FRANCAIS	عربي
Vie privée et protection des données	**الحياة الخاصة وحماية البيانات**
Introduction (Inès CHOUK)	توطئة
La vie privée est un droit humain internationalement reconnu consacré dans la déclaration universelle des droits de l'Homme, le pacte international des droits civils et politiques et dans les constitutions de plus de 100 pays à travers le monde. La vie privée est non seulement un droit important en soi mais aussi un élément clé de l'autonomie et la dignité des personnes. C'est un levier pour garantir les libertés politiques, spirituelles, religieuses et même sexuelles. Elle est centrale pour définir la relation ainsi que l'interaction sociale. entre les citoyens et leur gouvernement.	تعد الحياة الخاصة حقا من حقوق الإنسان المعترف به دوليا، والمنصوص عليه في الإعلان العالمي لحقوق الإنسان، والعهد الدولي للحقوق المدنية والسياسية، ودساتير أكثر من 100 بلدا عبر أنحاء العالم. ولا تمثل الحياة الخاصة حقا مهما في حد ذاته فحسب، وإنما هو أيضا عنصرا أساسيا للاستقلالية الفردية والكرامة، ودعما للحريات السياسية والروحية والدينية وحتى الجنسية. كما أنه أساسي لتحديد العلاقة والتفاعل الاجتماعي بين المواطنين وحكوماتهم.
Les technologies de l'information ont rendu possible la collecte, le stockage, le partage et l'analyse des données par des moyens jusqu'ici inimaginables. De même, le droit à la vie privée a évolué pour intégrer un droit à la protection des données personnelles. Le concept de protection des données implique que les individus aient le droit de décider ce qu'il veulent partager ou échanger comme informations personnelles et sous quelles conditions ils vont le faire. Les lois sur la protection des données comprennent généralement des garanties de protection quant à la sécurité des données personnelles et quant à leur utilisation conditionnée.	بما أن تكنولوجيا المعلومات جعلت من الممكن جمع البيانات وتخزينها وتقاسمها وتحليلها بصفة يصعب تخيلها سابقا، فقد تطور الحق في الحياة الخاصة ليشمل حماية البيانات الشخصية. [1] و يعني مفهوم حماية البيانات أن للأفراد الحق في أن يقرروا بخصوص تقاسم أو تبادل المعلومات الشخصية من عدمه، وأسسه. وتحتوي قوانين حماية البيانات بصفة عامة ضمانات تحمي سلامة البيانات الشخصية ولا تسمح باستخدامها من قبل الغير إلا في الحالات المنصوص عليها.
Les droits à la vie privée et à la protection des données ont une incidence sur une multitude d'institutions gouvernementales, qu'elles recueillent des données sur les citoyens et les stockent ou qu'elles les régulent. En particulier, la police et les services de sécurité publique	يؤثر الحق في الحياة الخاصة وفي حماية البيانات على العديد من المؤسسات الحكومية، سواء منها تلك التي تجمع وتمسك البيانات

ont des responsabilités qui engendrent inéluctablement une intrusion dans la sphère privée. C'est le cas quand ils ont des objectifs plus larges impliquant la justice pénale ou la protection de la sécurité nationale. Les fonctions de la police et des agences de sécurité peuvent toucher des questions relatives à la vie privée pour les recherches, les pouvoirs de saisie, les activités de surveillance des communications et la mise en place de bases de données ADN.	المتعلقة بالمواطنين، أو تلك التي تنظم الآخر منها ولا سيما الشرطة وأجهزة الأمن العام التي تتعهد بمسؤوليات تنطوي حتما اقتحام المجال الخاص في سعيها لتحقيق أهداف عامة أوسع نطاقا مثل إدارة شؤون القضاء الجنائية وحماية السلامة العامة والأمن القومي. ويذكر من بين مهام الشرطة والأجهزة الأمنية التي قد تترتب عنها انعكاسات على الحياة الخاصة، البحث والحجز وأنشطة المراقبة والاتصالات وإنشاء قواعد بيانات الحمض النووي.
La vie privée est également une notion importante au regard des lois relatives au droit à l'information, dans la mesure où il y a des conséquences sur les individus. C'est le cas par exemple de la mise en place de bases de données d'identification et d'enregistrement comme pour les soins de santé ou pour les élections.	يرتبط الحق في الحياة الخاصة بالقوانين المتعلقة بالحق في المعلومة، حيث توجد آثار على الأفراد عند إحداث قواعد بيانات تتعلق بتحديد الهوية والتسجيل في مجالات مثل الرعاية الصحية أو الانتخابات.
Parce que les technologies sont en train de changer si rapidement la nature et la valeur de l'information et en raison des volumes très importants de données à caractère personnel qui sont générés, transmis, partagés et agrégés, il est essentiel que les gouvernements soient transparents. Cette transparence concerne à la fois le type et le volume de données collectées mais aussi les moyens et les modes de surveillance utilisés. Il devrait y avoir des mécanismes pour rendre compte des actions de l'État ainsi que des lois explicites et claires pour régir son pouvoir de surveiller et d'accéder aux données véhiculées dans les communications.	لأن التقنيات تغير بنسق سريع طبيعةٍ المعلومات وقيمتها ولأن كميات ضخمة من البيانات الشخصية تنشأ بسرعة، وتتم إحالتها وتقاسمها وتجميعها، فمن الضروري أن تتوخى الحكومات الشفافية حول أنواع وكمية البيانات التي تجمعها ووسائل وطرق المراقبة التي تتوخاها. كما يجب أن توجد آليات رقابة ومساءلة قوية وقوانين واضحة تحكم استعمال الدولة لسلطات المراقبة والنفاد إلى بيانات الاتصالات.
Organismes spécialisés :	المنظمات االمختصة

