الإنتربول

دليل وابيس

برنامج منظومة المعلومات الشرطية لغرب أفريقيا

دليل أفضل الممارسات في مجال حماية البيانات الشخصية

حزيران/يونيو 2020

يموّل هذا البرنامج
من الاتحاد الأوروبي

أعد الفريق المعني ببرنامج وابيس دليل منظومة المعلومات الشرطية لغرب أفريقيا (’وابيس ’أو ’المنظومة‘) لأفضل الممارسات في مجال حماية البيانات الشخصية تحت إشراف مكتب الشؤون القانونية في الإنتربول وبفضل الإسهامات القيّمة للخبيرين في مجال حماية البيانات الشخصية، السيد Teki Akuetteh والدكتور Mouhamadou Lo.

يموّل هذا البرنامج
من الاتحاد الأوروبي

الجنرال
فرنسيس أ. بيهانزين

مفوض الشؤون السياسية والسلم
والأمن في الجماعة الاقتصادية
لدول غرب أفريقيا

مقدمة

في سياق سعينا إلى دخول مرحلة هامة (تبادل المعلومات الجنائية) ترمي إلى تحسين إدارة مكافحة الجريمة المنظمة بشكل عام والإرهاب بشكل خاص في غرب أفريقيا، لا يسعنا سوى إبداء شديد امتناننا للمنظمة الدولية للشرطة الجنائية (الإنتربول) التي، بفضل خبرتها العريقة التي تشارف على المائة عام (2020 - 1923) في مجال التحقيقات الشرطية، تضع في متناول الدول الأعضاء الـ 15 في الجماعة الاقتصادية لدول غرب أفريقيا وموريتانيا «منظومة المعلومات الشرطية لغرب أفريقيا» (وابيس) الممولة من الاتحاد الأوروبي. غير أن تنفيذ برنامج وابيس، الذي وُضع أصلا للمساعدة على كشف الجرائم الجنائية وجمع الأدلة المتصلة بها والبحث عن مرتكبيها وشركائهم المحتملين من أجل مكافحة الجريمة المنظمة والإرهاب، يؤدي بشكل غير مباشر إلى معاملة بيانات شخصية ويشتمل أيضا على إمكان تسجيل البيانات المتعلقة بالشهود والضحايا إذا اقتضى التحقيق ذلك. وللمضي قدما بهذا المشروع الهام للجماعة الاقتصادية، سيتعين على أجهزة إنفاذ القانون (الشرطة، والدرك، والجمارك، والهجرة، والمياه والغابات، وغيرها من الأجهزة المماثلة) تبادل المعلومات الحساسة عن الأشخاص والممتلكات بغية تحقيق الهدف النهائي المتمثل في ضمان أمن الأشخاص والممتلكات في منطقة الجماعة الاقتصادية لدول غرب أفريقيا وفي القارة الأفريقية وأوروبا والعالم أجمع. ويعني ذلك بالنسبة للأجهزة المذكورة تبادل البيانات الشخصية، أي جميع المعلومات المتعلقة بشخص طبيعي حُدِّدت هويته أو يمكن تحديدها، بشكل مباشر أو غير مباشر، استنادا إلى رقم تعريف أو إلى عنصر أو أكثر من عناصر المعلومات الخاصة به.

وفي غرب أفريقيا، يحمي هذه البيانات القانون الإضافي A/SA.1/01/10 المتعلق بحماية البيانات الشخصية في الجماعة الاقتصادية لدول غرب أفريقيا، الذي اعتُمد في 16 شباط/فبراير 2010 لحماية المواطنين في دول الجماعة الاقتصادية من أيّ إساءة استخدام لبياناتهم الشخصية ومعاملتها. لذا، حدد القانون الإضافي المبادئ الأساسية التي تحكم معاملة البيانات الشخصية ويحث الدول الأعضاء في الجماعة الاقتصادية على سن قوانين لحماية هذ النوع من البيانات وإنشاء هيئات حماية مناسبة لها، أي هيئات مكلفة بتطبيق قانون حماية البيانات الشخصية.

لمَ حماية البيانات الشخصية؟

حماية البيانات الشخصية هي حماية الخصوصية والكرامة وسائر حقوق الفرد الأساسية مثل الحق في احترام الحياة الخاصة، والحق في الصورة، والحق في صون الشرف، وغير ذلك.

وفي هذا السياق، وبهدف مساعدة أجهزة إنفاذ القانون على معاملة البيانات الشخصية في منظومة وابيس بما يتفق مع القانون الإضافي وسائر القوانين والأنظمة السارية في البلدان المعنية والمعايير الدولية المتعلقة بحماية البيانات، أُعدَّ هذا الدليل لأفضل الممارسات في مجال حماية البيانات الشخصية.

وهذا الدليل، الذي أعده برنامج وابيس ووافق عليه ممثلو البلدان المشاركة في هذا البرنامج خلال لقاءات تنسيق القوانين التي عقدتها لجنة خبراء الجماعة الاقتصادية لدول غرب أفريقيا في الفترة من 22 إلى 24 تشرين الأول/أكتوبر 2019، يستند إلى الممارسات الجيدة المعمول بها على الصعيدين الوطني والدولي وفقا لأحكام القانون الإضافي والتشريعات السارية في البلدان المشاركة في البرنامج. ويُرمى من دليل أفضل الممارسات هذا، وإن لم يكن ملزما، إلى أن يقوم مقام أداة توجيهية تهدف إلى تسهيل فهم المعايير السارية والمبادئ التوجيهية التي تحكم جمع البيانات الشخصية ومعاملتها وتبادلها وحفظها في إطار برنامج وابيس.

وتطبيق أجهزة إنفاذ القانون إرشادات هذا الدليل بشكل مناسب سيتيح للبلدان المشاركة في البرنامج اعتماد أفضل الممارسات التي ستيسّر تبادل المعلومات وتعزز استخدام منظومة وابيس إلى أقصى حد مع الحفاظ على التوازن اللازم بين فعالية منظومة لإنفاذ القانون وبين احترام الحقوق والحريات الأساسية الواجبة لكل فرد.

وإني أهيب بالبلدان المشاركة في برنامج وابيس إلى الاستفادة إلى أقصى حد من هذا الدليل على الصعيد المهني لتعزيز قدراتها على مكافحة الجريمة المنظمة والإرهاب من خلال تبادل معلومات جيدة النوعية.

الجنرال فرنسيس أ. بيهانزين

مفوض الشؤون السياسية والسلم والأمن في الجماعة الاقتصادية لدول غرب أفريقيا

المحتويات

مقدمة

ما هو دليل وابيس لأفضل الممارسات في مجال حماية البيانات الشخصية؟

إن الغرض من دليل منظومة المعلومات الشرطية لغرب أفريقيا ('وابيس 'أو 'المنظومة') لأفضل الممارسات في مجال حماية البيانات الشخصية هو مساعدة أجهزة إنفاذ القانون على معاملة البيانات في منظومة وابيس بما يتفق مع قانون 'Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS' ('القانون الإضافي') وسائر القوانين واللوائح القانونية السارية والمعايير الدولية وأفضل الممارسات المعتمدة في معاملة البيانات الشخصية.

ودليل أفضل الممارسات مخصص لكل أجهزة إنفاذ القانون والهيئات التي تعامل البيانات الشخصية عبر منظومة وابيس. وهو يوفر إرشادات بشأن كيفية حماية البيانات الشخصية عند معاملتها عبر هذه المنظومة. ويهدف إلى تسهيل فهم أجهزة إنفاذ القانون في البلدان المشاركة في منظومة وابيس للقوانين الحالية والمبادئ التوجيهية المتعلقة بإنفاذ القانون التي تسري على معاملة البيانات.

ولا يعفي هذا الدليل البلدان الأعضاء في الجماعة الاقتصادية لدول غرب أفريقيا مما عليها من واجبات بمقتضى القانون الإضافي، ولا سيما من حيث اعتماد تشريعات وطنية وإنشاء هيئة لحماية البيانات.

والدليل هو كناية عن أداة توجيهية لحماية البيانات استُحدثت خصيصا للبلدان المشاركة في منظومة وابيس لكفالة اتباعها أفضل الممارسات عند جمع البيانات الشخصية ومعاملتها وتوفيرها واستخدامها في هذه المنظومة. وهو يمثل مرجعا لأفضل الممارسات الوطنية والدولية التي تتفق مع القانون الإضافي الذي اعتمدته الجماعة الاقتصادية لدول غرب أفريقيا، وللبلدان المستفيدة التي لديها قوانين لحماية البيانات. وهو يحدد المبادئ والاستثناءات والحقوق الأساسية المتعلقة بحماية البيانات ويتضمن في الوقت نفسه هيكليات لإدارتها والتقيد بها لتيسير تنفيذها.

الغرض من دليل وابيس لأفضل الممارسات

إن وابيس منظومة إلكترونية للمعلومات الشرطية تعمل على الصُعد الوطني والإقليمي والدولي. والغرض العام منها هو زيادة قدرة أجهزة إنفاذ القانون في غرب أفريقيا على مكافحة الجريمة عبر الوطنية والإرهاب من خلال تحسين مستوى إدارة المعلومات وتبادلها. وتحتوي المنظومة على معلومات من أجهزة إنفاذ القانون تتعلق، على سبيل الذكر لا الحصر، بما يلي:

a. أشخاص (مثل المشتبه فيهم والشهود والضحايا)؛
b. وسائل نقل (مثل السيارات)؛
c. مستندات (مثل جوازات السفر ورخص القيادة وبطاقات الهوية الوطنية وغيرها)؛
d. أسلحة؛
e. أماكن؛
f. أحداث؛
g. أشياء عامة (تشمل أشياء غير مدرجة ضمن هذه الفئات المحددة – كالأشياء التي يُعثر عليها في مسرح جريمة ما، على سبيل المثال).

ويقع بعض هذه البيانات في إطار تعريف "البيانات الشخصية" لأنه يمكن أن يؤدي - بشكل مباشر أو غير مباشر - إلى كشف هوية الأشخاص.

وعلى الصعيد الإقليمي، قامت الأطراف السامية المتعاقدة في الجماعة الاقتصادية لدول غرب أفريقيا، إدراكا منها للضرر المحتمل الذي يمكن أن تستتبعه معاملة البيانات الشخصية على الحقوق والحريات الأساسية للأشخاص موضوع البيانات، باعتماد القانون الإضافي في 16 شباط/ فبراير 2010. ويعرض هذا القانون المبادئ الأساسية التي تحكم معاملة البيانات الشخصية داخل هذه الجماعة الاقتصادية ويتطلب من بلدانها الأعضاء سن تشريعات لحماية البيانات وإنشاء هيئات تُعنى بحمايتها. وثمة تفاوت حاليا بين البلدان المشاركة في منظومة وابيس من حيث الوفاء بهذه المتطلبات الرئيسية.

وجاء هذا الدليل استجابة لطلب قُدم خلال الندوة القانونية للبلدان المشاركة في منظومة وابيس التي عقدتها في 19 آذار/ مارس 2019 مفوضية الجماعة الاقتصادية لدول غرب أفريقيا والإنتربول والاتحاد الأوروبي، وحضرتها الجهات المنسقة لمنظومة وابيس وخبراء قانونيون من البلدان الـ 16 المشاركة في هذه المنظومة. وفي ضوء القلق الذي أُبدي بشأن عدم وجود تشريعات لحماية البيانات وسلطات تُعنى بحمايتها في بعض البلدان المشاركة في منظومة وابيس، اقتُرح تقديم مسودة دليل "أفضل الممارسات" المتعلق بمعاملة البيانات الشخصية في منظومة وابيس إلى الجهات المنسقة للمنظومة والخبراء القانونيين خلال حلقة عمل قانونية مخصصة لهذه المسودة لكي ينظروا فيها. وقُدِّمت هذه المسودة خلال ندوة قانونية للمتابعة، عقدتها أيضا مفوضية الجماعة الاقتصادية لدول غرب أفريقيا والإنتربول والاتحاد الأوروبي في أبيدجان من 22 إلى 24 تشرين الأول/أكتوبر 2019، ووافق عليها المشاركون.

لمحة عامة عن دليل وابيس لأفضل الممارسات

ينقسم هذا الدليل إلى 12 فصلا.

يقدم الفصل الأول نظرة عامة عن المصطلحات المستخدمة في الدليل. وهو يعرّف خصوصا المصطلحات المتصلة بأبرز الهيئات المسؤولة عن حماية البيانات الشخصية في إطار الدليل (الفصل 1، الفقرتان 1 و2)، ومتلقّي البيانات الشخصية (الفصل 1، الفقرة 8)، والأشخاص الذين تعامَل بياناتهم الشخصية (الفصل 1، الفقرة 4)، ونوع المعلومات التي تُعتبر بيانات شخصية (الفصل 1، الفقرة 7).

ويعرض الفصل الثاني المبادئ العامة التي تحكم حماية البيانات الشخصية والأسباب المشروعة التي لدى أجهزة إنفاذ القانون لمعاملة هذه البيانات. وتوفر هذه المبادئ لهذه الأجهزة إيضاحات عامة لمختلف شروط معاملتها في منظومة وابيس. ومبادئ حماية البيانات الشخصية المعروضة تتصل بما يلي: (a) الموافقة والمشروعية؛ و(b) الشرعية والإنصاف؛ و(c) الغرض والملاءمة والحفظ؛ و(d) الدقة؛ و(e) الشفافية؛ و(f) السرية والأمن؛ و(g) اختيار معامِل البيانات. ولا ينبغي لأجهزة إنفاذ القانون معاملة البيانات في منظومة وابيس إلا لأغراض إنفاذ القانون المشروعة التالية: منع ارتكاب الجرائم أو التحقيق فيها أو الكشف عنها أو مقاضاة مرتكبيها، وتنفيذ العقوبات، وصون النظام العام، وحماية الأمن العام من الأخطار التي تتهدده ومنعها، ولأداء أجهزة إنفاذ القانون أي مهمة أو مسؤولية يمليها عليها القانون.

ويبحث الفصل الثالث دور هيئات حماية البيانات، وأهمية التدريب على كيفية حماية هذه البيانات، وأهمية إشراك أصحاب المصلحة الرئيسيين في تنفيذ إطار حماية البيانات. فأولا، ينبغي لجميع البلدان المشاركة في منظومة وابيس إنشاء هيئة مستقلة لحماية البيانات تكون مسؤولة عن عمليات معاملة البيانات. وثانيا، ينبغي لأجهزة إنفاذ القانون تعيين موظف معني بحماية البيانات ليقوم بما يلي: (a) إطلاع أجهزة إنفاذ القانون على واجباتها القانونية؛ و(b) التحقق من مدى التقيد بشروط معاملة البيانات؛ و(c) تقديم المشورة بشأن تقييم نتائج حماية البيانات؛ و(d) التنسيق مع هيئات حماية البيانات؛ و(e) تنظيم برنامج تدريب مناسب ودائم لمستخدمي منظومة وابيس. وثالثا، يتعين على أجهزة إنفاذ القانون دمج حماية البيانات في صلب هيكليات إدارتها عبر إشراك أصحاب المصلحة الرئيسيين في تنفيذ إطار حماية البيانات التي تعامَل في هذه المنظومة.

