات، وتفاصيل الاتصال الخاصة بها، واسم الشخص الممثل عنها (في حال كان ذلك مناسباً).

- اسم الشخص المسؤول عن حماية البيانات.
- أهداف جمع البيانات، والأساس القانوني الذي يتم الجمع بناء عليه.
- الأشخاص والجهات التي ستطلع على المعلومات.
- إذا كانت الحالة تنطبق، يجب إبلاغ الشخص بنية الجهة المتحكمة في البيانات بأن تنقل البيانات لدولة أخرى.

* يجب على الجهة التي تجمع البيانات –أيضاً- إبلاغ صاحب البيانات بالمعلومات التالية؛ للتأكد من الالتزام بمبدأ الشّفافية والإنصاف:
  - مدة تخزين البيانات، أو إذا لم يكن ذلك ممكناً، فيجب تحديد الأسس التي سيتم بناء عليها تحديد المدة المناسبة لحفظ البيانات.
  - إعلام صاحب البيانات بحقه في الاطلاع على بياناته وتعديلها أو محوها أو طلب تقييد أو وقف معالجة البيانات الشخصية، وحقه بالاعتراض على معالجة هذه البيانات، وحقّه في نقل بياناته.
  - حقّه بسحب موافقته على معالجة بياناته في أي وقت، وعدم تأثير ذلك على قانونية معالجة البيانات، التي تمّت قبل سحب الموافقة.
  - حقّه في تقديم شكوى لدى الجهات المختصّة.
  - في حال كان يجب تقديم البيانات للوفاء بالتزامات عقد معيّن، أو دخول عقد معين أو للالتزام بالقانون، يجب توضيح ذلك مع تبيان نتائج عدم الالتزام بتوفير هذه البيانات.
  - وجود قرارات يتم أخذها بصورة آلية، منها "التصنيف" (Profiling) ومعلومات حول المنطق المستخدم، وتبعات استخدام تلك الآليات.
* إذا كانت الجهة المتحكّمة في البيانات تنوي معالجة البيانات لهدف آخر إضافي للسبب الذي تمّ جمع البيانات بخصوصه، فإنه يجب عليها أن تبلّغ صاحب البيانات بذلك قبل البدء بمعالجة البيانات، مع تزويده بكافة المعلومات حول ذلك الهدف.

ثالثاً: الالتزام بقانونية معالجة البيانات.

* نظراً لطبيعة وهدف معالجة البيانات، ونظراً لوجود مخاطر كبيرة لذلك على حريات وحقوق الأفراد، فإنه يجب على الجهة المتحكمة في البيانات التأكد من اتّباع كافة الخطوات، التي تضمن أن عملية معالجة البيانات تمّت بما يتماشى مع القانون.
* في حال كان هناك جهتان مجتمعتان تقومان بعملية معالجة البيانات والتحكم بها، فإنه يجب عليهما تحديد مسؤولياتهما بما يتعلق بالالتزامات القانونية المرتبطة بهذه العملية.

إبلاغ السلطات والأفراد عن أي عملية اختراق للمعلومات

* على الجهة المتحكمة في البيانات، في حال حدوث أي اختراق للبيانات الشخصية، ودون أيّ تأخير أن تقوم عند علمها بحدوث الاختراق بإبلاغ السلطات المختصة، إلا في حال كان هذا الاختراق لا يؤدي إلى تهديد للحقوق والحريات الخاصة بالأفراد. هذا ويجب أن يتم التبليغ خلال 72 ساعة من وقت العلم بالخرق، وإذا تم التأخر عن ذلك يجب تحديد الأسباب الداعية لذلك، ويجب أن يشتمل البلاغ على:
  - وصف طبيعة الاختراق والفئات التي تعرضت له وعدد الأفراد التقريبي، وعدد الملفات الشخصية التي تم اختراقها.
  - اسم الشخص المسؤول عن إدارة أو حماية البيانات ومعلومات التواصل معه، أو أي نقطة تواصل أخرى، يمكن للأفراد الحصول على معلومات أخرى منها.
  - وصف النتائج المتوقّعة من هذا الاختراق.
  - وصف الخطوات التي تمّ اتخاذها أو التي سيتم اتّخاذها للتعامل مع هذا الاختراق، والإجراءات التي ستستخدم لتخفيف الضرر.