• Privacy International - https://www.privacyinternational.org/ • Open Rights Group - http://www.openrightsgroup.org/ • Electronic Frontiers Foundation - https://www.eff.org/ • European Data Protection Supervisor - https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS • OCDE http://www.oecd.org/fr/sti/ieconomie/securitedelinformationetlavieprivee.htm • Global Privacy Enforcement Network https://www.privacyenforcement.net	بريفاسي إنترناشيونال https://www.privacyinternational.org/ مجموعة الحقوق المفتوحة http://www.openrightsgroup.org/ مؤسسة الحدود الالكترونية https://www.eff.org/ مشرف حماية البيانات الأوروبية https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS منظمة التعاون الاقتصادي والتنمية www.oecd.org/sti/security-privacy https://www.privacyenforcement.net .....

Overview of Illustrative commitments	لمحة حول الالتزامات التوضيحية
Niveau initial	المراحل الأولية
• Publish educational material about the importance of protecting personal information • Publish all laws setting out the surveillance powers of law enforcement and intelligence agencies	نشر المواد التعليمية حول أهمية حماية المعلومات الشخصية نشر جميع القوانين التي تضبط صلاحيات الوكالات المختصة في مراقبة تطبيق القوانين ووكالات الاستخبارات
Niveau intermédiaire	المراحل الوسيطة

• Enact data protection legislation • Repeal any requirements compelling the identification of phone or internet users	سن تشريعات تتعلق بحماية البيانات إلغاء جميع المتطلبات الإلزامية للتعرف على مستخدمي الهاتف أو الإنترنت
Niveau avancé	المراحل المتقدمة
access to communications data and Publish transparency reports about surveillance activities • Reform legislation relating to surveillance by state agencies to ensure it complies with the International Principles on the Application of Human Rights to Communications Surveillance	• نشر تقارير حول شفافية النفاذ إلى البيانات والاتصالات وأنشطة المراقبة تنقيح التشريعات المتعلقة بالمراقبة من قبل أجهزة الدولة لضمان مطابقتها مع المبادئ الدولية بشأن تطبيق حقوق الإنسان في مراقبة الاتصالات
Innovation	تدابير ابتكارية
Establish a public oversight body responsible for ensuring that all new technologies and techniques adopted by police and public security agencies comport with the right to privacy	إنشاء هيئة عامة للرقابة مسئولة على ضمان انسجام جميع التكنولوجيات والتقنيات الجديدة التي تعتمدها الشرطة ووكالات الأمن العام مع الحق في الحياة الخاصة
NB: Voir ci-dessous les détails des différents engagements type.	(ملاحضة : لمزيد من التفاصيل أنظر مايلي)
Niveau initial: Publier des ressources pédagogiques expliquant l'importance de protéger les données personnelles.	المراحل الأولية: نشر موارد تعليمية حول أهمية حماية المعلومات الشخصية
Pertinence :	توضيح

The first step towards securing the protection of individuals' personal information is educating citizens about the value of that information and the reasons why they should expect that data to be protected. Individuals need to be informed about the nature of digital technologies and the internet, how companies gather and use data, and how governments might be able to gain access to that data. Empowering individuals with respect to personal information is in line with the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), which emphasise the participation of individuals in the protection of their own personal data.	تتمثل المرحلة الأولى نحو ضمان حماية المعلومات الشخصية للأفراد في تثقيف المواطنين وتوعيتهم بقيمة المعلومات الشخصية والأسباب التي من شأنها أن تجعلهم ينتظرون حماية هذه البيانات. يحتاج الأفراد إلى أن يكونوا على علم بطبيعة التكنولوجيات الرقمية والإنترنت وبالطرق التي تمكن الشركات من جمع البيانات واستخدامها، وتلك التي تجعل الحكومات قادرة على الوصول إلى تلك البيانات. إن تدعيم قدرات الأفراد فيما يتعلق بالمعلومات الشخصية يتماشى مع المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية بشأن حماية الحياة الخاصة وتدفقات البيانات الشخصية عبر الحدود (1980) التي تؤكد على مشاركة الأفراد في حماية البيانات الشخصية الخاصة بهم.
Recommendations 1. Publish easy-to-read information about personal information and how it can be paired with other data and analysed in ways that might endanger privacy. 2. Provide individuals with simple steps they can take to protect their personal information, both online and off, to ensure that citizens play a proactive role in the protection of their personal data.	توصيات نشر معلومات سهلة القراءة حول المعلومات الشخصية وكيف يمكن لها أن تهدد الحياة الخاصة إن تم إرفاقها مع بيانات الأخرى وتحليلها بطرق معينة. تمكين الأفراد من معرفة الخطوات البسيطة التي يمكن اتخاذها لحماية المعلومات الشخصية الخاصة بهم، سواء على الانترنت وخارجها، لضمان الدور ألاستباقي للمواطنين في حماية بياناتهم الشخصية.
Exemples internationaux : The UK Information Commissioner's Office has published a booklet called *Protecting your personal information online* which provides a useful example of the types of material that are helpful - http://www.ico.org.uk/upload/documents/library/data_protection/practic	أمثلة من بعض الدول