ويحدد الفصل الرابع أفضل الممارسات في مجال جمع البيانات الشخصية وتبادلها. وكقاعدة عامة، يجب أن تقتصر البيانات الشخصية التي تُجمع على ما يقتضيه تحقيق الغرض الذي تُجمع لأجله وألا تتجاوزه.

ويقدم الفصل الخامس لمحة عامة عن نوعية البيانات وعن التدابير التي ينبغي لأجهزة إنفاذ القانون تنفيذها لضمان الحفاظ على سرية البيانات الشخصية وأمنها. وكقاعدة عامة، لا ينبغي ألهذه الأجهزة إرسال بيانات شخصية غير دقيقة أو قديمة أو ناقصة. ويتعين على أجهزة إنفاذ القانون، إذا اتضح لها أنها أعطت بيانات شخصية غير دقيقة، الإسراع في إبلاغ متلقّيها بذلك واتخاذ الخطوات المناسبة لتصحيحها أو حذفها أو منع معاملتها. وينبغي لها أيضا اتخاذ التدابير المناسبة لتأمين المنظومة.

ويحدد الفصل السادس الخطوات المناسبة التي ينبغي اتخاذها عند انتهاك بيانات ما. ويتعين على أجهزة إنفاذ القانون توثيق حالات انتهاكها وإبلاغ الهيئة المختصة بحماية البيانات بها بدون تأخير لا لزوم له، ويفضل أن يكون ذلك ضمن مهلة 72 ساعة من وقت انتهاكها. ويتعين عليها كذلك إبلاغ الأشخاص موضوع البيانات بدون أي تأخير لا لزوم له بأن بياناتهم الشخصية قد انتُهكت إذا كان من المحتمل أن يؤدي هذا الانتهاك إلى مس حقوقهم وحرياتهم.

ويعرض الفصل السابع أفضل الممارسات في مجالي تجهيز السجلات والاحتفاظ بالبيانات. فيجب على أجهزة إنفاذ القانون امتلاك سجلات لجميع عمليات معاملة البيانات. ويجب عليها أيضا الاحتفاظ بسجلات لما يلي: (a) جمع البيانات؛ و(b) تغييرها؛ و(c) الوصول إليها/ الاطلاع عليها؛ و(d) الكشف عنها، بما في ذلك إحالتها؛ و(e) دمجها في إطار واحد؛ و(f) حذفها. ولا ينبغي لها الاحتفاظ بالبيانات إلا لفترة محددة.

ويشير الفصل الثامن إلى أن البيانات الحساسة أي [«البيانات الشخصية التي تذكر الانتماء العرقي أو الإثني أو الأصل الجغرافي أو النسب أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية النقابية أو الحياة الجنسية أو البيانات الوراثية أو بشكل أعم البيانات المتصلة بالحالة الصحية لأي شخص» (الفصل 8.1، الفقرة 1) لا يتعين معاملتها في منظومة وابيس إلا عند الضرورة القصوى.

ويسلط الفصل التاسع الضوء على حقوق الأشخاص موضوع البيانات، أي حق الاطلاع على بياناتهم أو تصحيحها أو حذفها. وحق الاطلاع على البيانات يجيز للشخص المعني الوصول المباشر أو غير المباشر إلى ما يتعلق به من بيانات موجودة في منظومة وابيس، بينما يجيز له حق تصحيحها أو حذفها الطلب من أجهزة إنفاذ القانون تصحيح بياناته الشخصية غير الدقيقة الموجودة في هذه المنظومة أو حذفها.

ويناقش الفصل العاشر تقييم نتائج حماية البيانات الذي يمكن استخدامه لمساعدة أجهزة إنفاذ القانون على تبيان وتسجيل المخاطر التي تنطوي عليها معاملة البيانات الشخصية في منظومة وابيس. وسيثبت هذا التقييم، إذا أُجري بحسب الأصول، أن هذه الأجهزة بحثت المخاطر التي تستتبعها معاملة البيانات المقررة.

ويذكر الفصل الحادي عشر الحالات التي لا ينبغي فيها معاملة البيانات وفقا لهذا الدليل.

ويلخص الفصل الثاني عشر الغرض الشامل من هذا الدليل ألا وهو تمكين البلدان المشاركة في منظومة وابيس من تبنّي ممارسات قانونية عند معاملة البيانات تسهّل إدارة المعلومات وتبادلها واستخدام هذه المنظومة العام إلى أقصى حد ممكن.

الفصل الأول

مصطلحات عامة

أغراض هذا الدليل، المقصود بـــ::

1. "المتحكم بالبيانات": أي شخص أو كيان أو هيئة أو جمعية، سواء من الحقل العام أو الحقل الخاص، يقرر بمفرده أو مع آخرين جمع بيانات شخصية ومعاملتها وتحديد الأغراض التي لأجلها تعامَل[1] .

2. "معامِل البيانات": أي شخص أو كيان أو هيئة أو جمعية، سواء من الحقل العام أو الحقل الخاص، يتولى معاملة بيانات نيابة عن المتحكم بالبيانات [2].

3. "هيئة حماية البيانات": الهيئة المستقلة المسؤولة عن كفالة التقيد بقواعد حماية البيانات، التي يشكلها بلد مشارك في منظومة وابيس وفقا للمادة 14 من القانون الإضافي (Supplementary Act) و/أو القوانين المحلية في البلد المشارك فيها.

4. "الشخص موضوع البيانات" الشخص الذي تتم معاملة بياناته الشخصية[3] .

5. انتهاك البيانات الشخصية": خرق لأمن البيانات الشخصية يؤدي بشكل غير مقصود أو غير قانوني إلى إتلاف البيانات الشخصية المحالة أو المخزنة أو المعاملة أو ضياعها أو تغييرها، أو الكشف عنها أو الاطلاع عليها بدون إذن[4] .

6. "معاملة البيانات الشخصية": كل عملية أو مجموعة من العمليات تجري على البيانات الشخصية سواء بوسائل مؤتمتة أو غيرها من الوسائل، مثل الحصول على بيانات الشخصية أو استخدامها أو تسجيلها أو تنظيمها أو الاحتفاظ بها أو تعديلها أو تغييرها أو استخراجها أو حفظها أو نسخها أو الاطلاع عليها أو استخدامها لغير أغراضها أو الكشف عنها عبر إحالتها أو نشرها أو توفيرها أو ترتيبها أو دمجها، فضلا عن منع الوصول إليها أو تشفيرها أو حذفها أو إتلافها [5] .

7. "البيانات الشخصية": أي معلومات تتعلق بشخص مُحدَّد يمكن كشف هويته بشكل

---

[1]. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

[2]. المرجع نفسه.

[3]. المرجع نفسه.

[4]. توجيه الاتحاد الأوروبي Directive (EU) 2016/680, 27 April 2016, Art. 3(11).

[5]. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

مباشر أو غير مباشر بالرجوع إلى رقم تعريف أو عنصر واحد أو عدة عناصر تتعلق بأوصافه الجسدية أو الفيزيولوجية أو الجينية أو النفسية أو الثقافية أو الاجتماعية أو الاقتصادية[6]

8. "الجهة المتلقّية": أي جهة تزوَّد ببيانات شخصية، بما يشمل الأشخاص الطبيعيين أو الاعتباريين أو الأجهزة العامة أو الأجهزة أو سائر الهيئات، سواء أكانت جهة ثالثة أم لم تكن[7].

9. "البيانات الحساسة": البيانات الشخصية المتعلقة بآراء أو أنشطة الشخص الدينية أو الفلسفية أو السياسية أو النقابية، أو بحياته الجنسية أو أصله الإثني أو وضعه الصحي، في إطار تدابير اجتماعية وإجراءات قضائية وعقوبات جنائية أو إدارية[8] .

10. "القانون الإضافي" يعني قانون ECOWAS Supplementary Act A/SA.1/01/10 المتعلق بحماية البيانات الصادر في 16 شباط/ فبراير 2010.

11. "البلد المشارك في منظومة وابيس": أي من البلدان التالية: بوركينا فاسو، جمهورية بنن، جمهورية توغو، جمهورية تشاد، جمهورية الرأس الأخضر، جمهورية السنغال، جمهورية سيراليون، جمهورية غامبيا، جمهورية غانا، جمهورية غينيا، جمهورية غينيا بيساو، جمهورية كوت ديفوار، جمهورية ليبريا، جمهورية مالي، جمهورية موريتانيا الإسلامية، جمهورية النيجر، جمهورية نيجيريا الاتحادية.

12. ("وابيس" (أو "المنظومة"): برنامج منظومة المعلومات الشرطية لغرب أفريقيا (وابيس) – وهي بمثابة منظومة إلكترونية للمعلومات الشرطية تعمل على الصُعد الوطني والإقليمي والدولي.

---

[6] المرجع نفسه.

[7]. توجيه الاتحاد الأوروبي(10) Directive (EU) 2016/680, 27 April 2016, Art. 3.

[8]. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

الفصل الثاني

المبادئ السارية على حماية البيانات الشخصية والغرض من معاملتها

2.1 المبادئ السارية

عند معاملة البيانات الشخصية في المنظومة، ينبغي أن تسترشد أجهزة إنفاذ القانون بالمبادئ أدناه المنصوص عليها في الفصل الخامس من القانون الإضافي 'Supplementary Act':

1. مبدأ الموافقة والمشروعية: لا بد أن تكون لدى أجهزة إنفاذ القانون أسباب مشروعة لمعاملة البيانات الشخصية، ويتعين خصوصا التأكد من أن معاملتها ضرورية، ومن هذه الأسباب ما يلي:
   b. الوفاء بواجب قانوني ملزم لأجهزة إنفاذ القانون؛
   c. تحقيق مصلحة عامة أو تنفيذ مهمة أخرى ضرورية لممارسة السلطة العامة المسندة إلى جهاز إنفاذ القانون.

ومعاملة البيانات الشخصية لأغراض إنفاذ القانون المنصوص عليها في الفقرة 2-2 أدناه لا تستلزم طلب موافقة الشخص موضوع هذه البيانات.

2. مبدأ الشرعية والإنصاف: يجب على أجهزة إنفاذ القانون معاملة البيانات الشخصية بطريقة قانونية ومنصفة وغير احتيالية. وكل معاملة يجب أن يجيزها القانون وأن تحترم الحقوق الأساسية للأشخاص موضوع البيانات، بما يتفق والواجبات السارية المتصلة باحترام حقوق الإنسان. والغرض الرئيسي من ذلك هو حماية مصالح الأشخاص الذين تعامَل بياناتهم الشخصية. وهذا الأمر ينطبق على كل معاملة للبيانات الشخصية في المنظومة. ومن المهم الإدراك أن معاملة البيانات الشخصية لفرد ما لا تغدو بشكل تلقائي غير منصفة أو غير منطقية أو غير قانونية لأن لها أثرا سلبيا على هذا الفرد. والقرار يستند إلى ما إذا كان الأثر السلبي مبررا من الناحية القانونية للكشف عن جريمة ومنعها ولأغراض أخرى ذات صلة بإنفاذ القانون. ويعني ذلك من الناحية العملية أن أجهزة إنفاذ القانون ينبغي:
   a. أن تكون لديها أسباب مشروعة لجمع البيانات الشخصية واستخدامها ومعاملتها في المنظومة؛
   b. الامتناع عن استخدام المعلومات أو البيانات بطرق تستتبع آثارا ضارة غير مبررة على الأشخاص المعنيين؛
   c. أن تكون شفافة من حيث الطريقة التي تعتزم بها استخدام البيانات وأن توفر الإشعارات المناسبة بشأن حماية البيانات؛
   d. عدم التعامل مع البيانات الشخصية أو معاملتها إلا بقدر ما تجيزه المنظومة إلى حد ما؛

e. التأكد من أن مستخدمي المنظومة لا يستخدمون البيانات الشخصية بشكل غير قانوني.

3. مبدأ الغرض والأهمية والاحتفاظ: ينبغي لأجهزة إنفاذ القانون جمع البيانات الشخصية لأغراض محددة وصريحة وقانونية، وينبغي أن تتأكد من عدم المضي في معاملة البيانات بأي طريقة تتعارض مع هذه الأغراض. ويجب أن تكون البيانات الشخصية وافية وذات صلة بالأغراض التي لأجلها تُجمع ولاحقا تعامَل. ولا ينبغي الاحتفاظ بالبيانات الشخصية إلا للفترة المطلوبة لتحقيق الأغراض التي لأجلها تم الحصول عليها أو معاملتها. وبعد انقضاء الفترة المطلوبة، لا ينبغي الاحتفاظ بالبيانات إلا لأغراض تاريخية وإحصائية وبحثية، بما يتماشى مع الأحكام القانونية القائمة.

4. مبدأ الدقة: ينبغي أن تضمن أجهزة إنفاذ القانون دقة البيانات الشخصية التي يتم الحصول عليها، وعند الحاجة تحديثها. وينبغي اتخاذ جميع التدابير الممكنة لضمان حذف أو تصحيح البيانات غير الدقيقة وغير الكاملة بالنسبة لتحقيق الأغراض التي لأجلها تم الحصول عليها ومعاملتها.

5. مبدأ الشفافية: ينبغي لأجهزة إنفاذ القانون توفير معلومات عن معاملة البيانات الشخصية، شريطة التقيد بالاستثناءات السارية.

6. مبدأ السرية والأمن: يجب أن تضمن أجهزة إنفاذ القانون أن البيانات الموجودة في المنظومة تعامَل بشكل سري وأنها محميّة. ويجب تحديد مستوى سرية البيانات التي تعامَل في المنظومة وفقا للمخاطر التي يستتبعها الإفصاح عنها على الأشخاص موضوع البيانات وعلى مصادر البيانات.

7. مبدأ اختيار مُعامِل البيانات: يتعين على أجهزة إنفاذ القانون، عند معاملة البيانات نيابة عنها، اختيار معامِل البيانات الذي يوفر الضمانات الكافية. ومن مسؤولية هذه الأجهزة ومعامِل البيانات التأكد من التقيد بمبادئ حماية البيانات المعمول بها.

1. عدم جمع البيانات الشخصية بطريقة غير قانونية
2. احترام الحقوق الأساسية للأشخاص موضوع البيانات، لا سيما حقوق الإنسان
3. عدم معاملة البيانات الشخصية بطريقة غير عادلة أو غير منطقية أو غير قانونية
4. التأكد من أن لأي معاملة للبيانات غرضا محددا وصريحا ومشروعا
5. تحديد فترات الاحتفاظ بالبيانات الشخصية والالتزام بهذه الفترات
6. التأكد من دقة البيانات الشخصية التي تُجمع، وعند الحاجة تحديثها
7. حذف البيانات غير الدقيقة أو غير الكاملة أو تصحيحها
8. إدارة البيانات الشخصية بطريقة شفافة
9. إحكام أمن المنظومة والتأكد من إبقاء البيانات الشخصية سرية
10. الإشراف على المتعهدين من الباطن العاملين في المنظومة

2.2 الغرض من معاملة البيانات في المنظومة

1. يجب معاملة البيانات في المنظومة لتحقيق واحد أو أكثر من أغراض إنفاذ القانون التالية:
   a. منع الجرائم؛
   b. التحقيق في الجرائم؛
   c. الكشف عن الجرائم؛
   d. محاكمة مرتكبي الجرائم؛
   e. هـ. تنفيذ العقوبات؛
   f. صون النظام العام؛
   g. حماية الأمن العام من الأخطار التي تتهدده ومنعها؛
   h. أداء كل مهمة أو مسؤولية تقع على عاتق أجهزة إنفاذ القانون بموجب القانون.

