ملفات بريداتور: في أحابيل الشبكة

الخطر العالمي من برامج التجسس "الخاضعة لتنظيم الاتحاد الأوروبي"

الملخص التنفيذي

منظمة العفو الدولية

منظمة العفو الدولية هي حركة تضم 10 ملايين شخص، تعمل على استنهاض مشاعر التعاطف الإنساني لدى كل شخص، وتقوم بحملات من أجل التغيير حتى نتمكن جميعا من التمتع بحقوقنا الإنسانية.

وتتمثل رؤيتنا في عالم يفي فيه من هم في السلطة بوعودهم ويحترمون القانون الدولي، ويخضعون للمساءلة. نحن مستقلون عن أي حكومة أو عقيدة سياسية أو مصلحة اقتصادية أو دين، ويتم تمويلنا بشكل أساسي من قبل أعضائنا والتبرعات الفردية. ونؤمن أن العمل بالتضامن والتعاطف مع الناس في كل مكان يمكن أن يغير مجتمعاتنا نحو الأفضل.

الطبعة الأولى 2023
الناشر: منظمة العفو الدولية، شركة محدودة
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

رقم الوثيقة: ACT 10/7246/2023
اللغة الأصلية: الإنجليزية

amnesty.org

الرسم على الغلاف: © Colin Foo 2023

منظمة العفو الدولية

الملخص التنفيذي

على مدى العقد المنصرم، كشفت منظمات المجتمع المدني والباحثون والصحفيون النقاب عما تمارسه الحكومات في مختلف أنحاء العالم من أساليب الاستهداف غير المشروع للنشطاء والصحفيين والسياسيين باستخدام أدوات ابتكرتها شركات المراقبة السيبرانية الخاصة. ولقد حذرت منظمة العفو الدولية والعديد من منظمات المجتمع المدني مرارًا وتكرارًا من أن انخراط الحكومات في التجارة الغامضة لتكنولوجيات المراقبة التي تبتكرها شركات خاصة، ولا سيما برامج التجسس، واستخدامها لتلك التكنولوجيات، تسبّبت بأزمة مراقبة رقمية، وهي أزمة كانت لها عواقب وخيمة وآثار ضارة على حقوق الإنسان، وحريات الإعلام، والحركات الاجتماعية في شتى أنحاء العالم. وبفضل ما تكشف من حقائق عام 2021 بشأن مشروع بيغاسوس – مما أظهر للعيان النطاق والمدى العالمي للمراقبة غير المشروعة التي يسرها برنامج بيغاسوس التجسسي الذي ابتكرته مجموعة إن إس أو – وما أعقبه من أبحاث قامت بها منظمات المجتمع المدني، لم تجد الحكومات مناصًا من أن تعير اهتمامها للنطاق الهائل والمدى المستفحل لسوء استخدام برامج التجسس، وكان هذا محفزًا لبدايات التحرك من أجل كبح جماح بعضٍ من أسوأ شركات بيع برامج التجسس صيتًا. غير أن الحقائق الجديدة التي كشفت عنها منظمة العفو الدولية، ونتائج التحقيقات الجديدة بشأن ملفات بريداتور (Predator Files) التي جرت بتنسيق من شبكة التعاون الاستقصائي الأوروبي (EIC) الإعلامية، أظهرت بجلاء قصور الإجراءات الحكومية وعدم فعاليتها في وضع حد لسوء استخدام برامج التجسس؛ ويتناول التقرير الحالي تلك النتائج بالتفصيل.

أولًا، في إطار التحقيق بشأن ملفات بريداتور، تعاون مختبر الأمن التابع لمنظمة العفو الدولية مع شبكة التعاون الاستقصائي الأوروبي، وهي شراكة من المؤسسات الإعلامية الأوروبية، بصفته شريكًا تقنيًا؛ حيث عكفت منظمة العفو الدولية على تحليل الوثائق التي توصلت إليها الشبكة المذكورة للتحقق من المواصفات التقنية لطاقم من منتجات المراقبة التي قام بابتكارها وتشغيلها وتسويقها تحالف إنتلكسا (Intellexa) - وهو تحالف من شركات تكنولوجيا المراقبة – خلال الفترة بين عامي 2007 و2022؛ ووجدت منظمة العفو الدولية إلى أن ذلك يشمل طائفة من تكنولوجيات المراقبة المستهدفة والجماعية.