al_application/protecting_your_personal_information_online.pdf. Several UK government departments, with private sector partners, have also funded an initiative that provides comprehensive advice about online safety: https://www.getsafeonline.org.	نشر مكتب مفوض المعلومات في المملكة المتحدة كتيبا يسمى حماية المعلومات الشخصية الخاصة بك على الانترنت وهو مثالا يبين نوع المواد ذات الإفادة http://www.ico.org.uk/upload/documents/library/data_protection/practi .cal_applicati on/protecting_your_personal_information_online.pdf وبالإضافة إلى ذلك، مولت عديد الدوائر الحكومية في المملكة المتحدة، مع شركاء من القطاع الخاص، مبادرة تقدم نصائح شامل حول السلامة على الإنترنت: https://www.getsafeonline.org
Relevant standards and guidance European Data Protection Directive, 1995 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995 L0046:en:NOT Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981 - http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm Organisation for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980) - http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotection ofprivacyandtransborderflowsofpersonaldata.htm Federal Trade Commission, How to keep your personal information secure - http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-inf ormation-secure Electronic Frontier Foundation's Top 12 Ways to Protect Your Privacy Online -	المعايير والتوجهات ذات الصلة التوجيه الأوروبي حول حماية البيانات،1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995 L0046:en:NOT اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (عدد 108) 1981 http://conventions.coe.int/Treaty/en/Treaties/Html/108 الخطوط التوجيهية لمنظمة التعاون الاقتصادي والتنمية بشأن حماية الخصوصية والبيانات عبر الحدود تدفقات البيانات الشخصية (1980) http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectio nofprivacyandtransborderflowsofpersonaldata.htm لجنة التجارة الاتحادية، كيف الحفاظ على المعلومات الشخصية الخاصة بك آمنة http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-i nformation-secure

https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy	مؤسسة الحدود الإلكترونية 12 أفضل سبيل لحماية حياتك الخاصة على الإنترنت https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy
Initial step: Publish all laws setting out the surveillance powers of law enforcement and intelligence agencies	المراحل الأولية: نشر جميع القوانين التي تضبط صلاحيات الوكالات المختصة في مراقبة تنفيذ القوانين ووكالات الاستخبارات
Justification The administration of justice and the protection of national security in democratic countries require a transparent and open legal framework detailing the powers and responsibilities of police and public security agencies, including intelligence agencies. Where law enforcement and intelligence agencies are empowered to conduct surveillance in order to achieve security and policing aims, these powers must be clearly delineated and articulated in a way that enables individuals to foresee their application and scrutinise their use. A fundamental principle of international human rights law is that infringements of the right to privacy must be necessary, proportionate, and in accordance with the law. The European Court of Human Rights has emphasised that for surveillance to be “in accordance with the law” legislation must detail the following: [2] - “The nature of the offences which may give rise to surveillance; - The categories of people liable to be subject to surveillance; - A limit on the duration of surveillance; - The procedure to be followed for examining, using and storing the data obtain; - The precautions to be taken when communicating the data to	توضيح يتطلب إقامة العدل وحماية الأمن القومي في البلدان الديمقراطية إطارا قانونيا شفافا ومفصلاً لصلاحيات ومسؤوليات الشرطة ووكالات الأمن العام، بما في ذلك وكالات الاستخبارات. حيث يتم تقوية القانون والاستخبارات للمراقبة من أجل تحقيق الأمن وحفض النظام. هذه القوى يجب أن تكون محددة ومفصلة بطريقة تسمح للأفراد بتوقع تطبيقها والتدقيق في استخدمها. ومن المبادئ الأساسية للقانون الدولي لحقوق الإنسان أن انتهاكات للحق في الخصوصية يجب أن تكون ضرورية ومبررا وفقا للقانون. وقد أكدت المحكمة الأوروبية لحقوق الإنسان أنلمرصبة يجب أن تكون "وفقا للقانون" لا بد للتشريعات من تفصيلها كما يلي : طبيعة الجرائم التي قد تؤدي إلى المراقبة ، الفئات التي يمكن إخضاعها للمراقبة، الحد الأقصى للمراقبة، الإجراء الواجب اتباعه لدراسة البيانات المتحصل عليها واستعمالها وتخزينها،