2. لا ينبغي استخدام البيانات الشخصية التي تُجمع لأغراض إنفاذ القانون لأي غرض آخر يتعارض مع الغرض الأصلي الذي تُجمع لأجله، إلا إذا أجاز القانون ذلك.

أفضل الممارسات

الغرض من معاملة البيانات

1. التقيد بالأغراض المعلنة المنشودة من معاملة البيانات في المنظومة
2. التأكد من أن توسيع نطاق الأغراض من معاملة البيانات جائز قانونيا قبل توسيعه
3. عدم تغيير الأغراض المعلنة المنشودة من معاملة البيانات

الفصل الثالث

نظام حماية البيانات وإدارتها

3.1 المراقبة والإبلاغ

1. ينبغي أن تكون لدى كل بلد مشارك في منظومة وابيس هيئة مستقلة تُعنى بحماية البيانات، تطبيقا للمادة 14 من Supplementary Act.
2. وينبغي إبلاغ هيئة حماية البيانات بمنظومة وابيس بموجب قوانين البلد المشارك فيها.
3. وينبغي للبلد المشارك في منظومة وابيس، الذي لم يقم بعد باعتماد القوانين أو تشكيل هيئة حماية البيانات المستقلة المطلوبة، نشر Supplementary Act في الجريدة الرسمية واحترام المبادئ الواردة فيه. ويمكنه أيضا تشكيل أو تعيين هيئة إشراف مستقلة لأداء مهام هيئة حماية البيانات.
4. وينبغي لكل بلد مشارك في منظومة وابيس أن يضع أطرا قانونية، في شكل قوانين وأنظمة وقواعد وتوجيهات وسياسات وغيرها، تحدد بوضوح أجهزة إنفاذ القانون المسؤولة عن معاملة البيانات في المنظومة وتعرض الطريقة المقرر أن تعامَل بها البيانات الشخصية فيها.
5. وتتولى هيئة إنفاذ القانون مسؤولية جميع عمليات معاملة البيانات التي تجريها أو تسمح بإجرائها، وتخضع للمساءلة بشأنها.

أفضل الممارسات

المراقبة والإبلاغ

1. وضع قانون لحماية البيانات الشخصية وتشكيل هيئة مستقلة تُعنى بحمايتها تطبيقا للمادة 14من Supplementary Act
2. إبلاغ هيئة حماية البيانات بوجود المنظومة
3. توعية السلطات العامة التي لم تعتمد بعد تشريعات لحماية البيانات بضرورة الإسراع في نشر Supplementary Act في الجريدة الرسمية في بلدانها

3.2 الموظف المعني بحماية البيانات والتوعية بحماية البيانات والتدريب عليها

1. ينبغي لأجهزة إنفاذ القانون تعيين موظف معني بحماية البيانات يمتلك فهما دقيقا لقانون حماية البيانات والممارسات المتبعة لحمايتها، لأداء المهام التالية::
   a. إبلاغ أجهزة إنفاذ القانون التي تعامل البيانات في المنظومة بواجباتها القانونية من حيث معاملة البيانات الشخصية وإطلاعها عليها؛
   b. التحقق من مدى تقيّد أجهزة إنفاذ القانون بالمعايير التي تحكم معاملة البيانات في المنظومة؛
   c. إسداء المشورة عند الطلب بشأن تقييم تأثير حماية البيانات؛
   d. التعاون والتنسيق مع هيئات حماية البيانات المختصة؛
   e. تنظيم برامج تدريب دائمة مناسبة بشأن كيفية حماية البيانات مخصصة للأشخاص الذين يعملون على المنظومة.

2. حسب الاقتضاء، يجب أن يكون حصول الموظف المعني بحماية البيانات على الشهادات اللازمة والتدريب اللازم إلزاميا.

3. ينبغي لأجهزة إنفاذ القانون المشاركة في منظومة وابيس ضمان توعية جميع مستخدمي المنظومة بمسألة حماية البيانات وتدريبهم على كيفية حمايتها.

4. ينبغي أن يكون الموظف المعني بحماية البيانات حاصلا على التدريب اللازم و/ أو الشهادة اللازمة لإدارة إطار حماية البيانات في منظومة وابيس.

أفضل الممارسات

الموظف المعني بحماية البيانات

1. تعيين موظف معني حماية البيانات
2. التأكد من أن الموظف المعني بحماية البيانات يمتلك المؤهلات المناسبة للوظيفة
3. إعداد برنامج لبناء القدرات في مجال حماية البيانات مخصص للموظف المعني بحماية البيانات ومستخدمي المنظومة

عن تدريب أجهزة إنفاذ القانون على حماية البيانات

شرطة دايفد بويز، قرار مكتب مفوض المعلومات، المرجع COM0672404، COM0666484، COM0677576

أكد مكتب مفوض المعلومات، وهو هيئة حماية البيانات في المملكة المتحدة، بعد التدقيق أن 1 204 موظفين من أصل 2 258 موظفا لم يخضعوا للتدريب على حماية البيانات مما أدى إلى انتهاكات عديدة لقانون حماية البيانات. ومن ضمنهم موظف أرسل عبر الفاكس بيانات حساسة إلى جهاز فاكس مفتوح بدون إذن الشخص المعني، وموظف آخر وزع صورة لمكتبه عليه صورة لشاشة حاسوبه التي تعرض بيانات شخصية وحساسة. وأصدر مفوض المعلومات التعليمات التالية:

- وضع برنامج لتدريب كل الموظفين على كيفية حماية البيانات
- وضع برنامج تدريبي تجديدي لكل الموظفين بغية ضمان تقيّدهم الدائم بقانون حماية البيانات
- وضع برنامج لتسجيل البرامج التدريبية ومراقبتها
- اتخاذ أي تدابير أمنية أخرى، حسب الاقتضاء، لضمان حماية البيانات الشخصية من معاملتها بدون إذن وبشكل غير قانوني وإضاعتها عن غير قصد والتلف و/ أو الضرر.

*شرطة همبرسايد، قرار مكتب مفوض المعلومات، المرجع **COM0649315***

ردا على ضياع أقراص غير مشفرة تتضمن مقابلة مع ضحية اغتصاب مفترضة، حققت هيئة حماية البيانات مع شرطة Humberside. وخلص التحقيق إلى أن نسبة من تقيدوا في قسم الشرطة بحماية البيانات التي تدربوا عليها لم تتجاوز 16,8 في المائة. واتخذ المتحكم بالبيانات التدابير اللازمة لضمان ما يلي:

- يتلقى جميع الموظفين الحاليين المسؤولين عن التعامل مع البيانات الشخصية التدريب الملائم والمتعلق تحديدا بحماية البيانات وذلك في غضون ستة أشهر؛
- يتلقى جميع الموظفين الذين يتعاملون بانتظام مع وسائط الخزن القابلة للفك مثل الأقراص المدمجة وأقراص الفيديو الرقمية وشرائح ذاكرة USB التدريب على كيفية استخدام التشفير، بما في ذلك عندما يكون التشفير لازما وكيفية التشفير؛
- تنظيم برامج تدريبية سنوية لتجديد المعلومات؛
- تزويد الموظفين الجدد المسؤولين عن التعامل مع البيانات الشخصية بالتدريب اللازم والمتعلق تحديدا بحماية البيانات بعد الفترة التحضيرية؛
- التأكد من حضور برامج التدريب؛
- تعميم سياسات وإجراءات هيئة حماية البيانات وإتاحتها للموظفين في كل الأقسام التي تتعامل مع البيانات الشخصية.

3.3 التقيد بمبادئ حماية البيانات وإدارتها

1. لضمان التقيد بمبادئ حماية البيانات عند استخدام منظومة وابيس وتشغيلها، ينبغي لأجهزة إنفاذ القانون معاملة جمع البيانات الشخصية بطريقة تقلص إلى الحد الأدنى من مخاطر معاملتها بدون إذن وبشكل غير قانوني.

2. وينبغي لأجهزة إنفاذ القانون دمج مسألة حماية الخصوصيات والبيانات في هياكل الإدارة التابعة لها لمواءمة معايير مبادئ حماية البيانات مع أهدافها التنظيمية وثقافتها. ويمكن تحقيق ذلك من خلال فهم هذه المبادئ ونطاقها، وتبيان الثغرات التي تشوب التقيد بها على صعيد كل الأجهزة، ووضع الخطط الكفيلة بسدها وتنفيذ الخطط والسياسات والإجراءات ذات الصلة على المدى الاستراتيجي.

3. وينبغي لأجهزة إنفاذ القانون أيضا تنفيذ السياسات التي تضمن تكليف الموظفين أو العاملين بمسؤوليات واضحة في مجال حماية البيانات وإخضاعهم للمساءلة.

4. وأنشطة الإدارة الاستراتيجية التي يمكن أن تسهل تنفيذ المبادئ تشمل ما يلي:

a. إسناد مسؤولية حماية البيانات في استخدام منظومة وابيس وتشغيلها إلى شخص معين – مثل الموظف المعني بحماية البيانات. وينبغي أن يكون هذا الموظف مسؤولا عن تسهيل التقيد بالقواعد المطلوبة عند معاملة البيانات في المنظومة. ويتعيّن عليه تولي الإدارة اليومية لشؤون حماية البيانات في المنظومة. ويجوز أن يؤدي دورا محددا لحمايتها و/ أو يعمل في الأقسام القانونية أو تلك المعنية بالتقيد بالقيود أو تكنولوجيا المعلومات أو الأمن أو إدارة المعلومات.

b. توعية وإشراك مسؤولين رفيعي المستوى في إدارة إطار حماية البيانات في منظومة وابيس. ويتطلب تنفيذ هذا الإطار مشاركة الإدارة العليا ليكون سلسا. وهذه المشاركة الداعمة يمكن أن تشمل ما يلي:

i. إبلاغ جميع الموظفين ومستويات الإدارة الدنيا عن مدى أهمية حماية البيانات في منظومة وابيس؛

ii. المشاركة في مبادرات حماية البيانات؛

iii. توفير ما يكفي من موارد مالية لدعم أنشطة حماية البيانات.

c. إسناد مسؤولية إطار حماية البيانات في منظومة وابيس إلى مجمل أجهزة إنفاذ القانون. وتتطلب إدارة حماية البيانات مساهمة ومشاركة جميع مستخدمي المنظومة تقريبا. لذلك، في وسع الموظف المعني بحماية البيانات تشكيل فريق يُعنى بحماية البيانات للعمل في مختلف المجموعات الوظيفية داخل الوحدة للمساعدة على فهم ما تواجهه هذه المجموعات من مخاطر تتعرض لها حماية البيانات.

d. .كفالة التواصل الدائم بين الموظف المعني بحماية البيانات وفريق حماية البيانات من جهة والمسؤولين عن حماية البيانات داخل منظومة وابيس من جهة أخرى. ويساعد ذلك في تنفيذ إطار حماية البيانات فعليا من أجل:

i. المبادرة مسبقا إلى ترسيخ مبدأ حماية البيانات في المشاريع الجارية؛

ii. مساعدة المستخدمين على تحقيق أهدافهم.

e. إشراك جميع أصحاب المصلحة البارزين المعنيين بإطار حماية البيانات في منظومة وابيس. ويتعين على الموظف المعني بحماية البيانات التواصل مع مستخدمي المنظومة. ومشاركة هذه الجهات قد تكون في شكل نقاشات أو اجتماعات رسمية (مثل الاجتماعات الشهرية أو الفصلية) تتناول مسألة إطار حماية البيانات في المنظومة. ويتعين أيضا إشراك الموظف المعني بحماية البيانات في الأنشطة التي تؤثر في حمايتها، ومنها مثلا أمن المعلومات والتحقيقات وجمع المعلومات وما إلى ذلك.

f. رفع تقارير منتظمة ودائمة إلى المسؤولين الداخليين، مثل الإدارة العليا، عن حالة إطار حماية البيانات. ويتعين أن تسلط هذه التقارير الضوء على أبرز المخاطر التي تتعرض لها حماية البيانات أو انتهاكها أو الأحداث المتصلة بها وغير ذلك. وتوفير معلومات سريعة ودقيقة عن الخصوصيات وحماية البيانات للمسؤولين عن الإشراف على إطار حماية البيانات وإدارته ضروري لضمان تقيد أجهزة إنفاذ القانون التي تستخدم منظومة وابيس بالقواعد التي تحكم معاملة البيانات الشخصية وللحد من مخاطر عدم التقيد بها. ومن المهم النظر في استحداث مقاييس لمعرفة مدى التقيد بهذه القواعد وتنفيذها والمعلومات الواردة في التقارير المتعلقة بهاتين المسألتين.

g. رفع تقارير إلى أصحاب المصلحة الخارجيين مثل هيئات حماية البيانات، والسلطات العامة، وأجهزة إنفاذ القانون وأصحاب المصلحة الرئيسيين الآخرين عند الضرورة. وتشكل توعيتهم بتنفيذ إطار حماية البيانات عاملا حيويا لضمان الانفتاح والشفافية. وتوعية جميع أصحاب المصلحة الرئيسيين الخارجيين تعزز أيضا النزاهة وتبعث الثقة في المنظومة. ويتعين على أجهزة إنفاذ القانون التي تستخدم منظومة وابيس العمل جاهدة لاتباع نهج يركز على المستخدم وجعل الشفافية أولوية من خلال البحث عن طرق أكثر ملاءمة ليتسنى لها الوفاء بواجباتها. واستخدام لغة بسيطة أمر مشجع. ويمكن توعية أصحاب المصلحة الخارجيين عن طريق:

i. التقارير المتعلقة بالشفافية الصادرة عن جهاز إنفاذ القانون؛

ii. إيداع تقارير التدقيق في مدى التقيد بقواعد حماية البيانات لدى هيئة حماية البيانات (حيث توجد)؛

iii. ‘نشر تقارير التدقيق في حماية البيانات؛

iv. ‘تحقق تجريه أطراف ثالثة أو التدقيق في المسؤوليات؛

v. ‘إعداد إشعار بحماية البيانات وتحديثه.

h. إجراء تقييم للمخاطر في جميع الوحدات أو الإدارات التي يمكنها الوصول إلى منظومة وابيس. ويجب أن يكون تقييم المخاطر التي تتهدد حماية البيانات شرطا لا بد منه للمضي في إعداد سياسة عامة متعلقة بحمايتها. ويجب على موظف حماية البيانات أو الموظف المختص في جهاز إنفاذ القانون استحداثُ آلية تقييم ذاتي للوحدة أو للأقسام لمعرفة مستوى حماية البيانات تغطي ما يتصل بمنظومة وابيس من عمليات بحث وتحسين وتوفير معلومات وتدريب، والإشرافُ على هذه الآلية. وآلية تقييم هذه المخاطر ستمكّن موظف حماية البيانات من كشف الثغرات التي تعاني منها حمايتها وإيلائها الأولوية داخل جهاز إنفاذ القانون، ومن إدارة تنفيذ سياسة تخفيف المخاطر في منظومة وابيس. وعند الضرورة، يمكن لأجهزة إنفاذ القانون النظر في استشارة طرف ثالث مختص لمساعدتها.

i. مطالبة جميع الموظفين المعنيين بمنظومة وابيس بالإقرار بإدراك ماهية إطار حماية البيانات في المنظومة والموافقة على الالتزام به. وإن ذلك ضروري للتأكد من أن العاملين أو الموظفين يدركون الغرض من حماية البيانات على مستوى تطبيق المنظومة وتشغيلها. ومن المهم تحميل العاملين أو الموظفين مسؤولية أفعالهم في سياق معاملة البيانات الشخصية. لذلك يجب على كل موظف إدراك ماهية إطار حماية البيانات والموافقة عليه. ويمكن أن يتم ذلك في وثيقة منفصلة (ورقية أو إلكترونية) أو أن يكون جزءا من وثيقة موجودة مثل شروط الخدمة أو قواعد السلوك أو دليل الموظفين أو نسخ فردية من سياسة حماية البيانات.