أما تكنولوجيات المراقبة المستهدفة فهي تشمل برامج التجسس الشديدة التطفّل التي تستهدف هواتف المحمولة، مثل برنامج بريداتور، التي يمكن إيصالها للأجهزة إما عن طريق الهجمات بنقرة واحدة أم الهجمات بدون نقر. كما يقدّم تحالف إنتلكسا أساليب متنوعة لتثبيت برنامج التجسس من خلال "الهجمات التكتيكية"، التي تمكن المهاجم من استهداف أجهزة قريبة منه. وفضلًا عن ذلك، فقد قام تحالف إنتلكسا أيضًا بابتكار وتشغيل وتسويق طرق للإصابة الإستراتيجية تسمح لطرف فاعل حكومي ما بتسديد هجمات تحاول إحداث إصابات صامتة لأجهزة مستخدمي خدمات الإنترنت التي تقدمها شركات متعاونة، أو عبر بلد بأكمله إذا ما تسنى لمشغِّل برنامج التجسس الوصول مباشرة إلى حركة البيانات المتدفقة عبر الإنترنت. وتشبه أنظمة الإصابة الإستراتيجية أدوات المراقبة الجماعية من حيث كونها تتطلب الوصول إلى حركة البيانات المتدفقة على الإنترنت على نطاق واسع حتى يتسنى لها استهداف الأفراد وإصابتهم. وتوحي منتجات المراقبة الجماعية "الواسعة النطاق" التي يقدّمها تحالف إنتلكسا بتطور تكنولوجيات المراقبة السابقة وتحولها من أنظمة اعتراضية مشروعة كانت تسمح برصد تدفّق البيانات على نحو فردي ومستهدف – مما كان من المحتمل أن يتيح القيام بالمزيد من التحقّق وفرض المزيد من القيود – إلى طرق أوسع نطاقًا إلى حد كبير وأكثر عشوائية.

وتعتقد منظمة العفو الدولية أن كلا النوعين من التكنولوجيات – برامج التجسس الشديدة التطفّل وأدوات المراقبة الجماعية العشوائية – يتناقضان مع حقوق الإنسان تناقضًا جوهريًا. فبرنامج بريداتور التجسسي، وتنويعاته المعاد تصميمها وتسميتها، هي برامج تجسسية على قدرة عالية من التغلغل والتطفّل، تستطيع الوصول إلى كميات لا حد لها من البيانات على الجهاز المستهدف، وليس بالإمكان حاليًا إخضاعها للتمحيص المستقل. ومن ثم فإن التقييم الذي خلصت إليه منظمة العفو الدولية هو أن أي استخدام لبرنامج بريداتور،

وأمثاله من برامج التجسس الشديدة التطفّل، لا يمكن أن يكون منسجمًا مع حقوق الإنسان، ولا بد من حظره بصورة مستديمة.

ثانيًا، تكشف منظمة العفو الدولية في هذا التقرير عن عملية مراقبة مستهدفة لم يُكشف عنها النقاب من قبل، قام بها أحد عملاء تحالف إنتلكسا من مستخدمي برنامج بريداتور التجسسي، تربطه صلات بفيتنام. ويبدو أن هذا العميل يراعي مصالح حكومية في فيتنام، وقام خلال الفترة بين فبراير/شباط ويونيو/حزيران 2023 باستهداف ما لا يقل عن 50 من حسابات التواصل الاجتماعي التابعة لسبعة وعشرين فردًا و23 مؤسسة، باستخدام أدوات برامج التجسس التي ابتكرها وباعها تحالف إنتلكسا. وتم هذا الاستهداف باستخدام هجمات بنقرة واحدة أُرسلت إلى حسابات التواصل الاجتماعي للأفراد والمؤسسات من حساب على منصة إكس (المعروفة سابقًا باسم تويتر) اسمه @Joseph_Gordon16. وكان من بين المستهدفين في إطار هذا الهجوم ببرنامج تجسسي موقع إخباري مستقل مقرّه في برلين، وشخصيات سياسية في البرلمان الأوروبي، والمفوضية الأوروبية، وباحثون أكاديميون، ومراكز بحوث. وفضلًا عن هؤلاء، تضمن المستهدفون بمحاولات هجوم أخرى مسؤولين بالأمم المتحدة، ورئيسة تايوان، وأعضاء في مجلسي الشيوخ والكونغرس في الولايات المتحدة، وجهات دبلوماسية أخرى.