other parties; and - The circumstances in which data may or must be erased or the tapes destroyed.”	الاحتياطات الواجب اتخاذها عند بث البيانات إلى أطراف أخرى، الضروف التي يستحسن أو تستوجب محو البيانات وتدمير الأشرطة.
Recommendations 1. Publish all laws and regulations setting out the surveillance powers of law enforcement and intelligence agencies and adopt such laws where these do not exist. These should cover internal regulations and procedures, although internal regulations should, where possible, be legislated to ensure they are subject to sufficient scrutiny. 2. Ensure laws and regulations setting out surveillance powers are sufficiently clear in scope and detail to meet the requirements of foreseeability and accessibility necessitated by the rule of law. 3. Educate citizens about the oversight mechanisms in place that investigate and monitor the compliance of law enforcement and intelligence agencies with the laws and regulations pertaining to surveillance powers. Provide information about means of redress for citizens who believe that agencies have breached legislation relating to surveillance.	توصيات 1. نشر جميع القوانين والأنظمة التي تحدد سلطات المراقبة للقانون ووكالات الاستخبارات و اعتمدها في الدول التي لا تطبيقها بعد. ينبغي أن تشمل هذه اللوائح والقوانين الداخلية، حيث أمكن، ويتم تشريعها للتأكد من أنها قد خضعت للتدقيق 2. ضمان القوانين والأنظمة التي تحدد سلطات المراقبة واضحة بما فيه الكفاية من حيث النطاق والتفاصيل لتلبية التوقعات وسهولة الوصول إليها كما تقتضيها سيادة القانون. 3. توعية المواطنين حول آليات الرقابة في المكان الذي التحقيق ورصد الامتثال وكالات إنفاذ القانون والاستخبارات مع القوانين والأنظمة المتعلقة سلطات المراقبة. تقديم معلومات عن سبل الانتصاف للمواطنين الذين يعتقدون أن وكالات انتهكت التشريعات المتعلقة المراقبة.
Country examples	أمثلة من بعض الدول
Relevant standards and guidance International Principles on the Application of Human Rights to Communications Surveillance -	المعايير والتوجهات ذات الصلة المبادئ الدولية بشأن تطبيق حقوق الإنسان لمراقبة الاتصالات

https://necessaryandproportionate.org/take-action/ORG Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on privacy and communication surveillance, April 2013 - http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement	تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، فرانك لا رو، على مراقبة الخصوصية والاتصالات، أبريل 2013
Intermediate step: Enact data protection legislation	المراحل الوسيطة: سن تشريعات تتعلق بحماية البيانات
Justification The concept of data protection implies that individuals have the right to decide whether to share their personal information and to determine on what terms they are prepared to do so. Data protection (DP) laws generally incorporate safeguards protecting the security of personal data and allowing others to use it only in prescribed circumstances. More than 100 governments have enacted or are in the process of enacting data protection legislation.[3] Most DP regimes derive inspiration from the OECD's 1980 Privacy Guidelines. They apply to all personal data, defined as "any information relating to an identified or identifiable individual". The Guidelines are not legally binding but have long been recognised as a statement of norms that should govern personal data privacy and guide OECD members and private organisations in crafting their policies. The Guidelines call for any personal data collected to be relevant and necessary for the purposes for which it is collected, to be obtained lawfully and fairly and to be kept accurate and up-to-date (Part II, Basic Principles). Personal information should be protected by reasonable security safeguards and should not be disclosed or otherwise made available for purposes other than the ones originally	توضيح : مفهوم حماية البيانات يعني أن الأفراد لديهم الحق في أن يقرروا ما إذا ارادو مشاطرة معلوماتهم الشخصية وتحديد أسس ذلك. قوانين حماية البيانات (DP) تتضمن عموما ضمانات حماية أمن البيانات الشخصية والسماح للآخرين باستخدامه في ظروف محددة. وقد سنت أكثر من 100 حكومة أو هي بصدد سن تشريعات حماية البيانات معظم أنظمة DP تستمد الإلهام من المبادئ التوجيهية الخصوصية لمنظمة التعاون والتنمية في عام 1980 . أنها تنطبق على جميع البيانات الشخصية، الذي يعرف بأنه "معلومات تتعلق بفرد محدد أو يمكن تحديده". المبادئ التوجيهية ليست ملزمة قانونا ولكن تم الاعتراف بها كمبادئ باعتبارها بيان المعايير التي ينبغي أن تحكم خصوصية البيانات الشخصية كما تم توجيه أعضاء منظمة التعاون والتنمية والمنظمات الخاصة في صياغة سياساتها. المبادئ التوجيهية تستوجب أن أي بيانات الشخصية يتم جمعها يجب أن تكون ذات صلة وضرورية للأغراض التي جمعت من أجلها، يتم الحصول عليها بصورة قانونية وعادلة وأن تبقى دقيقة ومتجددة (الجزء الثاني، المبادئ الأساسية).

specified at the time of collection, except with the consent of the data subject or by the authority of law.