نظام حماية البيانات وإدارتها

1. تقليص المخاطر المرتبطة بمعاملة البيانات في المنظومة بدون إذن أو بشكل غير قانوني
2. تعريف وتحديد أدوار كل مستخدم للمنظومة ومسؤوليته
3. توعية وإشراك مسؤولين رفيعي المستوى في إدارة إطار حماية البيانات في منظومة وابيس
4. إنشاء قناة تواصل مفتوحة بين جميع مستخدمي منظومة وابيس
5. إعداد تقارير عن مشاكل حماية البيانات الناجمة عن عمل المنظومة
6. تقييم المخاطر التي تتعرض لها حماية البيانات في كل الوحدات أو الأقسام التي يمكنها الوصول إلى منظومة وابيس
7. التأكد من قيام كل مستخدم لمنظومة وابيس بتوقيع تعهد بحماية البيانات

جمع البيانات الشخصية وتوفيرها

4.1 جمع البيانات الشخصية

1. ينبغي لأجهزة إنفاذ القانون التأكد من وجود أساس قانوني لجمع البيانات الشخصية قبل جمعها.

2. لا ينبغي أن تتجاوز البيانات الشخصية التي تُجمع في المنظومة ما يقتضيه تحقيق الغرض الذي تُجمع لأجله والمتناسب مع أغراض إنفاذ القانون التي تُجمع لأجلها.

دراسة حالة

عن ضرورة معاملة البيانات الشخصية

Uzun ضد ألمانيا، حكم المحكمة الأوروبية لحقوق الإنسان، 2 أيلول/سبتمبر 2010، الطلب رقم 05/35629

اشتكى مقدم الطلب، المشتبه في مشاركته في اعتداء بالقنابل نفذته حركة يسارية متطرفة، من أن مراقبته عن طريق النظام العالمي لتحديد المواقع (GPS) واستخدام البيانات التي استُمدت منه في الدعوى الجنائية ضده قد انتهكت حقوقه وحمايته بموجب المادة 8 من حق احترام الحياة الخاصة.

ومع أن المحكمة أقرت بأن المراقبة عن طريق نظام GPS، بطبيعتها، أكثر ميلا للتدخل في حق الشخص في أن تُحترَم حياته الخاصة (المادة 8)، فإن هذا التدخل يكون مقبولا عندما تكون هذه التدابير «ضرورية في مجتمع ديمقراطي». والمراقبة لم تُطلب أو تُمنح في البداية، ولكنها مُنحت بعد عدة أشهر من المراقبة البصرية واتخاذ تدابير أقل تدخلا. أضف إلى ذلك أنه لم يراقَب عن طريق نظام GPS إلا عندما كان في السيارة، وبالتالي لا يمكن القول إنه خضع لمراقبة تامة وشاملة. وأخيرا، إن المراقبة، لكونها تمت على خلفية تهديد عام خطير (محاولات تفجير قنابل ضد سياسيين وموظفين في الخدمة المدنية)، «ضرورية» بالمعنى المقصود في المادة 8.

3. عند جمع البيانات الشخصية، يجب إقامة صلة واضحة بين الشخص الذي تعامَل بياناته الشخصية والغرض من معاملتها.

الفصل الرابع

عن الصلة القائمة بين البيانات الشخصية والشخص المعني

Mustafa Sezgin Tanrikulu ضد تركيا، حكم المحكمة الأوروبية لحقوق الإنسان، 18 تموز/يوليو 2017، الطلب رقم 06/27473

في أعقاب اعتداء بقنابل أسفر عن مقتل مفوض في الشرطة، استحصلت وكالة الاستخبارات الوطنية التركية على أمر من المحكمة للتنصت على جميع المكالمات الهاتفية المحلية والدولية التي أُجريت في الفترة من 8 نيسان/ أبريل و30 أيار/مايو 2005 باستخدام شركة Turk Telekom الخاصة وهي مشغلة شبكات الهاتف المحمول ومقدمة خدمات الإنترنت في البلد، وللحصول على المعلومات الواردة في الرسائل النصية (SMS) والرسائل المتعددة الوسائط (MMS) والخدمة الراديوية الحزمية العامة (GPRS) والمراسلات التي تمت بالفاكس، فضلا عن هويات المتصلين وعناوين بروتوكول الإنترنت (IP) وسائر المعلومات المتعلقة بالاتصالات.

واعتبرت المحكمة الأوروبية لحقوق الإنسان هذا الأمر – الذي أذن في التنصت على اتصالات كل شخص في جمهورية تركيا – غير قانوني على أساس أنه، من بين أمور أخرى، لم يقتصر على الأشخاص المشتبه في ارتكابهم جرائم جنائية ذات صلة على غرار المطلوب في القانون المعمول به.

4. ينبغي لأجهزة إنفاذ القانون التمييز بوضوح بين مختلف فئات الأشخاص الذين تعامَل بياناتهم، مثل المشتبه فيهم وذوي الأهمية بالنسبة للتحقيق والمدانين بجريمة جنائية والضحايا والشهود ومن على صلة بأي منهم، وغيرهم.

5. ينبغي لأجهزة إنفاذ القانون الحرص على أن تكون البيانات التي تُجمع دقيقة وغير مضللة ومحدّثة وكافية وذات صلة بالأغراض التي تعامَل لأجلها ولا تتجاوزها.

أفضل الممارسات

جمع البيانات الشخصية

1. التأكد بادئ ذي بدء من وجود أساس قانوني لجمع البيانات الشخصية
2. احترام مبدأ تناسب جمع البيانات الشخصية مع الغرض منه
3. التأكد من أن البيانات التي تُجمع دقيقة وغير مضللة ومحدثة وكافية وذات صلة بالأغراض التي تعامَل لأجلها ولا تتجاوزها

4.2 توفير البيانات لهيئات عامة أخرى أو إحالتها إليها

1. يجوز لأجهزة إنفاذ القانون توفير البيانات الشخصية لهيئات عامة أخرى ليست من أجهزة إنفاذ القانون أو إحالتها إليها، إذا:
   a. كان توفيرها منصوصا عليه في القانون؛
   b. إذا كانت البيانات مطلوبة من قبل متلقّيها لتمكينه من أداء مهامه القانونية (كالتحقيقات أو الواجبات القانونية الأخرى بمقتضى القانون الوطني، على سبيل المثال) أو لدرء خطر جسيم وشيك يتهدد أشخاصا آخرين أو النظام العام أو الأمن العام.
2. ينبغي لأجهزة إنفاذ القانون، عند بت ما إذا كان ينبغي لها توفير البيانات لهيئات عامة أخرى أو إحالتها إليها، إيلاء الاعتبار لما يستتبعه توفيرها أو إحالتها من أضرار على الشخص المعني.
3. ينبغي لأجهزة إنفاذ القانون إبلاغ الهيئة العامة التي تتلقى البيانات الشخصية بأن من واجبها عدم استخدام البيانات التي وفرتها لها أو أحالتها إليها إلا للأغراض التي لأجلها تم توفيرها أو إحالتها.
4. ينبغي لأجهزة إنفاذ القانون التأكد من أن الهيئات العامة اتخذت الخطوات اللازمة للتقيد بإطار حماية البيانات المطبق.

توفير / إحالة البيانات

1. قبل توفير البيانات الشخصية لهيئات أخرى / إحالتها إليها، ينبغي التأكد من أن توفيرها / إحالتها منصوص عليهما في القانون
2. قبل توفير البيانات لهيئات أخرى أو إحالتها إليها، ينبغي بحث ما قد يستتبعه توفيرها أو إحالتها من أضرار على الشخص المعني
3. إبلاغ الهيئة العامة التي تتلقى البيانات الشخصية بأن من واجبها عدم استخدام البيانات التي وفرتها لها أو أحالتها إليها إلا للأغراض التي لأجلها تم توفيرها أو إحالتها

4.3 توفير البيانات الشخصية لهيئات خاصة أو للعموم أو إحالتها إليهما

1. يجوز لأجهزة إنفاذ القانون، بموجب القانون المعمول به في كل بلد، توفير البيانات الشخصية لهيئات خاصة أو إحالتها إليها في واحدة أو أكثر من الحالات التالية::
   a. تحقيق أهداف تتعلق بإنفاذ القانون؛
   b. منع خطر جسيم وشيك يتهدد النظام العام أو الأمن العام؛
   c. دفاعا عن مصلحة الشخص موضوع البيانات؛
   d. لدواع إنسانية.

2. ينبغي لأجهزة إنفاذ القانون، عند بت ما إذا كان ينبغي لها توفير البيانات لهيئات عامة أخرى أو إحالتها إليها، بحث ما يستتبعه توفيرها أو إحالتها من أضرار على الشخص المعني.

3. عند توفير البيانات الشخصية لهيئة خاصة أو إحالتها إليها، ينبغي لجهاز إنفاذ القانون الحرص على الحصول من الهيئة الخاصة على تعهد خطي بأنها تتقيد بمبادئ حماية البيانات المعتمدة.

4. عند توفير بيانات شخصية للعموم أو إحالتها إليهم في سياق التحقيقات، ينبغي التحقق بشكل خاص من مدى ضرورة توفيرها أو إحالتها وفائدتها للمصلحة العامة. ويجب وضع الضمانات اللازمة لكفالة احترام حقوق الأشخاص المعنيين بالقضية.

5. ينبغي توفير البيانات للعموم أو إحالتها إليهم لتحقيق ما يلي:
   a. تنبيههم؛ أو
   b. طلب المساعدة منهم؛ أو
   c. لأي غرض آخر يتصل بإنفاذ القانون على النحو المحدد في النقطة 2.2 أعلاه.

6. ينبغي لجهاز إنفاذ القانون، عند تلقّيه بيانات شخصية من جهاز آخر لإنفاذ للقانون، أن يحصل منه على موافقته الرسمية قبل توفير هذه البيانات لهيئة خاصة أو للعموم أو إحالتها إليهما.

7. ينبغي لجهاز إنفاذ القانون، عند توفيره بيانات شخصية أو إحالتها، اتخاذ الترتيبات اللازمة للتأكد من أن هذه البيانات تخضع لنفس مستوى الحماية أو لمستوى أعلى منه.

أفضل الممارسات

توفير البيانات لهيئات خاصة أو للعموم أو إحالتها إليهما

1. التقيد بأحكام النصوص القانونية المعمول بها قبل توفير بيانات شخصية لهيئات خاصة أو إحالتها إليها
2. قبل توفير بيانات شخصية أو إحالتها، بحث ما يمكن أن يستتبعه توفيرها أو إحالتها من عواقب على الضحايا أو الشهود
3. إبلاغ الضحايا والشهود بأن بياناتهم الشخصية سيتم توفيرها للعموم أو إحالتها إليهم قبل القيام بذلك
4. احترام حقوق الأشخاص عند توفير بياناتهم الشخصية للعموم أو إحالتها إليهم
5. الحصول على موافقة رسمية من جهاز إنفاذ القانون قبل توفير البيانات الشخصية لهيئة عامة أو للعموم أو إحالتها إليهما
6. التأكد من توفير مستوى كافٍ من الحماية للبيانات الشخصية قبل توفيرها لهيئات خاصة أو العموم أو إحالتها إليهما
7. التأكد من توقيع الهيئات الخاصة تعهدا خطيا باحترام المبادئ السارية على حماية البيانات الشخصية

دراسة حالة

عن إحالة البيانات الشخصية إلى أفراد من العموم

شرطة ويست ميدلاندز، قرار مكتب مفوض المعلومات، المرجع ENF0674010

فُرض على شخصين أمر سلوك جنائي (CRIMINAL BEHAVIOUR ORDER) لإلحاقهما أضرارا بالممتلكات وإطلاقهما تهديدات باستخدام بالعنف. وحظر هذا الأمر عليهما دخول أماكن معينة والالتقاء في مناطق معينة. وقررت شرطة ويست ميدلاندز (المتحكم بالبيانات) إعلان أحكام هذا الأمر في منشور وُزع على نحو 30 منزلا وتضمن بيانات شخصية عن ضحايا الجرائم والشهود عليها بدون الحصول على إذن منهم. وطلب مكتب مفوض المعلومات (هيئة حماية البيانات) من المتحكم بالبيانات التأكد مما يلي:

- تقييم ما يستتبعه نشر أوامر السلوك الجنائي من مخاطر على ضحايا الجرائم والشهود عليها؛
- إبلاغ الضحايا والشهود بنشر هذه الأوامر قبل نشرها؛
- توثيق خطوات إعداد المنشور وتوزيعه؛
- تنظيم تدريب إلزامي على كيفية حماية البيانات الشخصية مخصص لجميع الموظفين الجدد والحاليين الذين يتولون معاملة البيانات الشخصية؛
- تنظيم تدريب لتجديد المعلومات المتعلقة بكيفية حماية البيانات الشخصية مخصص لجميع الموظفين الذين يتولون معاملة البيانات الشخصية؛
- اعتماد أنظمة للتحقق من مدى وضع المهارات المكتسبة من التدريب على حماية البيانات موضع التطبيق؛
- تنفيذ ما تقدّم يجري في مهلة ثلاثة أشهر.

4.4 توفير البيانات لجهات دولية أو إحالتها إليها

1. كقاعدة عامة، ينبغي لأجهزة إنفاذ القانون التي توفر البيانات الشخصية لجهات دولية أو تحيلها إليها أن تتحقق مما إذا كانت الهيئة التي تتلقاها تؤدي مهام مسندة إليها بموجب القانون ولأغراض إنفاذ القانون، ومما إذا كان أداء مهامها هذه يستلزم تزويدها بالبيانات. وإحالة البيانات إلى جهات دولية ينبغي أن تقتصر على أجهزة إنفاذ القانون.