وأكدت مجموعة تحليل المخاطر التابعة لشركة غوغل لمنظمة العفو الدولية أن الأبحاث التي قامت بها غوغل أظهرت أن النطاقات وعناوين المواقع الشبكية URL التي اكتشفتها منظمة العفو الدولية في إطار عملية برنامج التجسس كانت مرتبطة بنظام برنامج بريداتور التجسسي التابع لتحالف إنتلكسا. وإلى جانب الأدلة المستمدة من شركاء شبكة التعاون الاستقصائي الأوروبي، تظهر نتائجنا أدلة على مبيعات لمنتجات تحالف إنتلكسا الخاصة بالمراقبة إلى وزارة الأمن العام الفيتنامية، وتوحي بأن بعض عملاء السلطات الفيتنامية أو أشخاصًا يعملون لصالحها قد يكونون وراء حملة الهجمات ببرامج التجسس. وفضلًا عن ذلك، فقد أكدت غوغل لشركاء من شبكة التعاون الاستقصائي الأوروبي أنها "تعزو" حملة الهجمات ببرنامج بريداتور التابع لتحالف إنتلكسا ومؤشرات يتناولها هذا التقرير إلى "جهة فاعلة حكومية في فيتنام".

وهذه المعلومات التي تم الكشف عنها تستند إلى أبحاث تقنية لا يزال مختبر الأمن التابع لمنظمة العفو الدولية عاكفًا عليها لرصد ابتكار واستخدام تكنولوجيات المراقبة التي تقدمها شركات برامج التجسس المرتزقة، بما فيها تلك التي يقدمها تحالف إنتلكسا. وفي إطار هذه الجهود، يشير تحليل منظمة العفو الدولية للبنية التحتية التقنية الحديثة المرتبطة بنظام برنامج بريداتور للتجسس أيضًا إلى وجود عملاء نشطين محتملين أو استهداف محتمل للأفراد في السودان ومدغشقر وكازاخستان ومنغوليا ومصر وإندونيسيا وفيتنام وأنغولا.

وتستند النتائج الواردة في هذا التقرير أيضًا إلى مقابلة أجريت مع صحفي مستهدف من فيتنام، وسجلات شحن، وبيانات تجارية، وأبحاث أخرى قامت بها شبكة التعاون الاستقصائي الأوروبي وما أصدرته من تقارير عن مبيعات تحالف إنتلكسا لما تقدمه من حلول بشأن المراقبة والإصابة. كما استعرضت منظمة العفو الدولية تقارير وبيانات وقوانين ودراسات صادرة عن هيئات الأمم المتحدة وخبراؤها وسلطات إقليمية وأخرى على مختلف المستويات الوطنية، والتقارير الاستقصائية وتقارير السياسات التي أصدرتها منظمات المجتمع المدني، فضلًا عن تقارير صادرة عن وسائل الإعلام.

ثالثًا، يناقش هذا التقرير آثار الحقائق التي تكشفت بشأن ملفات بريداتور على حقوق الإنسان، والتي تظهر كيف يتم بيع ونقل مجموعة من تكنولوجيات المراقبة ذات القدرة العالية على التغلغل والتطفّل التي يوردها تحالف إنتلكسا في مختلف أنحاء العالم دون مساءلة أو عقاب. ويتألف تحالف إنتلكسا من شركات مختلفة تبيع تكنولوجيات ومنتجات المراقبة، والتي لها وجود مؤسسي في بلدان الاتحاد الأوروبي، فضلًا عن بلدان أخرى في مختلف أنحاء العالم. وتظهر الحقائق التي تكشفت النطاق والمدى العالمي لمبيعات تكنولوجيات المراقبة الواردة من تحالف واحد فقط من الشركات التي تبيع هذه التكنولوجيات. وقام هذا التحالف ببيع منتجاته لمصر وليبيا ومدغشقر والسعودية وفيتنام وفرنسا، ضمن بلدان أخرى كثيرة خلال الفترة من 2007 إلى 2022. ونقل هذه التكنولوجيات يقترن باحتمال كبير لارتكاب انتهاكات حقوق الإنسان نظرًا للسوابق في هذه البلدان فيما يخص المراقبة غير المشروعة و/أو غياب الضمانات في مجال المراقبة على الصعيد الوطني التي يمكن أن تحول دون تسليط تلك التكنولوجيات بصورة غير مشروعة على المجتمع المدني، أو الصحفيين، أو المعارضين السياسيين.