These Guidelines stipulate that the following principles should be adhered to when collecting and processing personal information and data:

- Collection limitation: there should be limits to the collection of personal data, and data, which should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual;
- Data quality: personal data should be relevant to the purposes for which they are used, and should be accurate, complete and kept up-to-date;
- Purpose specification: the purposes for which personal data are collected should be specified and any subsequent use must be limited to that specification;
- Use limitation: data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the individual or b) by the authority of law;
- Security safeguards: data should be protected by reasonable security safeguards to protect against lost, destruction, use, modification or disclosure;
- Openness: there should be a general policy about openness with respect to personal data
- Individual participation: an individual should have the right to find out information about their data and to have incorrect data erased or rectified
- Accountability: a data controller is accountable for complying with these measures.

ينبغي حماية المعلومات الشخصية عن طريق ضمانات أمنية معقولة ويجب أن لا يتم الكشف عنها أو جعلها متاحة إلا لأغراض أخرى غير تلك المحددة أصلا في وقت جمعهاو لا تكون إلا بموافقة من موضوع البيانات أو عن طريق القانون.

هذه المبادئ التوجيهية تنص على أن المبادئ التالية يجب الالتزام بها عند جمع ومعالجة المعلومات الشخصية والبيانات:

- الحد من الجمع: يجب أن يكون هناك حدود لجمع البيانات الشخصية، والبيانات والتي ينبغي الحصول عليها عن طريق الوسائل المشروعة والعادلة، عند الاقتضاء، ومع علم أو موافقة الفرد
- جودة البيانات: يجب أن تكون البيانات الشخصية ذات سيلا بالغرض التي يتم استخدامها، ويجب أن تكون دقيقة وكاملة وحديثة

تحديد الغرض: الأسباب التي يتم جمع البيانات الشخصية لأجلها وينبغي تحديد أي استخدام لاحق لها

- تحديد : يجب أن لا يتم الكشف عن البيانات، وإتاحتها أو استخدامها لأغراض أخرى غير تلك المحددة قانوناً باستثناء في حالة موافقة الفرد
- ضمانات الأمن: ينبغي حماية البيانات عن طريق ضمانات أمنية معقولة لحمايتها ضد أي فقدان أو تدمير أو إستخدام أو تعديل أو كشف
- فتح البيانات: يجب أن يكون هناك سياسة عامة حول فتح البيانات الشخصية
- المشاركة الفردية: يجب أن يكون للفرد الحق في معرفة معلومات عن البيانات الخاصة بهم والحصول على بيانات غير صحيحة أو محوها لتصحيحها
- المساءلة: وحدة تحكم البيانات مسؤولة عن الامتثال لهذه التدابير.

Recommendations 1. Enact data protection legislation regulating the use of personal information by both the private and public sectors. 2. Establish a data protection authority to oversee compliance with data protection legislation and to mediate complaints. 3. Provide educational material to inform citizens and businesses about data protection standards, their application and opportunities for redress when data breaches occur. Country examples The Dominican Republic committed to enact the law on personal data protection as part of its Open Government Action Plan http://www.opengovpartnership.org/country/commitment/enact-law-personal-data-protection	توصيات 1. سن تشريعات لحماية البيانات الذي ينظم استخدام المعلومات الشخصية من قبل كل من القطاعين الخاص والعام. 2. إنشاء سلطة حماية البيانات للإشراف على الامتثال للتشريعات حماية البيانات و الاهتمام بالشكاوى 3. توفير المواد التوعوية لإبلاغ المواطنين والشركات حول معايير حماية البيانات، وتطبيقها وفرص التعويض عندما تحدث خروقات. أمثلة عن دول جمهورية الدومنيكان ملتزمة بسن قانون بشأن حماية البيانات الشخصية كجزء من خطة عمل الحكومة المفتوحة
Relevant standards and guidance European Data Protection Directive, 1995 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981 - http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm Organisation for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows	المعايير والتوجهات ذات الصلة توجيه حماية البيانات الأوروبية، 1995 اتفاقية مجلس أوروبا لحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (رقم 108)، 1981 إرشادات منظمة التعاون الاقتصادي والتنمية بشأن حماية الخصوصية والبيانات عبر الحدود تدفقات البيانات الشخصية (1980)