2. عند توفير البيانات الشخصية لأحد أجهزة إنفاذ القانون في بلد ثالث أو لمنظمة إقليمية أو دولية ما، ينبغي للسلطة التي توفرها وللسلطة التي تتلقاها الحرص على أن يوفر البلد و/ أو جهاز إنفاذ القانون مستوى كافيا من الحماية لأمن المعلومات والخصوصيات والحريات والحقوق الأساسية للأشخاص المعنيين في سياق معاملة هذه البيانات.

3. يجب على جهاز إنفاذ القانون الذي يوفر البيانات الشخصية أو يحيلها اتخاذ التدابير الكافية لكفالة خضوع هذه البيانات لنفس مستوى الحماية أو لمستوى أعلى منه.

أفضل الممارسات

توفير البيانات الشخصية لجهات دولية أو إحالتها إليها

1. التقيد بأحكام النصوص القانونية قبل توفير البيانات الشخصية لجهات دولية أو إحالتها إليها
2. التأكد من توفير البلد و/ أو جهاز إنفاذ القانون مستوى كافيا من الحماية للبيانات عند معاملتها

الفصل الخامس

نوعية البيانات وسريتها وأمنها

5.1 نوعية البيانات

1. ينبغي لأجهزة إنفاذ القانون اتخاذ جميع التدابير الممكنة للتأكد من عدم إحالة البيانات الشخصية غير الدقيقة أو غير الكاملة أو القديمة وعدم توفيرها وعدم وضعها في المتناول. ولتحقيق ذلك، ينبغي للأجهزة المذكورة التحقق من نوعية البيانات الشخصية قبل إحالتها أو توفيرها أو إتاحتها.

2. ينبغي قدر الإمكان، في جميع عمليات إحالة البيانات الشخصية أو توفيرها، تزويد الجهة المتلقية بالمعلومات اللازمة التي تمكّنها من تقييم درجة دقة هذه البيانات واكتمالها وموثوقيتها وإلى أي حد هي محدثة.

3. إذا وُفرت أو أحيلت بيانات شخصية غير دقيقة أو مغلوطة، أو في حال توفيرها أو إحالتها بشكل غير مشروع، ينبغي إبلاغ الجهة المتلقية بذلك بدون إبطاء. وفي مثل هذه الحال، ينبغي تصحيحها أو حذفها أو معاملتها بطريقة مقيدة، حسب الاقتضاء.

4. ينبغي تصنيف البيانات التي تُجمَع وفقا لدرجة دقتها أو موثوقيتها، وينبغي بشكل خاص التمييز بين البيانات المستندة إلى وقائع وبين تلك المستندة إلى آراء أو عمليات تقييم شخصية.

دراسة حالة

بشأن معاملة بيانات شخصية مغلوطة

Cemalettin Canli ضد تركيا، حكم المحكمة الأوروبية لحقوق الإنسان، 18 تشرين الثاني/نوفمبر 2008، الطلب رقم 04/22427

في عام 2003، بينما كانت تساق تُهم جنائية بحق السيد CEMALETTIN CANLI، قدمت أجهزة الشرطة تقريرا شرطيا أشير فيه إلى مجموعتين سابقتين من هذه التهم سيقتا بحقه في عام 1990 لانتمائه إلى منظمة غير مشروعة. وقد بُرِّئ السيد CANLI من إحداهما وأُغلق ملف الثانية.

وأعلنت المحكمة أن التقرير الشرطي لم يلتزم بالقانون لأنه لم يُشر إلى تبرئة السيد CANLI في القضية الأولى ولا إلى إغلاق ملف الثانية.

Mikolajova ضد سلوفاكيا، حكم المحكمة الأوروبية لحقوق الإنسان، 18 كانون الثاني/يناير 2011، الطلب رقم 03/4479

في عام 2000، رفع زوج مقدمة الطلب شكوى جنائية ضدها متهما إياها بالاعتداء عليه. وأُسقطت التهمة بعد أيام من ذلك ولم توجه المحكمة أي تهمة لها ولم تُدنها. إلا أن الشرطة سجلت في ملف القضية أن مقدمة الطلب ارتكبت جناية بإلحاقها أضرارا جسدية بشخص آخر، وأنها ذكرت هذه المعلومة لطرف ثالث استخدمها ضدها. واعتبرت المحكمة أن قرار الشرطة قد انتهك حقوق مقدمة الطلب لأنه صيغ بشكل أشار إلى أنها مذنبة في حين أن التهمة لم توجَّه إليها قط ولم يثبت عليها ذنب ارتكاب الجناية.

أفضل الممارسات

نوعية البيانات

1. التحقق من نوعية البيانات الشخصية قبل إحالتها أو توفيرها أو وضعها في المتناول
2. إبلاغ الجهات المتلقية في حال توفير بيانات غير دقيقة أو مغلوطة أو إحالتها أو وضعها في المتناول
3. تصنيف البيانات وفقا لدرجة دقتها أو موثوقيتها

5.2 السرية والأمن

1. ينبغي لأجهزة إنفاذ القانون اتخاذ التدابير التقنية والتنظيمية المناسبة والكافية لحماية المنظومة من مخاطر مثل الوصول غير المقصود أو غير المأذون فيه إلى البيانات الشخصية أو إتلافها أو اختفائها أو استخدامها أو تغييرها أو الكشف عنها.

2. وينبغي لأجهزة إنفاذ القانون تنفيذ تدابير تهدف إلى:

a. منع الأشخاص غير المأذون لهم في استخدام المنظومة من الوصول إلى معدات المنظومة المستخدمة لمعاملة البيانات؛

b. منع قراءة البيانات من المنظومة أو نسخها أو تغييرها أو حذفها بدون إذن؛

c. منع تسجيل البيانات الشخصية والاطلاع على البيانات الشخصية المسجلة أو تعديلها أو حذفها بدون إذن؛

d. منع الأشخاص غير المأذون لهم في استخدام المنظومة من استخدام منظومات المعاملة المؤتمتة وذلك بواسطة معدات إحالة البيانات؛

e. التأكد من أن للأشخاص المأذون لهم في استخدام المنظومة إمكانية الوصول فقط إلى البيانات الشخصية التي يجيز لهم الوصول إليها الإذنُ الذي في حوزتهم؛

f. الحرص على أنه يمكن تأكيد وإثبات الهيئات التي أحيلت إليها البيانات الشخصية المسجلة في المنظومة أو التي قد تحال إليها أو توفَّر لها؛

g. الحرص على أنه يمكن لاحقا تأكيد وإثبات البيانات الشخصية التي سُجلت في المنظومة وتاريخ تسجيلها والجهة التي سجلتها؛

h. منع قراءة البيانات الشخصية أو نسخها أو تغييرها أو حذفها بدون إذن أثناء إحالتها أو أثناء نقل الوسائط المسجلة عليها البيانات؛

i. التأكد من أنه يمكن إعادة تشغيل المنظومة بسرعة في حالة حدوث عطل ما؛

j. كفالة عمل كل جوانب المنظومة بسلاسة، والإبلاغ عن أي أعطال تطرأ عليها، وعدم احتمال تعرّض البيانات الشخصية المسجلة للضرر بسبب خلل في عمل المنظومة.

3. يجب أن تُعطى البيانات الشخصية التي يرسلها متعهدون من الباطن أو يديرونها ضمانات كافية من السرية.

بشأن كشف غير مقصود عن بيانات شخصية

شرطة غلوسترشر، غرامة مالية فرضها مكتب مفوض المعلومات، 11 حزيران/يونيو 2018

في 19 كانون الأول/ديسمبر 2016، أرسل أحد ضباط الشرطة الذين يحققون في قضايا اعتداء على أطفال قديمة العهد رسالة إلكترونية إلى 56 شخصا بدون استخدام وسيلة إخفاء هوية المرسل إليهم (BCC)، مما سمح لجميع المتلقين (52 شخصا على الأقل) برؤية عناوين البريد الإلكتروني العائدة لضحايا وصحافيين ومحامين. وطُلب استرجاع البريد الإلكتروني في 21 كانون الأول/ديسمبر 2016 وأُبلغت هيئة حماية البيانات بالأمر. وخلصت هذه الهيئة إلى ما يلي:

- لم توجه الشرطة رسائل إلكترونية منفصلة إلى كل من هؤلاء الأشخاص بل استخدمت وسيلة البريد الإلكتروني الجماعي؛
- لم تستخدم الشرطة وسيلة إخفاء هوية المرسل إليهم (BCC) في برمجية OUTLOOK الخاصة بمايكروسوفت؛
- لم توفر الشرطة لأفرادها أي سياسات أو إرشادات أو تدريب (أو المستوى الكافي منها) في مجال استخدام البريد الإلكتروني الجماعي واستخدام وسيلة إخفاء هوية المرسل إليهم (BCC) في برمجية OUTLOOK وخاصة في الحالات التي توجَّه فيها الرسائل الإلكترونية إلى عدد من الضحايا في قضايا حساسة أو لم تُبت بعد؛
- قامت الشرطة فورا، على النحو المطلوب، بإبلاغ الأشخاص موضوع البيانات وهيئة حماية البيانات بهذا الأمر.

فرضت هيئة حماية البيانات غرامة مالية قدرها 80 000 جنيه إسترليني بعد أن أخذت في الاعتبار بعض الأسباب التخفيفية، وأبرزها أن الشرطة بادرت على الفور بإبلاغ الأشخاص موضوع البيانات بهذا الأمر، وأن عددا من متلقّي الرسائل الإلكترونية كانوا على علم بالأمر، وأن هيئة حماية البيانات أُبلغت على الفور به، وأن الإدارة المعنية في صدد تحسين التدابير الفنية والتنظيمية لمنع حصول حوادث مماثلة في المستقبل.

دراسة حالة

بشأن تسجيل بيانات شخصية لغايات خبيثة

CNBC، 'صرف ضابط هجرة من الخدمة لتسجيله اسم زوجته في قائمة إرهابيين من أجل منعها من العودة إلى البلد جوّا'، 1 تموز/يوليو 2011

حاول أحد ضباط الهجرة البريطانيين التخلص من زوجته بإضافة اسمها إلى قائمة أشخاص مشتبه في أنهم إرهابيون. وقد استغل إمكانية وصوله إلى قواعد البيانات الأمنية لإدراج اسم زوجته في قائمة مراقبة تشمل أشخاصا ممنوعين من السفر جوا إلى بريطانيا لأن وجودهم في البلد «لا يخدم المصلحة العامة». ونتيجة لذلك، تعذرت على المرأة العودة إلى البلد من باكستان لمدة ثلاث سنوات بعد أن توجهت إليها لزيارة أسرتها. ولم يُكتشَف أمر العبث بالقائمة إلى حين اختيار الضابط للترقية والعثور فيها، أثناء عملية التدقيق في هذا الصدد، على اسم زوجته. وأكدت وزارة الداخلية أن الضابط أُقيل لسوء سلوك جسيم.

أفضل الممارسات

سرية البيانات وأمنها

1. السهر على ضمان أمن المنظومة
2. إعداد سياسة عامة في مجال أمن البيانات
3. كفالة سرية البيانات في المنظومة
4. الإبلاغ عن الأعطال التي تصيب المنظومة
5. اتخاذ تدابير تقنية وتنظيمية طارئة إذا تعطلت المنظومة

انتهاك البيانات

6.1 الإبلاغ بانتهاك البيانات

1. ينبغي لأجهزة إنفاذ القانون توثيق جميع عمليات انتهاك البيانات الشخصية التي يمكن أن تشكل خطرا على حقوق أشخاص طبيعيين وحرياتهم.
2. إذا حصل انتهاك للبيانات الشخصية يمكن أن يشكل خطرا على حقوق أشخاص طبيعيين وحرياتهم، ينبغي لجهاز إنفاذ القانون – عن طريق موظفه المكلف بحماية البيانات – إبلاغ هيئة حماية البيانات بهذا الانتهاك بدون تأخير لا مبرر له، وحيث أمكن في مهلة لا تتجاوز 72 ساعة بعد أخذ العلم بهذا الانتهاك. وينبغي لهذا الإبلاغ أن:
   a. يحدد طبيعة الانتهاك بما في ذلك، عند الإمكان، فئات الأشخاص موضوع البيانات المعنيين وعددهم التقريبي وفئات سجلات البيانات الشخصية المعنية وعددها التقريبي؛
   b. يذكر اسم الموظف المكلف بحماية البيانات وطريقة الاتصال به أو بجهة اتصال أخرى يمكن الحصول منها على مزيد من المعلومات؛
   c. يشير إلى العواقب المحتمل أن يخلفها انتهاك البيانات الشخصية؛
   d. يعرض التدابير المتخذة أو المقترح اتخاذها من قبل المتحكم بالبيانات لمعالجة الانتهاك، بما يشمل عند الاقتضاء، التدابير الكفيلة بتخفيف نتائجه السلبية المحتملة.
3. عندما يقوم جهاز لإنفاذ القانون بتوفير أو إحالة بيانات إلى متلقّ في بلد آخر، ينبغي إبلاغه بالمعلومات الواردة في النقطة 2 أعلاه.

6.2 إبلاغ الشخص موضوع البيانات بانتهاك البيانات المتعلقة به

1. إذا حصل انتهاك للبيانات الشخصية يمكن أن يشكل خطرا على حقوق أشخاص طبيعيين وحرياتهم، ينبغي لأجهزة إنفاذ القانون إبلاغ الشخص موضوع البيانات بهذا الانتهاك بدون تأخير لا مبرر له. وينبغي لجهاز إنفاذ القانون:
   a. تزويد الشخص موضوع البيانات باسم الموظف المكلف بحماية البيانات وطريقة الاتصال به أو بجهة اتصال أخرى يمكن الحصول منها على مزيد من المعلومات؛

b. الإشارة إلى العواقب المحتمل أن يخلفها انتهاك البيانات الشخصية؛

c. عرض التدابير المتخذة أو المقترح اتخاذها لمعالجة هذا الانتهاك، بما يشمل عند الاقتضاء، التدابير الكفيلة بتخفيف نتائجه السلبية المحتملة.

2. لا حاجة إلى تزويد الشخص موضوع البيانات بالتفاصيل المذكورة أعلاه إذا:

a. كان جهاز إنفاذ القانون قد نفذ تدابير الحماية التكنولوجية والتنظيمية المناسبة السارية على البيانات الشخصية التي انتُهكت، وبخاصة تلك التي تجعل البيانات الشخصية غير مفهومة لأي شخص غير مأذون له في الوصول إليها، مثل التشفير؛

b. اتخذ جهاز إنفاذ القانون لاحقا تدابير معينة للتخفيف من المخاطر المحتمل أن يخلفها هذا الانتهاك على حقوق الأشخاص موضوع البيانات وحرياتهم؛

c. كان ذلك يقتضي جهودا مفرطة. وفي هذه الحال، ينبغي لجهاز إنفاذ القانون بدلا من ذلك إصدار بلاغ عام أو اتخاذ تدبير على نفس القدر من الفعالية لإبلاغ الأشخاص موضوع البيانات بالانتهاك.