- في حال قد يؤدي ذلك الاختراق إلى أيّ تأثير على الحقوق والحرّيات الأساسية للأفراد، فإنه يجب على الجهة المتحكِّمة في البيانات إبلاغ صاحب البيانات بحدوث الاختراق دون أيّ تأخير، وبشكل يتيح لصاحب البيانات اتخاذ أي خطوات ضرورية احترازية. هذا ويجب أن يوضح البلاغ طبيعة الاختراق واقتراحات لصاحب البيانات عن كيفية تخفيف الضرر الناتج عن ذلك.

أيضا يجب أن يتم هذا التبليغ باستخدام لغة واضحة وبسيطة، وتحتوي على البيانات التالية، كحد أدنى:

- اسم المسؤول عن حماية البيانات ومعلومات التّواصل معه، أو أي نقطة تواصل أخرى، يتمكن الأفراد من خلالها الحصول على المعلومات.
- وصف النتائج المتوقعة من هذا الاختراق.
- وصف الخطوات التي تمّ اتخاذها، أو التي سيتمّ اتخاذها للتعامل مع هذا الاختراق، والإجراءات التي ستستخدم لتخفيف الضرر.

- لا يتوجب إبلاغ صاحب البيانات بحدوث الاختراق في الحالات التالية:

- في حال اتخذت الجهة المتحكمة في البيانات كافة خطوات وضمانات الحماية، وتم تطبيق هذه الخطوات على معلومات الشخص، التي تم اختراقها. مثال على تلك الخطوات: عدم السماح لأي شخص غير مسموح له الدخول إلى البيانات، عبر استخدام خاصية التشفير.
- في حال كان هناك خطوات للتأكد من عدم وجود أي تهديد لحقوق وحريات صاحب البيانات.
- في حال تطلب الإبلاغ خطوات معقدة وكبيرة، في هذه الحالة، يجب أن يكون هناك إعلان عام أو إجراء آخر، يضمن إبلاغ أصحاب البيانات بشكل عادل وفعال.

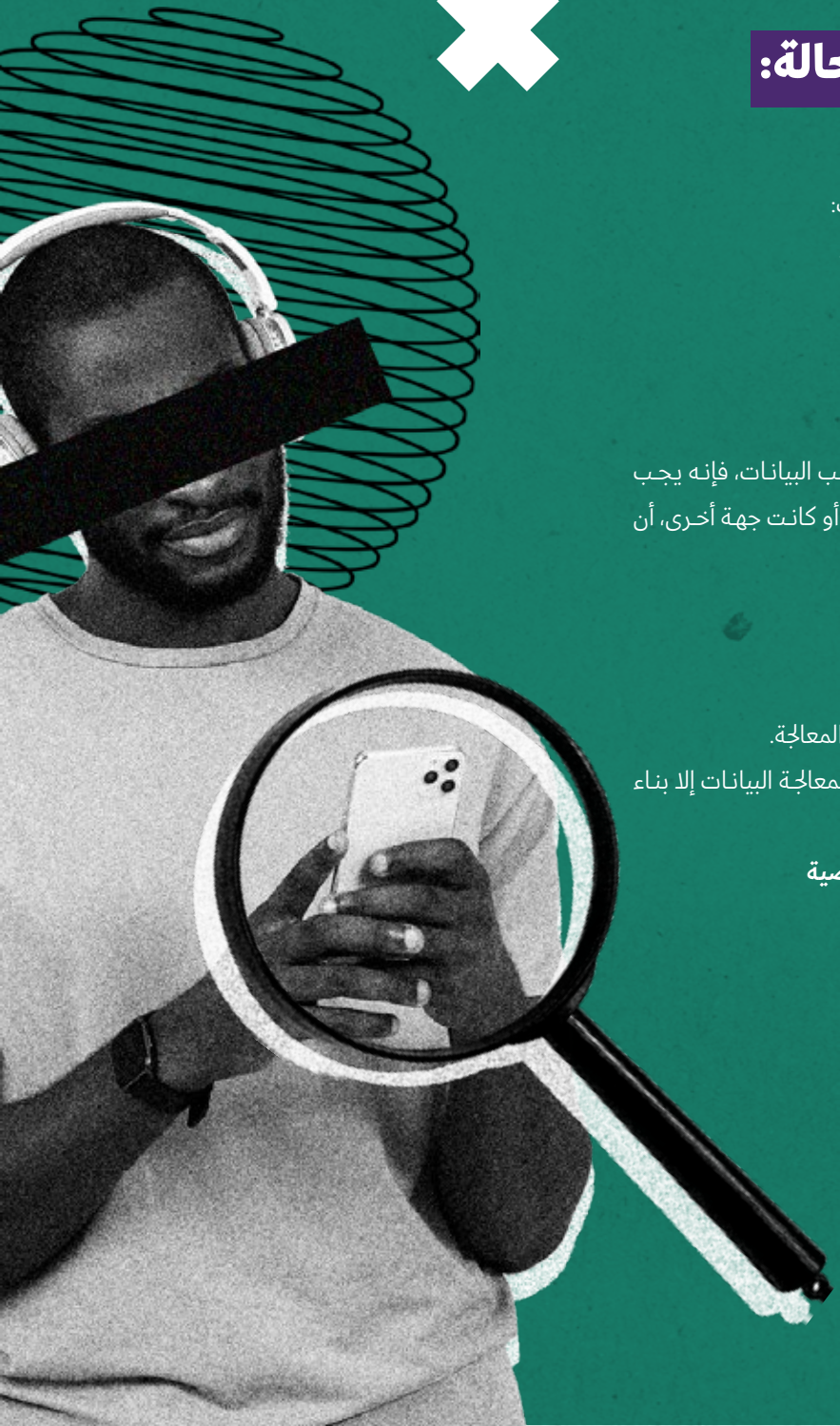
الاحتفاظ بسجلٍّ لعمليات معالجة البيانات:

ويجب أن يشمل هذا السجل:

- اسم وتفاصيل الاتصال الخاصة بالجهة المتحكمة بالبيانات. الهدف من معالجة البيانات، وصف لتصنيف البيانات، التي تتمّ معالجتها، وأصحاب تلك البيانات، والجهات التي ستتمكن من الاطلاع على البيانات، وعمليات نقل البيانات إلى بلاد أخرى، ومدة حفظ كل نوع من البيانات، ووصف عام للتدابير التنظيمية والتقنية الموضوعة لحفظ سرية المعلومات.

ما الذي يختلف عندما تُوكل الجهة المتحكِّمة بالبيانات، عملية معالجتها لجهة أخرى؟

- عند رغبة الجهة التي تتحكم بالبيانات بتوكيل عملية معالجتها إلى جهة أخرى، يجب على الجهة التي تتحكم بالبيانات أن تتعامل حصراً مع جهات معالجة، توفر ضمانات كافية لتطبيق المعايير التقنية والتنظيمية، التي تضمن أن عملية المعالجة ستتم بشكل يتوافق مع حقوق وحريات أصحاب البيانات.
- في حال تم الاتفاق على معالجة البيانات من قبل جهة أخرى، غير الجهة المتحكمة في البيانات، فإنه يجب تنظيم ذلك بعقد مكتوب، على أن ينظم العقد مدة العملية وطبيعتها والهدف منها، ونوع البيانات التي ستتم معالجتها وحقوق وواجبات الجهة التي تتحكم بالبيانات.
- يمنع على الجهة التي تقوم بعملية معالجة البيانات بأن تقوم بمعالجتها إلا وفق تعليمات الجهة التي تتحكّم بالبيانات.
- لا يمكن للجهة التي تعالج البيانات أن تشاركها مع جهة أخرى، دون إذن مسبق ومكتوب من الجهة المتحكِّمة في البيانات.



الالتزامات المفروضة على الجهة المعالجة للبيانات في هذه الحالة:

1. **إعداد كشف لجميع عمليات المعالجة:**

يجب على أي جهة تحلل البيانات أن تقوم بحفظ ملف أو أرشيف لعمليات معالجة البيانات، ويجب أن يشمل الكشف:

- اسم وتفاصيل الاتصال الخاصة بها وتفاصيل الاتصال الخاصة بالجهة المتحكّمة بالبيانات، التي تتبع لها وتمثّلها.
- أنواع البيانات التي تقوم بمعالجتها لكل جهة من الجهات المتحكّمة بالبيانات.
- في حال كان هناك نقل للبيانات بين الدول، فيجب ذكر ذلك مع تحديد الدولة أو الجهة.
- وصف عام للتدابير التنظيمية والتقنية الموضوعة لحفظ سرية المعلومات.

2. **الحفاظ على أمن وسرّية البيانات عند المعالجة:**

مع الأخذ بعين الاعتبار تكلفة وطبيعة ونطاق وهدف معالجة البيانات، ومدى تأثيرها على حرّيات وحقوق صاحب البيانات، فإنه يجب على الجهة التي تتحكم بالبيانات والجهة التي تعالج هذه البيانات، سواء كانت ذات الجهة التي تقوم بجمع البيانات أو كانت جهة أخرى، أن تتخذ إجراءات تقنية وتنظيمية، تضمن أمن البيانات، ومنها:

- الأسماء المستعارة وتشفير البيانات، وذلك لعدم استخدامها لتحديد شخص طبيعي معين.
- القدرة على ضمان سرية ونزاهة وقوة أنظمة وخدمات المعالجة.
- القدرة على استعادة البيانات في وقت مناسب في حال حدوث أي حادث تقني أو مادي يستدعي ذلك.
- ضمان وجود عملية اختبار منتظمة لتقييم واختبار فاعلية الضمانات التقنية والتنظيمية، المتعلّقة بأمان عملية المعالجة.