of Personal Data (1980) - http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm	
Intermediate step: Repeal any requirements compelling the identification of phone or internet users	المراحل الوسيطة: إلغاء جميع المتطلبات الإلزامية للتعرف على مستخدمي الهاتف أو الإنترنت
Justification One of the most important features of the Internet is the ability to anonymously access and impart information, and to communicate securely without having to be identified. Initially, this was possible because there was no “identity layer” built into the Internet. However, in the name of security and law enforcement, States have gradually eradicated opportunities for anonymous communication. In many States, individuals must identify themselves at cybercafés and have their transactions on public computers recorded. Increasingly, identification and registration are also required when buying a SIM card or mobile telephone device, for visiting certain major websites, or for making comments on media sites or blogs. Restrictions on anonymity facilitate State communications surveillance by making it easier to identify individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of surveillance. Thus restrictions on anonymity dissuade the free expression of information and ideas and can in practice result in people being unable to access vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities. Furthermore, restrictions on anonymity allow for the collection and compilation of large amounts of data by the private sector, placing a significant burden and responsibility on corporate	توضيح واحدة من أهم سمات للإنترنت هو القدرة على الوصول خفيةً ونقل المعلومات، والتواصل بشكل آمن دون الحاجة إلى تحديدها. في البداية، كان هذا ممكنا بسبب عدم وجود "طبقة الهوية" في صلب الإنترنت. لكن باسم الأمن و القانون تم القضاء تدريجياً على الاتصالات المجهولة. في كثير من الدول، يجب تحديد الأفراد أنفسهم في مقاهي الإنترنت و تسجيل استخدمهم لأجهزة الكمبيوتر العامة. و على نحو متزايد، يلزم تحديد ألهوية أيضا عند شراء بطاقة ذكية أو جهاز الهاتف النقال، أو خلال زيارة بعض المواقع الرئيسية، أو الإدلاء بتعليقات على مواقع وسائل الاعلام أو BLOG القيود المفروضة على عدم كشف الهوية تسهل مراقبة الاتصالات الخارجية من خلال تسهيل تحديد الأفراد أو نشر محتوى محظور، مما يجعل هؤلاء الأفراد أكثر عرضة لأشكال أخرى من المراقبة. وبالتالي القيود المفروضة على عدم الكشف عن هويته تثنيه عن التعبير الحر عن الأفكار والمعلومات ويمكن أن يؤدي إلى عدم القدرة على وصول الشعب إلى معطيات المجالات الاجتماعية الحيوية، مما يقوض حقهم في التعبير والمعلومات، وتفاقم التفاوت الاجتماعي. وعلاوة على ذلك، القيود المفروضة علة عدم الكشف عن الهوية تسمح بجمع وتجميع

actors to protect the privacy and security of such data. Reference: UN General Assembly, 2013, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue Recommendations 1. Repeal any laws or regulations that require the use of real names or the verification of identity in online fora, social media or other internet spaces. 2. Remove requirements that individuals identify themselves when using cybercafés or public computers. 3. Roll back mandatory SIM registration rules, making SIM registration an optional practice.	كميات كبيرة من البيانات من قبل القطاع الخاص، ووضع عبئا كبيرا ومسؤولية على الشركات الفاعلة لحماية خصوصية وأمن هذه البيانات. المرجعية: الجمعية العامة للأمم المتحدة، عام 2013، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، frank la rue توصيات 1. إلغاء أية قوانين أو لوائح تتطلب استخدام الأسماء الحقيقية أو التحقق من الهوية في الإنترنت ووسائل الإعلام الاجتماعية أو مسافات الإنترنت الأخرى. 2. إزالة المتطلبات التي تجبر الأفراد على تعريف بأنفسهم عند استخدام مقاهي الإنترنت أو أجهزة الكمبيوتر العامة. 3. رفض إلزامية قواعد القيد SIM، مما يجعل تسجيل SIM ممارسة اختيارية.
Country examples	أمثلة من بعض الدول
Relevant standards and guidance The Mandatory Registration of Prepaid SIM Card Users – A White Paper, November 2013 - http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf	المعايير والتوجهات ذات الصلة التسجيل إلزامي من مستخدمي بطاقة SIM مسبقة الدفع - ورقة بيضاء، نوفمبر 2013

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on privacy and communication surveillance, April 2013 - http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement	تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، فرانك لا رو، على مراقبة الخصوصية والاتصالات، أبريل 2013
Advanced step: Publish transparency reports about access to communications data and surveillance activities	المراحل المتقدمة: نشر تقارير حول شفافية النفاذ إلى بيانات الاتصالات وأنشطة المراقبة.
Justification Transparency around the use of surveillance powers is a crucial means of ensuring that law enforcement and intelligence agencies are kept in check and the privacy of individuals is not interfered with outside the strict confines of the law. Transparency allows the citizenry to watch over the government, ensure that it is not exceeding its powers, and to know when the balance between protecting security and infringing on human rights has tipped too far in favour of the police and public security forces. In recent years, numerous internet services and service providers have taken to publishing transparency reports, detailing the numbers of requests they receive from governments for access to individuals' communications data, and the number of requests they get for the removal of information from their services. Examples include: · Facebook Global Government Requests Report - https://www.facebook.com/about/government_requests	توضيح الشفافية حول استخدام سلطات المراقبة هو وسيلة حاسمة لضمان أن وكالات القانون والاستخبارات تحت المراقبة و لا تتدخل في خصوصية الأفراد. الشفافية تتيح للمواطنين لمراقبة الحكومة، وضمان أنها لا تتجاوز صلاحياتها، وتمنح المواطن الحق في معرفة متى قد يختل التوازن بين حماية الأمن والتعدي على حقوق الإنسان لصالح قوات الشرطة والأمن العام. في السنوات الأخيرة، اتخذت العديد من خدمات الإنترنت ومقدمي الخدمات قراراً بنشر تقارير الشفافية، تفصل أعداد الطلبات التي وردت من الحكومات من أجل الوصول إلى البيانات والاتصالات الأفراد، وعدد الطلبات التي تحصل لإزالة المعلومات من خدماتها. تقرير إدارة الفيسبوك