3. يمكن تأخير إبلاغ الشخص موضوع البيانات بالانتهاك أو وضع سقف له أو حجبه إذا ما تبيّن، بعد إيلاء الاعتبار الواجب لحقوق الشخص الطبيعي المعني الأساسية ومصالحه المشروعة، أن ذلك ضروري ومعقول من أجل: :

a. تفادي عرقلة التحريات أو التحقيقات أو الملاحقات الرسمية أو القضائية؛

b. تفادي إعاقة منع الجرائم الجنائية أو كشفها أو التحقيق فيها أو ملاحقة مرتكبيها، أو تنفيذ العقوبات الجنائية؛

c. حماية الأمن العام؛

d. حماية الأمن الوطني؛

e. حماية حقوق الآخرين وحرياتهم.

بشأن إبلاغ أشخاص موضوع البيانات وهيئة حماية البيانات بانتهاك البيانات المتعلقة بهؤلاء الأشخاص

النيابة العامة البريطانية (Crown Prosecution Service - CPS)، غرامة مالية فرضها مكتب مفوض المعلومات (ICO، 14 أيار/مايو 2018)

أرسلت الشرطة إلى CPS أقراص فيديو رقمية تحتوي على مقابلات مع ضحايا اعتداء جنسي على أطفال، اختفت بعد تسليمها. وأُبلغ الأشخاص موضوع البيانات وهيئة حماية البيانات بذلك. ولم تكن الأقراص الرقمية مشفرة مع أن النيابة العامة كانت قادرة على تشفيرها، ولم تكن الطرود التي نُقلت فيها محمية بحيث لا يمكن التلاعب بها. وخلصت هيئة حماية البيانات إلى ما يلي:

- لم تتسبب CPS عمدا باختفاء الأقراص ولكن كان عليها أن تُدرك احتمال اختفائها؛
- تعاملت CPS سابقا مع هذا النوع من المقابلات وسبق أن ارتكبت انتهاكا مماثلا من حيث عجزها عن توفير الحماية المناسبة لتسجيلات ضحايا وشهود في قضايا اعتداءات جنسية؛
- •لم تتخذ CPS التدابير الكافية لمنع اختفاء الأقراص، مثل القيام، بعد تشفيرها في طرود مختومة لا يمكن التلاعب بها، بنقلها عن طريق شركة مأمونة تشترط توقيعا عند الاستلام، وبوضع الأقراص التي سُلمت في مكان آمن؛
- لم تبادر CPS على الفور إلى إبلاغ الأشخاص موضوع البيانات بالانتهاك؛
- لم تبادر CPS على الفور إلى إبلاغ هيئة حماية البيانات بالانتهاك كما كان ينبغي لها أن تقوم به؛
- لم تسارع CPS إلى إبلاغ مستويات الإدارة المختصة بالمشكلة؛
- لم يُعثَر بعد على الأقراص الرقمية.

فرض مكتب مفوض المعلومات غرامة مالية قدرها 200 000 جنيه إسترليني.

الإبلاغ بانتهاك البيانات

1. إبلاغ هيئة حماية البيانات والأشخاص موضوع البيانات في حال انتهاك البيانات
2. إطلاع هيئة حماية البيانات والأشخاص موضوع البيانات على التدابير المتخذة أو المقترح اتخاذها لمعالجة انتهاك البيانات الشخصية
3. المسارعة إلى إبلاغ هيئة حماية البيانات والشخص موضوع البيانات بانتهاك البيانات الشخصية

معاملة السجلات وحفظ البيانات

7.1 سجلات بعمليات معاملة البيانات

1. ينبغي لأجهزة إنفاذ القانون الاحتفاظ بسجلات لجميع فئات عمليات معاملة البيانات المشمولة بمسؤوليتها بما فيها:
   a. اسم وطريقة الاتصال بالشخص المسؤول (الأشخاص المسؤولين) عن المنظومة في البلد والموظف المكلف بحماية البيانات؛
   b. الغرض من معاملة البيانات؛
   c. فئات الجهات التي كُشف لها عن البيانات الشخصية أو سيُكشَف لها عنها، بما فيها الجهات الموجودة في بلدان ثالثة أو في منظمات دولية؛
   d. وصف لفئات الأشخاص موضوع البيانات وفئات البيانات الشخصية؛
   e. استخدام تحديد المواصفات والصفات، عند الاقتضاء؛
   f. عند الاقتضاء، فئات إحالات البيانات الشخصية إلى بلد ثالث أو منظمة دولية؛
   g. الإشارة إلى الأساس القانوني للمعاملة المخصصة لها البيانات الشخصية، بما في ذلك الإحالات؛
   h. المهل الزمنية المقررة لحذف مختلف فئات البيانات الشخصية، عند الإمكان؛
   i. وصف عام لتدابير الأمن التقنية والتنظيمية السارية على المنظومة، عند الإمكان.

7.2 الملفات

1. ينبغي لأجهزة إنفاذ القانون الاحتفاظ بملفات عن عمليات المعاملة التالية:
   a. جمع البيانات؛
   b. تغييرها؛
   c. الوصول إليها/الاطلاع عليها؛
   d. الكشف عنها بما في ذلك إحالتها؛
   e. دمجها في إطار واحد؛
   f. حذفها.

2. في حال الاطلاع على بيانات شخصية أو الكشف عنها، ينبغي أن تتيح ملفات العمليات ذات الصلة تبيان الدافع وراء هاتين العمليتين وتاريخ ووقت إجرائهما وتحديد هوية الشخص الذي اطلع على هذه البيانات أو كشف عنها وهوية الشخص الذي تلقّاها.

3. لا ينبغي استخدام ملفات العمليات إلا للتحقق من مدى قانونية المعاملة وللمراقبة الذاتية وكفالة سلامة وأمن البيانات الشخصية وللإجراءات الجنائية. وينبغي لأجهزة إنفاذ القانون وضع هذه الملفات بتصرف هيئة حماية البيانات عند الطلب.

4. لا ينبغي أن يقيّم ملفات العمليات إلا شخص يضطلع بدور "المدقق" المعتمد في المنظومة، وذلك عن طريق هذه المنظومة لا غير.

5. يمكن تعديل الملفات أو حذفها وفقا للسياسات و/أو أفضل الممارسات المقبولة.

7.3 الاحتفاظ بالبيانات

1. ينبغي لأجهزة إنفاذ القانون وضع قواعد و/أو توصيات داخلية تحدد فترة الاحتفاظ بالبيانات الشخصية أو تنص على مراجعة دورية لمدى الحاجة إلى تخزين هذه البيانات.

2. ينبغي لأجهزة إنفاذ القانون أن تراجع دوريا أسباب الاحتفاظ بالبيانات الشخصية ومعاملتها.

3. لتحديد الفترة المناسبة للاحتفاظ بالبيانات الشخصية في المنظومة، ينبغي لأجهزة إنفاذ القانون:
   a. مراجعة طول فترة الاحتفاظ بالبيانات الشخصية استنادا إلى التشريعات الوطنية السارية وطبيعة البيانات والسياسات التي تتبعها وأفضل الممارسات؛
   b. النظر في الغرض المحدد للمعلومات قبل أن تقرر ما إذا كانت ستحتفظ بالبيانات الشخصية (وإلى متى)؛
   c. القيام بشكل مأمون بحذف المعلومات التي لم تعد ضرورية للأغراض المحددة؛
   d. تحديث المعلومات أو وضعها في المحفوظات أو حذفها بشكل مأمون إذا أصبحت قديمة.

4. لا ينبغي الاحتفاظ بالبيانات التي تعامَل في المنظومة إلا للفترة التي تحتاج إليها أجهزة إنفاذ القانون المعنية لتحقيق الغرض منها.

دراسة حالة

الاحتفاظ بالبيانات

Brunet ضد فرنسا، حكم المحكمة الأوروبية لحقوق الإنسان، 18 آب/أغسطس 2014، الطلب رقم 10/21010

وُضع السيد Brunet قيد الاحتجاز بعد وقوع مشادة عنيفة بينه وبين شريكته. وكتب الاثنان إلى المدعي العام للإعراب عن عدم موافقتهما على التهم فأُسقطت التهم الجنائية. إلا أن بيانات السيد Brunet الشخصية حُفظت في قاعدة البيانات على خلفية هذه المشادة وتقرر إبقاؤها فيها لمدة 20 عاما. وبعد أن حاول السيد Brunet عدة مرات الدفع باتجاه حذف بياناته الشخصية من قاعدة البيانات لكن بدون أي نتيجة، أبلغه المدعي العام بأنه لا يعرف ما إذا كان في الإمكان حذفها من قاعدة البيانات.

واعتبرت المحكمة أن قاعدة البيانات تتضمن معلومات ومواصفات شخصية لأغراض التحري عن الجرائم، وبالتالي فإن الاحتفاظ بمعلومات عن السيد Brunet فيها لمدة 20 عاما هو أمر مبالَغ فيه ولا سيما في ضوء إسقاط التهم وعدم الشروع في أي إجراءات جنائية ضده. وبالإضافة إلى ذلك، لم يُعطَ السيد Brunet فرصة حقيقية لطلب حذف البيانات المتعلقة به لأن المدعي العام لم يكن قادرا على بحث مدى ملاءمة الاحتفاظ بها.

أفضل الممارسات

الاحتفاظ بالبيانات

1. وضع قواعد و/أو توصيات داخلية تحدد فترة الاحتفاظ بالبيانات الشخصية أو تنص على مراجعة دورية لمدى الحاجة إلى تخزين هذه البيانات
2. ينبغي لأجهزة إنفاذ القانون أن تراجع دوريا أسباب الاحتفاظ بالبيانات الشخصية ومعاملتها
3. التأكد من أنه لا يتم الاحتفاظ بالبيانات إلا للفترة التي تحتاج إليها أجهزة إنفاذ القانون المعنية لتحقيق الغرض منها

الفصل الثامن

معاملة البيانات الحساسة

8.1 معاملة البيانات الحساسة

1. البيانات الشخصية التي تكشف الانتماء العرقي أو الإثني أو الأصل الجغرافي أو النسب أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية النقابية أو الحياة الجنسية أو البيانات الوراثية أو بشكل أعم البيانات المتصلة بالحالة الصحية لأي شخص ("البيانات الحساسة") لا ينبغي معاملتها في المنظومة إلا عند الضرورة القصوى، شريطة منح الضمانات اللازمة لحماية حقوق الشخص موضوع البيانات وحرياته، وحصريا:
   a. إذا كان معاملة البيانات الحساسة تجيزها لوائح الجماعة الاقتصادية لدول غرب إفريقيا أو لوائح البلد المشارك في واديس؛ أو
   b. لحماية المصالح الحيوية للشخص موضوع البيانات أو لشخص طبيعي آخر؛ أو
   c. إذا كانت المعاملة تتعلق ببيانات كشف عنها الشخص المعني.

دراسة حالة

عن معاملة بيانات حساسة

شرطة همبرسايد، غرامة مالية فرضها مكتب مفوض المعلومات، 28 آذار/مارس 2018

لم تستطع الشرطة العثور على ثلاثة أقراص فيديو مدمجة تحتوي على مقابلة مع ضحية اغتصاب مفترضة. وكانت هذه الأقراص النسخة الوحيدة وكانت تتضمن بيانات حساسة وشخصية عن الضحية المفترضة والجاني المزعوم، شملت اسميهما الكاملين وتاريخ ولادتهما، والحالة النفسية للضحية المفترضة والعلاج الذي تخضع له. والملاحظات المكتوبة التي لا نسخة أخرى منها وتضمنت تفاصيل المقابلة كانت موجودة مع الأقراص. ولم يُكتشَف اختفاء الأقراص إلا بعد 14 شهرا من المقابلة. وقد أُبلغت الضحية بذلك ورفضت المشاركة في أي مقابلات أخرى مع الشرطة. ولم يُعثَر على الأقراص. وخلصت هيئة حماية البيانات إلى ما يلي:

- لم تتأكد الشرطة من أن الأقراص كانت مشفرة لنقلها إلى خارج مكاتبها؛
- لم تعِدّ الشرطة نسخا من الأقراص قبل نقلها إلى خارج مكاتبها؛
- لم تتقيد الشرطة بالسياسات التي تحكم أمن المعلومات؛
- لم تحتفظ الشرطة بدليل يتابع مكان الأقراص؛

- لم توفر الشرطة لأفرادها برنامج تدريب ومتابعة مناسبا في مجال حماية البيانات؛
- لم تقم الشرطة بتمتين السياسات والآليات المعتمدة حاليا في مجال تخزين البيانات وإحالتها.

وفرض مكتب مفوض المعلومات غرامة مالية قدرها 130 000 جنيه إسترليني.

معالجة البيانات الحساسة

1. احترام حقوق الأشخاص موضوع البيانات وحرياتهم قبل جمع بيانات حساسة
2. تمتين السياسات المعتمدة حاليا في مجال أمن البيانات الحساسة.

أفضل الممارسات

الفصل التاسع

حقوق الأشخاص موضوع البيانات

9.1 الحق في الوصول إلى البيانات

1. عندما تُعامَل في المنظومة بيانات شخص ما لأغراض إنفاذ القانون، ينبغي لجهاز إنفاذ القانون، بمجرد أن تسمح الظروف بذلك بشكل مأمون، أن يأذن للشخص موضوع البيانات، بناء على طلبه، في الوصول المباشر أو غير المباشر إلى البيانات، شريطة التقيد بالإطار القانوني الساري.

2. وبالنسبة للوصول المباشر إلى البيانات، يمكن للشخص موضوع البيانات أن يقدم طلبه مباشرة إلى جهاز إنفاذ القانون المسؤول عن البيانات. وينبغي لهذا الجهاز النظر في الطلب وفي أي قيود محتملة أو استثناءات لا يمكن تطبيقها إلا إذا كان ذلك لازما لأغراض إنفاذ القانون أو لحماية الشخص موضوع البيانات أو حقوق الآخرين وحرياتهم، والرد مباشرة على الشخص موضوع البيانات.

3. وبالنسبة للوصول غير المباشر إلى البيانات، ينبغي للشخص موضوع البيانات تقديم طلبه إلى هيئة حماية البيانات التي يمكنها متابعته بالنيابة عنهم والتحقق من قانونية معاملة البيانات الشخصية للشخص المعني ومن توفرها. ويمكن لهيئة حماية البيانات بعدئذ الرد على الشخص موضوع البيانات بالشكل المناسب.

4. وعندما لا يكون حاليا لدى بلد مشارك في منظومة وابيس هيئة لحماية لبيانات أو هيئة للإشراف عليها وحتى تشكيل هذه الهيئة، ينبغي، شريطة التقيد بالإطار القانوني الساري، أن يكون الحق في الوصول إلى البيانات مباشرا.

5. وعندما يكون حاليا لدى بلد مشارك في منظومة وابيس هيئة لحماية البيانات يجيز إطارها القانوني للشخص موضوع البيانات ممارسة الحق في الوصول غير المباشر إلى بياناته الشخصية عن طريق هذه الهيئة، يمكن أن يكون الحق في الوصول المباشر إلى البيانات محدودا.

6. وعند الاقتضاء وإذا كان ذلك متناسبا، يمكن أن يكون وبشكل استثنائي الحق في الوصول إلى البيانات محدودا أو غير ممنوح كليا أو جزئيا، وفقا للإطار القانوني الساري، من أجل:

   a. تفادي عرقلة التحريات أو التحقيقات أو الملاحقات الرسمية أو القضائية؛
   b. تفادي إعاقة منع الجرائم الجنائية أو كشفها أو التحقيق فيها أو ملاحقة مرتكبيها، أو تنفيذ العقوبات الجنائية؛
   c. حماية حقوق وحريات الآخرين؛
   d. عدم تعقيد أي تحقيقات أو ملاحقة قضائية أو مهمة بارزة أخرى لإنفاذ القانون؛
   e. حماية مصالح الدولة (مثل الأمن العام والأمن الوطني).

7. وعندما يكون الحق في الوصول إلى البيانات محدودا أو غير ممنوح، يتعين على جهاز إنفاذ القانون المعني أو هيئة حماية البيانات المعنية إبلاغ الشخص موضوع البيانات خطيا وبدون تأخير لا مبرر له، بأسباب رفض طلبه الوصول إلى البيانات أو الوصول إليها بشكل محدود. ويمكن القفز عن هذه الأسباب عندما يُخشى أن يمس سَوْقها أحد الأغراض الواردة في الفقرة 6 أعلاه. وينبغي لجهاز إنفاذ القانون إبلاغ الشخص موضوع البيانات بأن في وسعه تقديم شكوى إلى هيئة حماية البيانات أو اللجوء إلى القضاء، بحسب الحالة.

8. وينبغي، من حيث المبدأ، أن يكون الحق في الوصول إلى البيانات مجانيا. ويمكن فرض رسم إداري معقول على الطلب إذا سمح القانون الوطني بذلك.

9. وينبغي لجهاز إنفاذ القانون أن يحدد في سياسة أو إشعار مهلة معقولة لبحث طلبات الوصول إلى البيانات.

عن الحق في الوصول إلى البيانات

Segerstedt-Wiberg وآخرون ضد السويد، حكم المحكمة الأوروبية لحقوق الإنسان، 6 حزيران/يونيو 2006، الطلب رقم 00/62332

حاول مقدمو الطلب في هذه الحالة الوصول إلى بياناتهم الشخصية الواردة في ملفات شرطة الأمن السويدية. وتتعلق القضية بخمسة أفراد هم SEGERSTEDT-WIBERG وNYGREN وEHNEBOM و FREJD وSCHMID. واستندت الحكومة السويدية إلى قانون عام 1980 المتعلق بالسرية لحجب المعلومات محتجة بأنه «ليس ما يؤكد أنه يمكن كشف المعلومات بدون التأثير سلبا في الغرض المنشود من القرار أو التدابير المقررة أو الأنشطة المستقبلية».

كانت السيدة SEGERSTEDT-WIBERG عضوا بارزا في البرلمان عن الحزب الليبرالي وطلبت الوصول إلى ملفات الشرطة بعد نشر معلومات عنها أضرت بها، من بينها شائعات بأنها «غير موثوقة» من حيث العلاقة مع الاتحاد السوفياتي. وكشفت الشرطة جميع المعلومات المتعلقة بالمذكورة حتى عام 1976، ولكنها أبقت على القيود المفروضة على بقية الملف بسبب التهديدات المستمرة ضدها. وأقرت المحكمة بأن الاحتفاظ بهذه المعلومات كان لغرض مشروع (منع الاضطرابات أو الجريمة) ولم تجد أي سبب للتشكيك في قرار الدولة القاضي بحجب المعلومات عنها في ضوء التهديدات التي تستهدف أمنها (مثلا، تهديد بتفجير قنبلة في عام 1990).

كان السيد NYGREN صحافيا كتب عددا من المقالات عن النازية وشرطة الأمن السويدية. وسُمح له بالاطلاع على صفحتين من ملفه ورُفض طلبه الاطلاع على بقية الملف. واعتبرت المحكمة أن طبيعة المعلومات المتعلقة به وقِدَمها لا يبرران استمرار الاحتفاظ بها بداعي حماية الأمن الوطني.

كان السيد EHNEBOM عضوا في حزب شيوعي. ومُنِح حق الاطلاع على 30 صفحة من ملفه وادعى أن المعلومات الواردة فيها هي المسؤولة عن صرفه من الخدمة. وكان السيد FREJD أيضا عضوا في حزب شيوعي وكان معروفا في الأوساط الرياضية في جميع أنحاء السويد. وأُذن له في الاطلاع على أجزاء من ملفه تتعلق بانتمائه إلى الحزب، بما في ذلك محاولته أن يُنتخَب كعضو فيه. إلا أنه مُنع من الاطلاع على مجمل ملفه. وبالنسبة لكلتا القضيتين، أقرت المحكمة بأن الرجلين كانا ينتميان إلى منظمة تناصر المعارضة المسلحة وتشكيل مجموعة معينة بدلا من أخرى، لكن كان هذا الأمر الدليل الوحيد الذي استخدمته الحكومة لتبرير الاحتفاظ بالبيانات الشخصية.

كان السيد SCHMID عضوا في البرلمان الأوروبي وينتمي إلى حزب اليسار السويدي. وسُمح له بالاطلاع على ملفات مختارة متعلقة بحركات سياسية ذات صلة بنزع السلاح النووي والانتماء إلى مجموعات اشتراكية ديمقراطية. واعتبرت المحكمة أنه لا يوجد سبب للاحتفاظ بالملف أو الاطلاع على أجزاء منه إليه لمصلحة الأمن الوطني السويدي، وأن المضي في الاحتفاظ بالمعلومات هو بالتالي مبالغٌ فيه قياسا بأهداف القانون المشروعة.

9.2 الحق في تصحيح البيانات الشخصية أو حذفها

1. يحق للأشخاص موضوع البيانات أن يطلبوا بشكل مباشر أو غير مباشر من أجهزة إنفاذ القانون تصحيح أو حذف بيانات شخصية غير دقيقة متعلقة بهم ومسجلة في وابيس، وفقا للإطار القانوني الساري للبلد المشارك في هذه المنظومة. ويمكن لهؤلاء الأشخاص أن يطلبوا أيضا تكملة البيانات الشخصية الناقصة.

2. بالنسبة لممارسة هذا الحق بشكل مباشر، يمكن للشخص موضوع البيانات أن يقدم طلب تصحيح البيانات الشخصية أو حذفها مباشرةً إلى جهاز إنفاذ القانون المسؤول عنها. وينبغي لهذا الجهاز النظر في الطلب وفي أي قيود محتملة أو استثناءات لا يمكن تطبيقها إلا إذا كان ذلك لازما لأغراض إنفاذ القانون أو لحماية الشخص موضوع البيانات أو حقوق الآخرين وحرياتهم، والرد مباشرة على الشخص موضوع البيانات.

3. بالنسبة لممارسة هذا الحق بشكل غير مباشر، ينبغي للشخص موضوع البيانات تقديم طلب تصحيح البيانات الشخصية أو حذفها إلى هيئة حماية البيانات التي يمكن أن تتابع الطلب بالنيابة عنهم والتحقق من إمكانية وقانونية معاملة البيانات الشخصية للشخص المعني. ويمكن لهيئة حماية البيانات بعدئذ الرد على الشخص موضوع البيانات بالشكل.

4. وعندما لا يكون حاليا لدى بلد مشارك في منظومة وابيس هيئة لحماية البيانات، ينبغي، شريطة التقيد بالإطار القانوني الساري، أن يمارَس الحق في طلب تصحيح البيانات الشخصية أو حذفها مع جهاز إنفاذ القانون مباشرة.

5. وعندما يكون حاليا لدى بلد مشارك في منظومة وابيس هيئة لحماية البيانات أو هيئة للإشراف عليها يجيز إطارها القانوني للشخص موضوع البيانات ممارسة الحق في طلب تصحيح البيانات الشخصية أو حذفها بشكل غير مباشر عن طريقها، يمكن أن يكون الحق في طلب تصحيحها أو حذفها محدودا.

6. وبدلا من حذف البيانات، ينبغي لأجهزة إنفاذ القانون معاملتها بشكل محدود عندما:
   a. يطعن الشخص موضوع البيانات في دقتها ويتعذر تأكيد هذه الدقة أو عدمها؛
   b. يجب الاحتفاظ بالبيانات الشخصية لأغراض تقديم الأدلة.

7. وينبغي لجهاز إنفاذ القانون أو هيئة حماية البيانات، حسب الحالة، إبلاغ الشخص موضوع البيانات خطيا بأي رفض لتصحيح بياناته الشخصية أو حذفها أو معاملتها بشكل محدود وأسباب هذا الرفض.

8. ووفقا للقوانين السارية، يجوز لجهاز إنفاذ القانون أن يقلص، كليا أو جزئيا، واجبه من حيث توفير هذه المعلومات بقدر ما يكون هذا التقليص ضروريا ومتناسبا، مع إيلاء الاعتبار الواجب للحقوق الأساسية والمصالح المشروعة للشخص موضوع البيانات وللقوانين السارية، من أجل:
   a. تفادي عرقلة التحريات أو التحقيقات أو الملاحقات الرسمية أو القضائية؛
   b. تفادي إعاقة منع الجرائم الجنائية أو كشفها أو التحقيق فيها أو ملاحقة مرتكبيها، أو تنفيذ العقوبات الجنائية؛
   c. حماية حقوق وحريات الآخرين؛
   d. عدم تعقيد أي تحقيقات أو ملاحقة قضائية أو مهمة بارزة أخرى لإنفاذ القانون؛
   e. حماية مصالح الدولة (مثل الأمن العام والأمن الوطني).

9. وعند تصحيح جهاز لإنفاذ القانون بيانات شخصية أو حذفها أو معاملتها بشكل محدود، ينبغي له أن يُخطر بذلك جميع الجهات التي أحيلت إليها هذه البيانات وأن يطلب منها أن تحذو حذوه.

دراسة حالة

بشأن الحق في تصحيح بيانات شخصية

Khelili ضد سويسرا، حكم المحكمة الأوروبية لحقوق الإنسان، 18 تشرين الأول/أكتوبر 2011، الطلب رقم 07/16188

في عام 1993، سجلت شرطة جنيف في قاعدة بيانات الشرطة معلومات تتعلق بالسيدة Khelili تضمنت كلمة "بغيّ". وكان القانون يسمح للشرطة بالاحتفاظ بهذه المعلومات طالما كانت البيانات ضرورية لأداء مهامها (المعاقبة على الجرائم ومنع الجريمة). وفي الأعوام 2001 و2002 و2003، قُدمت بحق السيدة Khelili شكاوى جنائية أخرى بتهمة توجيه إهانات وتهديدات. واكتشفت السيدة Khelili في هذه الأثناء أن الشرطة احتفظت بكلمة "بغيّ" في ملفها. وفي عام 2006، طلبت حذف هذه الكلمة من سجلها وأبلغها رئيس الشرطة بأنها حُذفت. إلا أن هذه الكلمة، على الرغم من حذف سجل 1993، ظلت مرتبطة بالشكاوى المقدمة ضدها في الأعوام 2001 و2002 و2003.

وافقت المحكمة على أن إدراج كلمة "بغيّ" في ملف السيدة Khelili لدى الشرطة كان يشكل تدخلا بموجب القانون يرمي إلى منع الفوضى والجريمة وإلى حماية حقوق الآخرين. وهذه الكلمة، لئن حُذفت من قاعدة بيانات الشرطة كمهنة، لم تُحذف من التهم الجنائية المتعلقة بالشكاوى الجنائية الأخرى المرفوعة ضدها ويمكنها أن تشوه سمعتها في الدوائر الخاصة والعامة. ونظرت المحكمة أولا في مسألة أن التهم بالدعارة ضبابية وعامة، وأن العلاقة بين ملف عام 1993 وتهم الأعوام 2001 و2002 و2003 ليست وثيقة بالقدر الكافي. ومن ثم لاحظت أن الشرطة حذفت كلمة "بغيّ" من جزء من ملف السيدة المذكورة لا منه بأكمله، بينما أبلغتها بأنها شطبت هذه الكلمة من كل الملف. وهكذا فإن الشرطة كانت تحتفظ ببيانات كاذبة عن السيدة Khelili، وإبقاء كلمة "بغيّ" في ملفها ليست مبررة ولا ضرورية في مجتمع ديمقراطي.

أفضل الممارسات

حقوق الأشخاص موضوع البيانات

1. احترام ممارسة الأشخاص المعنيين لحقهم في الوصول إلى بياناتهم
2. احترام ممارسة حق تصحيح وحذف البيانات الشخصية غير الدقيقة المسجلة في المنظومة

الفصل العاشر

تقييم نتائج حماية البيانات

10.1 تقييم نتائج حماية البيانات

1. ينبغي لأجهزة إنفاذ القانون تقييم نتائج حماية البيانات وتوثيقه لتسجيل المخاطر التي تم تبيانها والتدابير التي نُفذت لمعالجتها.

2. (وعند الضرورة، يجب تقييم نتائج حماية البيانات قبل وضع المنظومة حيّز التطبيق وبعد ذلك على فترات زمنية منتظمة.

3. وينبغي أن يحدد تقييم النتائج ويأخذ في الاعتبار ما يلي:
   a. معلومات عن البيانات التي ستعامَل أو الخاضعة للمعاملة؛
   b. الأشخاص أو فئة الأشخاص الذين ستعامَل بياناتهم أو الخاضعة للمعاملة؛
   c. طريقة المعاملة، بما يشمل جدولا زمنيا لمسار البيانات بدءا من جمعها وانتهاء بحذفها؛
   d. المخاطر المرتبطة بمعاملة البيانات الشخصية؛
   e. التدابير المتخذة لمعالجة المخاطر التي تم تبيانها؛
   f. الأنظمة/الواجبات القانونية السارية، إن وجدت؛
   g. التوجيهات التي تعطيها هيئة حماية البيانات؛
   h. أي مخاطر أخرى تتعذر معالجتها أو تدابير لا يمكن تنفيذها ومبررات هذه المخاطر وقبولها.

4. لأغراض تقييم نتائج حماية البيانات، ينبغي لأجهزة إنفاذ القانون وضع نهج مستند إلى المخاطر وتطبيقه على برنامج حماية البيانات في وابيس وذلك استنادا إلى أفضل الممارسات وإلى المخاطر التي ينطوي عليها عدم التقيد بالقوانين والأنظمة. وتحقيقا لهذه الغاية، ينبغي لأجهزة إنفاذ القانون:
   a. فهم المخاطر التي تتعرض لها حماية البيانات في وابيس، وأهدافها التنظيمية الشاملة، وثقافتها ولغتها وعملياتها؛
   b. تحديد المجالات التي يُحتمَل أن يتم فيها جمع البيانات الشخصية أو معاملتها أو استخدامها في وابيس؛
   c. استنادا إلى ما تم تبيانه من مخاطر تتعرض لها حماية البيانات، تحديد أولويات حماية البيانات لتتوافق مع أهدافها العامة.