يجب أن تضمن الجهات، التي تتعامل مع البيانات أنّ كل شخص يتعامل مع البيانات تحت سلطتها، لا يقوم بمعالجة البيانات إلا بناء على تعليمات الجهة التي يعمل لديها.

3. **إبلاغ الجهة التي تتحكّم بالبيانات عند حدوث أي اختراق لها دون تأخير، فور العلم باختراق أي معلومات شخصية**

أمثلة عمليّة

تعدّ الأمثلة التّالية بعض السّيناريوهات الرّائجة لعمليات جمع البيانات والتحكم بها، التي يجدر في جميع هذه العمليات اتّباع معايير حقوق الإنسان والمعايير الدولية الفضلى، وبشكل خاص قواعد حماية البيانات الشخصية؛ وحقوق أصحاب هذه البيانات؛ وفقاً لما تمّ التّطرق له في هذا الدليل الإجرائي أعلاه.

المثال (1): الحكومة كجهة متحكِّمة ومعالجة للبيانات

عندما تقوم الحكومات، كما في الحالة الفلسطينية، بتقديم الخدمات للمواطنين/ات من خلال وزاراتها المختلفة، بما في ذلك عبر مقرّاتها ومواقعها الرّسمية عبر الإنترنت،كوزارة الداخلية، والخارجية، والاقتصاد، والعدل، والعمل وغيرها من الوزارات والجهات الرسمية؛ فإنها تطلب من المواطنين/ات بعض المعلومات الشّخصية، فمثلاً عند القيام بتسجيل شركة لدى وزارة الاقتصاد، يتمّ تزويد الوزارة بالعديد من البيانات، التي تشمل صور هويات الشركاء، وعناوينهم، والنظام الداخلي للشركة وغيرها من البيانات.

مثال (2) : البنك كجهة متحكِّمة ومعالجة للبيانات

عند القيام بتقديم طلب لفتح حساب بنكي، فإنّ البنك يطلب من المتقدم العديد من المعلومات والبيانات الشخصية. وعند فتح الحساب فإن البنك يكون على إطلاع وتحكم دائم في البيانات الحسابية الخاصة بالعميل. في مثل هذه الحالات يكون البنك جهة متحكِّمة في بيانات العملاء ومعالجة لها.

مثال (3) : الشركات كجهة متحكّمة ومعالجة للبيانات

تطلب بعض الشركات من الأفراد بيانات شخصية مختلفة، لغايات التحقّق من هوية العميل أو الزبون، و/أو تحسين جودة الخدمة، و/أو تحسين تجربة العميل و/أو لأغراض تسويقية مشروعة. مثال ذلك: شركات التأمين تطلب العديد من البيانات من عملائها لتحديد حزمة التأمين المناسبة لهم، كما وتطلب شركات الاتصالات وتزويد الخدمات العديد من البيانات الشخصية من الأفراد لتخصيص رقم اتصال لهم، وتزويدهم بالخدمات ذات العلاقة. في مثل هذه الحالات تكون الشركات جهة متحكمة في بيانات العملاء ومعالجة لها.

مثال (4): التطبيقات الذكية والمواقع الإلكترونية المختلفة

تستخدم الحكومة والمؤسسات والشركات المواقع الإلكترونية والتطبيقات الذكية لضمان سرعة وسهولة عملها. في حال تم جمع بيانات ومعالجتها سواء بشكل أوتوماتيكي أو غير أوتوماتيكي فإن الجهة المالكة و/أو المشغلة لهذه المواقع أو التطبيقات تكون جهة متحكِّمة في البيانات و/أو معالجة لها.

لذلك، يجب على كافة الجهات، التي تملك و/أو تشغل التطبيقات الذكية و/أو المواقع الإلكترونية أن تنشر على منصاتها المختلفة شروط استخدام وسياسة خصوصية؛ وذلك لضمان قانونية جمع ومعالجة وتخزين البيانات، التي تتحكم بها و/أو تعالجها.

حملة – المركز العربي
لتطوير الإعلام الاجتماعي

7amleh - The Arab Center for
the Advancement of Social Media