رابعًا، يعرض هذا التقرير بالتفصيل تاريخًا من انتهاكات حقوق الإنسان التي ثبتت صلتها بتحالف إنتلكسا في اليونان وليبيا ومصر؛ ويروج هذا التحالف لنفسه بوصفه "شركة تتخذ مقرها في الاتحاد الأوروبي وتخضع لتنظيمه". وورد أن تحالف إنتلكسا يتألف من الشركات التالية: نكسا تكنولوجيز (NexaTechnologies) وأدفانست ميدل إيست سيستمز (Advanced Middle East Systems) (ما يشكّل مجموعة نكسا - Nexa group)، فضلًا عن شركات وايسبير (WiSpear)، وسيتروكس (Cytrox) وسينباي تكنولوجيز (Senpai Technologies) (ما يشكّل مجموعة إنتلكسا - Intellexa group). وتتحكم مجموعتا شركات نكسا وإنتلكسا في العديد من الكيانات المؤسسية التي أعيدت تسمية بعضها؛ وتمتد هذه الكيانات عبر ولايات قضائية مختلفة، داخل الاتحاد الأوروبي وخارجه. ويكتنف الغموض والسرية الطبيعة الدقيقة للروابط القائمة

بين هذه الشركات، إذ إن الكيانات المؤسسية والهياكل التي تربط بينها دائمة التغير والتحور والتطور، ويعاد توصيفها وتصميمها وتسميتها باستمرار. ويبدو أن هذه الهياكل المؤسسية التي يكتنفها الغموض والتعقيد تسهّل على الشركات تجنب المساءلة والشفافية والتملص من النظم واللوائح الحكومية، بما في ذلك الضوابط الإقليمية والوطنية على التصدير، وآليات الحيطة الواجبة الخاصة بالشركات. بل إن الصورة أكثر تعقيدًا في حالة تحالف إنتلكسا ليس بسبب الهياكل المؤسسية لشركة أم واحدة فحسب، وإنما أيضًا هياكل الشركات المتحالفة معها التي تبيع منتجات المراقبة، وشركاتها الأم، ومستثمريها. والطبيعة بالغة التعقيد والالتفاف لهذا الكيان المؤسسي يمكن أن تزيد من صعوبة تحقيق المساءلة والشفافية بشأن الاستهداف غير المشروع باستخدام أدوات المراقبة التي ينتجها هذا التحالف.

ووفقًا لما تنص عليه المبادئ التوجيهية للأمم المتحدة بشأن الأعمال التجارية وحقوق الإنسان (المبادئ التوجيهية للأمم المتحدة)، فإن الشركات مسؤولة عن احترام حقوق الإنسان حيثما تمارس نشاطها التجاري في العالم؛ ومن أجل تحمل هذه المسؤولية، ينبغي على الشركات اتخاذ إجراءات الحيطة الواجبة حفاظًا على حقوق الإنسان. ولم تبادر شركات تحالف إنتلكسا نفسها إلى الكشف عن أي معلومات عن ممارساتها التي تلتزم فيها بالحيطة الواجبة إزاء حقوق الإنسان؛ وأي تقييمات، إن وجدت، لما تفضي إليه تكنولوجيات المراقبة التي تنتجها من آثار على حقوق الإنسان لا تزال محاطة بالسرية. كذلك فإن الدول القومية تقع على عاتقها التزامات بموجب القانون الدولي لحقوق الإنسان تلزمها بحماية حقوق الإنسان من أي انتهاكات ترتكبها أطراف ثالثة؛ ويشمل ذلك الالتزام بتنظيم سلوك الشركات التي تتخذ مقرها في بلدانها أو تخضع لسيطرتها الفعلية من أجل منعها من التسبب بانتهاكات حقوق الإنسان، أو المساهمة فيها، حتى إذا وقعت تلك الانتهاكات في بلدان أخرى. وقد وقعت انتهاكات لحقوق الإنسان بسبب تقاعس الدول عن فرض ضوابط مجدية على تحالف إنتلكسا - على سبيل المثال الدول التي توجد بها مقار الكيانات المؤسسية التي يضمها التحالف، ومن بينها اليونان، وأيرلندا، وفرنسا، وألمانيا، والجمهورية التشيكية، وقبرص، والمجر، وسويسرا، وإسرائيل، وشمال مقدونيا، والإمارات العربية المتحدة. وتظهر النتائج المذكورة فيما تقدم، في مجملها، أن المجتمع المدني والصحفيين ما برحوا يواجهون عواقب وخيمة للاستخدام غير المشروع، بلا ضابط ولا رابط، لتكنولوجيات المراقبة التي لا تزال تهدد حقوق المستهدفين في الخصوصية وحرية التعبير وحرية تكوين الجمعيات أو الانضمام إليها، وحرية التجمع السلمي. وفضلًا عن ذلك، وعلى نحو ما يوضحه هذا التقرير بالتفصيل، فإن استهداف السلطات الرسمية، الإقليمية والوطنية والدولية يظهر مرة أخرى أن برامج التجسس التجارية تكون لها آثار بالغة على كل من حقوق الإنسان وأمن المنظومة البيئية الرقمية؛ فبدون إخضاع تكنولوجيات المراقبة هذه لأي رقابة أو تنظيم، يصبح بالإمكان استخدامها ضد حكومات أو سلطات ثالثة، وقد استُخدمت بالفعل على هذا النحو.