· Google Transparency Report - http://www.google.com/transparencyreport/ · Microsoft Law Enforcement Requests Report - https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ · Twitter Transparency Report - https://transparency.twitter.com/ Governments should embrace a similar process. By publishing transparency reports detailing the number of requests they make to communications services providers and internet services, and the number of authorisations granted to law enforcement and intelligence services for different types of online or offline surveillance, governments can ensure that its surveillance is scrutinised by the public in a way that ensures accountability.	تقرير الشفافية لشركة google تقرير شركة microsoft لمساندة القانون تقرير الشفافية ل-twitter يتعين على الحكومات تبني عملية مماثلة. من خلال نشر تقارير الشفافية بالتفصيل عدد الطلبات التي يقدمونها لمقدمي خدمات الاتصالات وخدمات الإنترنت، وعدد التراخيص الممنوحة لدوائر إنفاذ القانون والاستخبارات لمختلف أنواع المراقبة على الانترنت أو خدمات خارج الانترنت ، يمكن للحكومات أن تضمن التدقيق في المراقبة من قبل الشعب لضمان حقهم في المساءلة
Recommendations 1. Enact legislation compelling law enforcement and intelligence agencies to publish yearly disaggregated data about the number of requests made and acceded to by the private sector for access to corporate communications data, and the number of requests made to and approved by the courts or other oversight mechanisms for authorization to conduct online or offline surveillance. 2. Ensure transparency reports are published in an easy and accessible way.	توصيات 1. سن وكالات القانون والاستخبارات تشريعات تضمن نشر بيانات سنوية مفصلة عن عدد من الطلبات المقدمة إلى لشركات القطاع الخاص من أجل الوصول إلى البيانات والاتصالات، وعدد الطلبات التي قدمت و وافقت عليها المحاكم أو غيرها من آليات الرقابة للإذن بإجراء المراقبة على الانترنت أو الخدمات غير المتصلة بالانترنت 2. يتم نشر تقارير ضمان الشفافية بطريقة سهلة ويمكن الوصول إليها.

Country examples Relevant standards and guidance Global Network Initiative Principles - http://www.globalnetworkinitiative.org/principles/index.php	أمثلة من بعض الدول المعايير والتوجهات ذات الصلة مبادئ الشبكة العالمية للمبادرة
Advanced step: Reform legislation relating to surveillance by state agencies to ensure it complies with the International Principles on the Application of Human Rights to Communications Surveillance	خطوة متقدمة: تحوير التشريعات المتعلقة برقابة أجهزة الدولة لضمان احترامها للمبادئ الدولية بشأن تطبيق حقوق الإنسان على مراقبة الاتصالات
Justification As technologies that facilitate surveillance of communications advance, and the powers of intelligence agencies expand, there is a failure on the part of governments to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. There needs to be an updated understanding of how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. The International Principles on the Application of Human Rights to Communications Surveillance were developed to provide governments with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights. The Principles are the outcome of a global consultation with	توضيح أبرز تطور التقنيات التي تيسر مراقبة الاتصالات وتوسع صلاحيات وكالات الاستخبارات فشل الحكومات في ضمان انصهار القوانين واللوائح المتعلقة بمراقبة الاتصالات ضمن الحقوق الدولية للإنسان و توفير الحماية الكافية للحق في الحياة ولحرية التعبير. من هنا الضرورة لتحديث الفهم لكيفية تطبيق القانون الدولي لحقوق الإنسان في البيئة الرقمية الحالية، خاصة في ضوء تطور تقنيات وتكنولوجيات مراقبة الاتصالات وتغيراتها. وقد وضعت المبادئ الدولية بشأن تطبيق حقوق الإنسان على مراقبة الاتصالات لمنح الحكومات إطارا لتقييم مدى موافقة قوانين المراقبة وممارساتها الحالية أو المقترحة مع حقوق الإنسان. وانبثقت هده المبادئ عن مشاورة عالمية مع مجموعات من المجتمع المدني

civil society groups, industry and international experts in communications surveillance law, policy and technology.	والصناعة و خبراء دوليين في مجال قانون مراقبة الاتصالات وسياستها و تكنولوجيتها
Recommendations 1. Thoroughly review all laws and regulations pertaining to the surveillance powers of law enforcement and intelligence agencies to identify where legislation conflicts with or falls short of the standards articulated in the International Principles. 2. Amend legislation to ensure compliance with the International Principles.	توصيات إجراء مراجعة شاملة لجميع القوانين والأنظمة المتعلقة بصلاحيات مراقبة وكالات تنفيذ القانون والاستخبارات لتحديد موضع الاختلافات في التشريعات أو عدم ارتقائها إلى مستوى المعايير المنصوص عليها بالمبادئ الدولية. تعديل التشريعات لضمان الامتثال للمبادئ الدولية.
Country examples	أمثلة من بعض الدول
Relevant standards and guidance International Principles on the Application of Human Rights to Communications Surveillance - https://necessaryandproportionate.org/take-action/ORG	المعايير والتوجهات ذات الصلة المبادئ الدولية بشأن تطبيق حقوق الإنسان لمراقبة الاتصالات
Innovative step: Establish a public oversight body responsible for ensuring that all new technologies and techniques adopted by police and public security agencies uphold the right to privacy	تدابير ابتكارية: إنشاء هيئة عامة للرقابة مسئولة على ضمان انسجام جميع التكنولوجيات والتقنيات الجديدة التي تعتمدها الشرطة ووكالات الأمن العام مع الحق في الحياة الخاصة
Justification In general legislation has not kept pace with the changes in technology, resulting in legal standards which are either non-existent	توضيح