تقييم النتائج

1. تقييم نتائج حماية البيانات قبل وضع المنظومة حيّز التطبيق وبعد ذلك على فترات زمنية منتظمة
2. التحقق من مدى احتمال أن تستتبع معاملة البيانات الشخصية خطرا شديدا على حقوق الأشخاص موضوع البيانات وحرياتهم

الفصل الحادي عشر

الاستثناءات

11.1 الاستثناءات من معاملة البيانات وفقا لهذا الدليل

1. لا ينبغي اللجوء إلى الاستثناء من معاملة البيانات وفقا لهذا الدليل إلا إذا:
   a. كان منصوصا عليه صراحة في القانون؛
   b. كان يشكل تدبيرا ضروريا لأغراض حماية الأمن الوطني، والدفاع، والأمن العام، والمصالح الاقتصادية والمالية الكبرى، ونزاهة القضاء واستقلاليته، ومنع الجرائم الجنائية والتحقيق فيها ومقاضاة مرتكبيها، وتنفيذ العقوبات الجنائية، وحماية أهداف أساسية ذات مصلحة عامة، أو حماية حقوق الآخرين وحرياتهم الأساسية، ومتناسبا مع هذه الأغراض.
2. إذا طلبت أجهزة إنفاذ القانون استثناء يحدده القانون الوطني مع منح ضمانات محددة، لا ينبغي استخدامه إلا لأغراض مشروعة وفقط بالقدر الضروري لتحقيق الهدف المتوخى منه وبطريقة متناسبة مع تحقيقه. وطلب أجهزة إنفاذ القانون استثناءات ينبغي أن يقتصر على الحالات التي يؤدي فيها عدم طلبها إلى المس بغرض إنفاذ القانون المنشود من معاملة البيانات.

الفصل الثاني عشر

خاتمة

ليس الغرض من هذه الوثيقة أن تكون بمثابة مقام قانون أو لائحة قانونية، بل هي وثيقة مرجعية وُضعت لتسترشد بها أجهزة إنفاذ القانون لتطبيق مبادئ حماية البيانات التي يقتضيها القانون، أو استخدامها كآلية للتنظيم الذاتي في الحالات التي لا يوجد فيها قانون لحماية البيانات. وحسن تنفيذها سيتيح للبلدان المشاركة في منظومة وابيس تبنّي أفضل الممارسات التي تسهّل تبادل المعلومات واستخدام هذه المنظومة إلى أقصى حد ممكن. ويمكنها أيضا توجيه كيفية حماية البيانات خارج المنظومة ليشمل العمليات العامة التي تضطلع بها أجهزة إنفاذ القانون.

أبرز النقاط للحفظ

مقدمة

وقّع رؤساء دول وحكومات الدول الأعضاء في المجموعة الاقتصادية لدول غرب أفريقيا (ECOWAS) القانون الإضافي Supplementary Act A/SA.1/01/10 ('القانون') المتعلق بحماية البيانات الشخصية داخل المجموعة الاقتصادية في 16 شباط/فبراير 2010.

إن القانون:

- يحدد المبادئ الأساسية السارية على معاملة البيانات الشخصية في منظومة المعلومات الشرطية لغرب أفريقيا (وابيس)؛
- يدعو البلدان الأعضاء إلى سن تشريعات بشأن حماية البيانات وإنشاء هيئة لحماية البيانات.

الفصل الأول – مصطلحات عامة

يقدم الفصل الأول نظرة عامة عن المصطلحات المستخدمة في الدليل. ويحدد:

- مَن يتعين عليه التقيد بالقانون؟ المتحكمون بالبيانات ومعاملوها.
- مَن يتلقى البيانات؟ الجهات متلقّية البيانات.
- مَن هم المعنيون بعمليات معاملة البيانات الشخصية؟ الأشخاص موضوع البيانات.
- ما هو نوع البيانات التي يحكمها القانون؟ البيانات الشخصية.

الفصل الثاني – المبادئ والأغراض

يعرض الفصل الثاني المبادئ العامة التي تحكم حماية البيانات الشخصية والأسباب المشروعة التي لدى أجهزة إنفاذ القانون لمعاملة هذه البيانات.

2.1 – مبادئ حماية البيانات الشخصية

تتضمن مبادئ الحماية ما يلي:

المشروعية	الشرعية والإنصاف	الغرض والأهمية والاحتفاظ	الدقة
الشفافية	السرية والأمن	اختيار معامل البيانات	

2.2 – الأغراض من معاملة البيانات في المنظومة

ينبغي لأجهزة إنفاذ القانون أن تتكون مدركة تمام الإدراك للحالات التي يمكنها فيها معاملة بيانات في وابيس. والأغراض التي لأجلها يمكنها معاملتها هي التالية:

- منع ارتكاب الجرائم أو التحقيق فيها أو الكشف عنها أو مقاضاة مرتكبيها؛
- تنفيذ العقوبات؛
- صون النظام العام؛
- حماية الأمن العام من الأخطار التي تتهدده ومنعها؛
- أداء أجهزة إنفاذ القانون أي مهمة أو مسؤولية يمليها عليها القانون.

الفصل الثالث – نظام حماية البيانات وإدارتها

يتناول الفصل الثالث هيئات حماية البيانات، والتوعية والتدريب في مجال حماية البيانات، ومسألة التقيد بشروط معاملة البيانات بصورة عامة..

3.1 – المراقبة والإبلاغ

ينبغي لجميع البلدان المشاركة في منظومة وابيس إنشاء هيئة مستقلة لحماية البيانات تكون مسؤولة عن عمليات معاملة البيانات.

3.2 – الموظف المعني بحماية البيانات والتدريب والتوعية في مجال حماية البيانات

ينبغي لأجهزة إنفاذ القانون تعيين موظف معني بحماية البيانات ليقوم بما يلي:

- إطلاع أجهزة إنفاذ القانون على واجباتها القانونية؛
- التحقق من مدى التقيد بشروط معاملة البيانات؛
- تقديم المشورة بشأن تقييم نتائج حماية البيانات؛
- التنسيق مع هيئات حماية البيانات؛
- تنظيم برنامج تدريب مناسب ودائم لمستخدمي منظومة وابيس.؛

3.3 – التقيد بمبادئ معاملة البيانات وحمايتها

ينبغي لأجهزة إنفاذ القانون دمج حماية البيانات في صلب هيكليات إدارتها عبر إشراك أصحاب المصلحة الرئيسيين في تنفيذ إطار حماية البيانات التي تعامَل في هذه المنظومة.

الفصل الرابع – جمع البيانات الشخصية وتبادلها

يعرض الفصل الرابع أفضل الممارسات في مجال جمع البيانات الشخصية وتبادلها.

4.1 – جمع البيانات الشخصية

كقاعدة عامة، لا ينبغي أن تتجاوز البيانات الشخصية التي تُجمع في المنظومة ما يقتضيه تحقيق الغرض الذي تُجمع لأجله والمتناسب مع أغراض إنفاذ القانون التي تُجمع لأجلها.

4.2 – توفير البيانات لهيئات عامة أخرى أو إحالتها إليها.

بعد جمع البيانات الشخصية، يمكن لأجهزة إنفاذ القانون توفيرها لهيئات عامة أخرى (لا تشمل أجهزة إنفاذ القانون) إذا كان القانون يجيز توفيرها وكانت البيانات مطلوبة من الجهة المتلقّية ليتسنى لها أداء واجباتها القانونية.

4.3 – توفير البيانات لهيئات خاصة أو العموم أو إحالتها إليهما وللجمهور ولهيئات عامة.

بعد جمع البيانات الشخصية، يمكن لأجهزة إنفاذ القانون توفيرها لهيئات خاصة إذا كان ذلك، في إطار إنفاذ القانون، ضروريا لدرء خطر جسيم ووشيك يتهدد الأمن العام؛ أو يخدم مصلحة الشخص موضوع البيانات؛ أو يتم لدواع إنسانية. وبعد جمع البيانات الشخصية، يمكن لأجهزة إنفاذ القانون توفيرها للعموم إذا كان الغرض منه تنبيههم، أو طلب المساعدة منهم، أو لأي غرض آخر من أغراض إنفاذ القانون.

4.4 – توفير البيانات على الصعيد الدولي.

بعد جمع البيانات الشخصية، يمكن لأجهزة إنفاذ القانون توفيرها لأجهزة إنفاذ قانون دولية أو لمنظمات دولية إذا: (a) كانت الجهة المتلقية تضطلع بمهمة موكلة إليها بموجب القانون لأغراض إنفاذ القانون؛ (b) كان توفير البيانات ضروريا لهذه الجهة لأداء مهام إنفاذ القانون المنوطة بها؛ (c) كان الجهاز الذي يوفر البيانات يضمن أن الجهة المتلقية تطبق مستوى كافيا من الحماية لأمن المعلومات في إطار معاملة هذه البيانات.

الفصل الخامس – نوعية البيانات وسريتها وأمنها

يقدم الفصل الخامس لمحة عامة عن نوعية البيانات وعن التدابير التي ينبغي لأجهزة إنفاذ القانون تنفيذها لضمان الحفاظ على سرية البيانات الشخصية وأمنها.

5.1 – نوعية البيانات

لا ينبغي لأجهزة إنفاذ القانون توفير بيانات شخصية غير دقيقة أو قديمة أو ناقصة. ويتعين عليها، إذا وُفِّرت بيانات شخصية غير دقيقة، الإسراع في إبلاغ الجهات المتلقّية بذلك واتخاذ الخطوات المناسبة لتصحيحها أو حذفها أو منع معاملتها.

5.2 – السرية والأمن

ينبغي لأجهزة إنفاذ القانون اتخاذ التدابير التقنية المناسبة والكافية لحماية المنظومة من مخاطر الوصول غير المقصود أو غير المأذون فيه إلى البيانات الشخصية أو إتلافها أو اختفائها أو استخدامها أو تغييرها أو الكشف عنها.

الفصل السادس – عمليات انتهاك البيانات

يحدد الفصل السادس الخطوات المناسبة التي ينبغي أن تتخذها أجهزة إنفاذ القانون عند انتهاك بيانات.

انتهاك البيانات

هيئة حماية البيانات

6.1 – الإبلاغ بانتهاك البيانات

ينبغي لأجهزة إنفاذ القانون توثيق حالات انتهاك البيانات وإبلاغ هيئة حماية البيانات بها بدون تأخير لا لزوم له، ويفضل أن يكون ذلك ضمن مهلة 72 ساعة من وقت انتهاكها.

الشخص موضوع البيانات

6.2 – إبلاغ الشخص موضوع البيانات بانتهاك البيانات

ينبغي لأجهزة إنفاذ القانون أيضا إبلاغ الأشخاص موضوع البيانات بدون تأخير إذا كان من المحتمل أن يؤدي انتهاك بياناتهم الشخصية إلى مس حقوقهم وحرياتهم.

الفصل السابع – معاملة السجلات والاحتفاظ بالبيانات

يعرض الفصل السابع أفضل الممارسات في مجالي تجهيز السجلات والاحتفاظ بالبيانات.

7.1 – سجلات أنشطة معاملة البيانات

ينبغي لأجهزة إنفاذ القانون امتلاك سجلات لجميع أنشطة معاملة البيانات.

7.2 – ملفات العمليات

ينبغي لأجهزة إنفاذ القانون أيضا إعداد ملفات للبيانات عن أنشطة معاملة البيانات التالية: (a) جمعها؛ و(b) تغييرها؛ و(c) الوصول إليها/ الاطلاع عليها؛ و(d) الكشف عنها، بما في ذلك إحالتها؛ و(e) دمجها في إطار واحد؛ و(f) حذفها.

7.3 – الاحتفاظ بالبيانات

ينبغي لأجهزة إنفاذ القانون الاحتفاظ بالبيانات لفترة مناسبة فقط.

الفصل الثامن – معاملة البيانات الحساسة

يشير الفصل الثامن إلى أن البيانات الحساسة أي [”البيانات الشخصية التي تذكر الانتماء العرقي أو الإثني أو الأصل الجغرافي أو النسب أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية النقابية أو الحياة الجنسية أو البيانات الوراثية أو يشكل أعم البيانات المتصلة بالحالة الصحية لأي شخص“ (الفصل 8.1، الفقرة 1)] لا يتعين معاملتها في منظومة وابيس إلا عند الضرورة القصوى.

الفصل التاسع – حقوق الأشخاص موضوع البيانات

يسلط الفصل التاسع الضوء على حقوق الأشخاص موضوع البيانات، أي حقهم في الوصول إلى بياناتهم أو تصحيحها أو حذفها.

9.1 – الحق في الوصول إلى البيانات و9.2 الحق في تصحيحها أو حذفها.

9.1 – الحق في الوصول إلى البيانات

إن الحق في الوصول إلى البيانات يتيح للشخص موضوع بيانات الوصول المباشر أو غير المباشر إلى البيانات المتعلقة به التي تعامَل في منظومة وابيس.

9.2 – الحق في تصحيح البيانات أو حذفها

إن الحق في تصحيح البيانات أو حذفها يجيز للشخص موضوع البيانات الطلب من سلطات إنفاذ القانون تصحيح أو حذف البيانات الشخصية غير الدقيقة المتعلقة به والمدرجة في وابيس.

الفصل العاشر – تقييم نتائج حماية البيانات

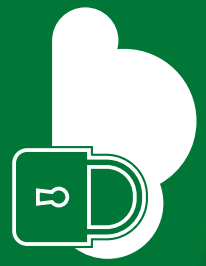
يناقش الفصل العاشر تقييم نتائج حماية البيانات، وهو آلية يمكن استخدامها لمساعدة أجهزة إنفاذ القانون على تبيان وتسجيل المخاطر التي ينطوي عليها وضع منظومة وابيس قيد الاستخدام. ويثبت هذا التقييم، إذا أُجري بحسب الأصول، أن هذه الأجهزة بحثت المخاطر التي تستتبعها معاملة البيانات المقررة وكذلك واجباتها الأوسع نطاقا على صعيد حماية البيانات.

الفصل الحادي عشر – الاستثناءات

يذكر الفصل الحادي عشر الحالات النادرة التي لا ينبغي فيها معاملة البيانات وفقا لهذا الدليل.

الفصل الثاني عشر – خاتمة

أخيرا، يلخص الفصل الثاني عشر الغرض الشامل من هذا الدليل ألا وهو تمكين البلدان المشاركة في منظومة وابيس من تبنّي ممارسات قانونية عند معاملة البيانات تسهّل إدارة المعلومات وتبادلها واستخدام هذه المنظومة العام إلى أقصى حد ممكن.



الإنتربول

المكتب الإقليمي للإنتربول في أبيدجان

ANNEXE
RUE E70, À PROXIMITÉ DE
L'ÉGLISE BON PASTEUR
RIVIERA 3 EECI, LOT 1199 ILOT 125
ABIDJAN
CÔTE D'IVOIRE

WWW.INTERPOL.INT

INTERPOLHQ WWW.INTERPOL.INT @INTERPOL_HQ