وليست هذه النتائج سوى غيض من فيض؛ فحيث إن شركات المراقبة وعملاءها من الدول لا تزال ممعنة في الاختباء وراء تصريحاتها بشأن الأمن الوطني والسرية بهدف التملص من الشفافية والمساءلة، فأغلب الظن أن النطاق والمدى الحقيقي للاستهداف غير المشروع باستخدام الأدوات التي يوردها تحالف إنتلكسا أكبر وأوسع بكثير. وترجِّح تحذيرات المجتمع المدني والدروس المستفادة من مشروع بيغاسوس (Pegasus Project) أن المجتمع المدني في كل بلد من البلدان التي أظهرت الحقائق التي انكشفت أن تحالف إنتلكسا قد باع تكنولوجياته فيها قد يكون عرضة للمراقبة السرية الشاملة. ومرة أخرى، توضح هذه الحقائق الجديدة أن بيع ونقل تكنولوجيات المراقبة بلا ضابط ورابط قد يظل من العوامل التي تسهِّل انتهاك حقوق الإنسان على نطاق عالمي هائل؛ إذ لا يزال يُسمَح للشركات ببيع ونقل منتجاتها بشكل حر وبسرية مطلقة. وتظهر نتائجنا مرة أخرى أن أي ادعاءات من الشركات مفادها أن الاستهداف غير المشروع أمر شاذ هي باطلة بلا جدال؛ فانتهاك حقوق الإنسان هو سمة من سمات هذا القطاع وليس آفة من آفاته.

وفي أعقاب ما تكشف من حقائق بشأن مشروع بيغاسوس، قطعت الدول بعض الخطوات في الاتجاه الصحيح بهدف تنظيم هذا القطاع واستخدام الدول لهذه التكنولوجيات؛ بعضها كانت خطوات مهمة وجديرة بالترحيب في الاتجاه الصحيح. غير أن التصريحات العلنية والتوصيات والالتزامات الطوعية لم تترجم إلى أفعال في جميع الأحوال، ولم ينل المستهدفون بصورة غير مشروعة ببرامج التجسس في مختلف أنحاء العالم أي تعويضات فعالة ولم تتحقّق أي مساءلة فعالة حتى الآن. ولئن كانت بعض الدول قد بادرت إلى بذل جهود طوعية، فقد جنحت دول أخرى إلى المماطلة في التحقيقات وعرقلتها، ولم تتحلَّ بالشفافية على نحو مجدٍ. ويجب على الدول بذلك المزيد من الجهود المتضافرة لإرساء ضمانات ملزمة قابلة للتنفيذ لحماية حقوق الإنسان على الصعيد الوطني والإقليمي والدولي. وفي عام 2019، أشارت المقررة الخاصة للأمم المتحدة المعنية بالحق في حرية الرأي والتعبير إلى أنه "لا يكفي القول بوجود نظام شامل ومُختلٍ لمراقبة واستعمال تكنولوجيات المراقبة المحددة الهدف. فهو لا يكاد يكون موجودًا". وتعتقد منظمة العفو الدولية أن هذا الوضع لا يزال ساريًا، بالرغم مما أحرز من تقدم أولي.

وبوجه خاص، ترسم أحدث الحقائق التي كشف النقاب عنها صورة قاتمة لإخفاقات الاتحاد الأوروبي والدول الأعضاء فيه في كبح جماح الشركات التي لا تخضع للمساءلة والدول الأعضاء الجانحة التي لا تزال تستغل الشقوق الكبيرة الواضحة للعيان في الأطر التنظيمية على الصعيدين الإقليمي والوطني. وتظهر حملة

المراقبة السافرة التي يتناولها هذا التقرير بالتفصيل والتي تستخدم أدوات تحالف إنتلكسا المخاطر المباشرة المنبثقة عن الانتشار والنقل غير المنضبطين لأدوات المراقبة السيبرانية من دول الاتحاد الأوروبي؛ فهي لا تفضي إلى وقوع انتهاكات حقوق الإنسان خارج الاتحاد الأوروبي فحسب، وإنما تشكل أيضًا خطرًا يهدد الأمن وحقوق الإنسان داخله.

وتخضع صادرات برامج التجسس من الاتحاد الأوروبي للتراخيص بموجب لائحة تنظيم الصادرات ذات الاستخدام المزدوج، التي ينبغي، من الناحية النظرية، أن تأخذ بعين الاعتبار ما تنطوي عليه تلك الصادرات من أخطار على حقوق الإنسان. غير أن الحقائق التي تكشفت بشأن "ملفات بريداتور" تظهر أن تراخيص تصدير تكنولوجيات المراقبة قد منحتها دول أعضاء في الاتحاد الأوروبي في حالات تنطوي على خطر كبير باستخدامها في ارتكاب انتهاكات حقوق الإنسان من قبل المستخدمين النهائيين. كما تظهر تلك الحقائق أن لوائح تنظيم الصادرات لدى الاتحاد الأوروبي قد تم التحايل عليها من خلال هياكل وكيانات مؤسسية غامضة في دول ثالثة. ومن الواضح أن لائحة الاتحاد الأوروبي لتنظيم الصادرات ذات الاستخدام المزدوج تشوبها عيوب بالغة؛ وقد مضت سنتان على صدور اللائحة التنظيمية المعادة صياغتها بشأن الاستخدام المزدوج، ولم توضع موضع التنفيذ بقوة وشفافية. كما أشارت لجنة الاتحاد الأوروبي للتحقيق بشأن بيغاسوس وغيره من برامج التجسس المماثلة (لجنة PEGA) إلى غياب الإرادة السياسية لدى الاتحاد الأوروبي والدول الأعضاء فيه. ولئن كانت الجهود التشريعية المستمرة، مثل التوجيه المتعلق بالحيطة الواجبة في إطار الاستدامة المؤسسية (CSDDD)، تتيح فرصة في الوقت المناسب للبدء في معالجة أضرار قطاع المراقبة المستهدفة، فإن الثغرات التي تشوب ما تقدم به مشرعو الاتحاد الأوروبي المشاركون من مقترحات قد تؤدي إلى عدم تطبيق هذا التوجيه كما ينبغي على شركات تكنولوجيا المراقبة.

توصيات رئيسية للدول

نظرًا لعدم فعالية اللوائح والأنظمة الحالية، فضلًا عن الطبيعة الانتهاكية المتأصلة لبرنامج بريداتور، يجب على جميع الدول القيام بما يلي:

- (بخاصة الدول التي منحت تراخيص تصدير) الإلغاء الفوري لجميع تراخيص التسويق والتصدير الصادرة لتحالف إنتلكسا، وإجراء تحقيق مستقل ومحايد وشفاف لتحديد مدى الاستهداف غير المشروع، بحيث تؤدي هذه الجهود في نهاية المطاف إلى إصدار بيان علني بشأن نتائج الجهود والخطوات الرامية لتفادي أي أضرار في المستقبل.
- فرض حظر على استخدام برامج التجسس ذات القدرة العالية على التطفّل؛ ففي الوقت الحالي، ليس بالإمكان إخضاع مثل هذه البرامج للتمحيص والتدقيق المستقل أو قصر وظائفها على الوظائف الضرورية والمتناسبة مع استخدام وهدف محددين.
- تنفيذ إطار تنظيمي لحقوق الإنسان يحكم المراقبة، بحيث يكون متمشيًا مع المعايير الدولية لحقوق الإنسان؛ وإلى حين تنفيذ مثل هذا الإطار، يجب تنفيذ أمر بوقف شراء وبيع ونقل واستخدام جميع برامج التجسس.
- تنفيذ تشريعات وطنية تفرض ضمانات ضد انتهاكات وتجاوزات حقوق الإنسان التي تحدث من خلال المراقبة الرقمية، وإرساء آليات للمساءلة مصممة بحيث تتيح سبل التعويض لضحايا انتهاكات المراقبة.
- إلزام شركات المراقبة قانونًا باتباع إجراءات الحيطة الواجبة بشأن حقوق الإنسان فيما يتعلق بعملياتها العالمية، بما في ذلك فيما يخص استخدام منتجاتها وخدماتها.

توصيات رئيسية للاتحاد الأوروبي والدول الأعضاء فيه

- يجب على الدول الأعضاء في الاتحاد الأوروبي والمفوضية الأوروبية ضمان التنفيذ الصارم لقواعد الاتحاد الأوروبي للرقابة على الصادرات لعام 2021؛ ويشمل هذا اتخاذ إجراءات فورية من أجل التأكيد على التزامات الحيطة الواجبة فيما يتعلق بحقوق الإنسان المنبثقة عن اللائحة التنظيمية للاستخدام المزدوج، وخلق سوق تتسم بالشفافية لتكنولوجيات المراقبة السيبرانية بحيث تكون ملتزمة بضمانات فعالة لحقوق الإنسان.
- يجب على الدول الأعضاء في الاتحاد الأوروبي اعتماد وتنفيذ تشريعات تفرض على جميع الأطراف المؤسسية احترام حقوق الإنسان وتنفيذ تدابير الحيطة الواجبة لمراعاة حقوق الإنسان تمشيًا مع المبادئ التوجيهية للأمم المتحدة. وفي إطار المداولات المستمرة بشأن التوجيه المتعلق

بالحيطة الواجبة في إطار الاستدامة المؤسسية، يجب على الاتحاد الأوروبي إلزام الشركات باتخاذ الحيطة الواجبة لمراعاة حقوق الإنسان فيما يتعلق بسلسلة القيمة الكاملة بما في ذلك شراء المنتجات وبيعها ونقلها وتصديرها واستخدامها. ويجب على الشركات العاملة في جميع القطاعات تنفيذ المتطلبات الواردة في التوجيه المتعلق بالحيطة الواجبة في إطار الاستدامة المؤسسية، بما في ذلك الشركات المنتجة لبرامج التجسس، فضلًا عن المؤسسات المالية.

التوصيات الرئيسية لحكومة فيتنام

يجب على حكومة فيتنام إجراء تحقيق مستقل ومحايد وشفاف بشأن المراقبة المستهدفة غير المشروعة المشار إليها في هذا التقرير، بما في ذلك التحقيق فيما إذا كانت هذه الحملة من الهجمات ببرامج التجسس تمت بأي صلة لأي وكالات حكومية معينة.

توصيات رئيسية لتحالف إنتلكسا

يجب على تحالف إنتلكسا التوقف عن إنتاج وبيع برنامج بريداتور أو أي برنامج تجسسي مماثل آخر يتمتع بقدرة تطفلية عالية ولا يشتمل على أي ضمانات تقنية تسمح باستخدامه المشروع في إطار تنظيمي يراعي حقوق الإنسان. ويجب على التحالف أيضًا تقديم تعويض كافٍ أو أشكال أخرى من الإنصاف الفعال لضحايا المراقبة غير المشروعة.

منظمة العفو الدولية حركة عالمية لحقوق الإنسان عندما يقع ظلم على أي إنسان فإن الأمر يهمنا جميعاً.

اتصلوا بنا

info@amnesty.org

mena@amnesty.org

+44 (0)20 7413 5500

انضموا إلى المحادثة

www.facebook.com/AmnestyArabic

@AmnestyAR