or inadequate to deal with the modern communications surveillance environment. Governments therefore are increasingly seeking to justify the use of new technologies using old legal frameworks, which do not reflect the expanded capabilities of newer technologies. In many countries, this means that vague and broadly conceived legal provisions are used to legitimize and sanction the use of intrusive techniques. Technologies applied and techniques that go far beyond what was originally foreseen by legislation are being applied without explicit laws authorizing them or defining the scope of their use, making it impossible for individuals to foresee – or even know about – their application. At the same time, laws are being adopted to broaden the breadth of national security exceptions, providing for the legitimization of intrusive surveillance techniques without oversight or independent review. A specially constituted public oversight body with competency to deal with technology and surveillance issues from a human rights perspective could play an important role in ensuring that new technologies adopted by law enforcement and intelligence agencies comply with existing laws and human rights standards. Reference: UN General Assembly, 2013, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue	لم تواكب التشريعات بصفة عامة التغيرات في التكنولوجيا ، مما أدى إما إلى غياب معايير قانونية او عدم ملائمتها للتعامل مع البيئة الحديثة لمراقبة الاتصالات. لذا تسعى الحكومات بشكل متزايد لتبرير استعمال التكنولوجيات الجديدة بالاستناد إلى أطر قانونية قديمة لا تعكس القدرات الواسعة لأحدث التقنيات. واستخدمت في عديد البلدان أحكاما قانونية غامضة وواسعة النطاق إما لإضفاء الشرعية على استخدام تقنيات دخيلة أو لمعاقبته. ويجري تطبيق التكنولوجيات والتقنيات التي تتجاوز استعمالاتها ما توقعته القوانين خارج أي إطار تشريعي يجيز استخدامها أو يحدد نطاقه، مما يستحيل معه على الأفراد التكهن بتطبيقها من عدمه أو حتى معرفة ذلك. في الوقت ذاته، تعتمد قوانين يوسع بمقتضاها مجال الاستثناءات المتعلقة بالأمن الوطني بغية إضفاء الشرعية على تقنيات مراقبة متطفلة دون رقابة أو مراجعة مستقلة. ولعل إحداث خصيصا هيئة رقابة عامة مختصة في شؤون التكنولوجيا و المراقبة من منظور حقوق الإنسان من شأنه أن تلعب دورا هاما في ضمان امتثال التكنولوجيات الجديدة المعتمدة من قبل

	وكالات تنفيد القانون والاستخبارات للقوانين و معايير حقوق الإنسان الجاري بها العمل. المرجع : الجمعية العامة للأمم المتحدة ، عام 2013، تقرير المقرر الخاص للنهوض و حماية الحق في حرية الرأي والتعبير، فرانك لا رو عامة التغيرات ف
Recommendations 1. Adopt legislation constituting a new public oversight body with expertise in law and technology; 2. Delegate to the body responsibility for ensuring that all new surveillance technologies and techniques adopted by law enforcement and intelligence agencies comport with the right to privacy; 3. Ensure the deliberations and decisions of the oversight body are open to the public.	شن تشريعات تتعلق بإحداث هيئة رقابة عامة تتكون من ذوي الخبرة في القانون والتكنولوجيا؛ تفويض الهيئة مسؤولية ضمان انسجام تكنولوجيات وتقنيات المراقبة الجديدة التي تعتمدتها وكالات تطبيق القانون ووكالات الاستخبارات مع الحق في الحياة الخاصة ضمان فتح مداولات وقرارات هيئة الرقابة للعموم.
Country examples Relevant standards and guidance International Principles on the Application of Human Rights to Communications Surveillance - https://necessaryandproportionate.org/take-action/ORG	أمثلة من بعض الدول المعايير والتوجهات ذات الصلة المبادئ الدولية بشأن تطبيق حقوق الإنسان لمراقبة الاتصالات

References: [1] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17). [2] *Weber and Saravia v Germany,* application no 54934/00, admissibility, 29 June 2006, at [95] [3] See *Global Tables of Data Privacy Laws and Bills:* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875	التعليق العام للجنة حقوق الإنسان رقم 16 (1988) بشأن الحق في احترام الحياة الخاصة والأسرة والبيت والمراسلات، وحماية شرفه وسمعته (المادة 17). [2] ويبر وسارافيا ضد ألمانيا، الطلب رقم 54934/00، المقبولية، 29 يونيو 2006، في [95] [3] انظر الجداول العالمية للبيانات قوانين الخصوصية وفواتير: