

على الخلاف

«الأخ الأكبر» يراقبنا: الخصوصية انتهكت

إليها «منظمة تبادل الإعلام الاجتماعي»، في تقرير تحت عنوان «رسم خريطة المراقبة الرقمية الجماعية في لبنان». هذا لا يعني أنّ الجهات الخمس المذكورة وحدها تمتلك مثل هذه القدرة، إلا أن التسريبات قدّمت أدلة تتصل بهذه الجهات تحديداً، وهي عبارة عن مراسلات مع شركات وفرق عمل لطلب إيضاحات ومعلومات وتجارب على أجهزة وبرامج تُستخدم لأغراض التجسس الشامل، وفواتير بملايين الدولارات لشراء مثل هذا

ثلاثة أجهزة أمنية: الأمن العام وقوى الأمن الداخلي ومخابرات الجيش. وشركتان خاصتان: IncoNet - Data Management و virtual isp. يُرجح أنها تمتلك تقنيات «المراقبة الشاملة»، وهي المصطلح المهذب لعمل سبيل للغاية: التجسس على الناس ورصد تحركاتهم واختراق بياناتهم الشخصية من أي نوع كانت، حتى الحميمة منها. هذا ما تكشفه تسريبات «ويكيليكس» الأخيرة عن لبنان ومصادر أخرى، التي استندت

تسريبات ويكيليكس إنهم يتجسسون علينا

الأميركية وأوروبا، بعد صعود الهجمات الإرهابية، وبالتالي هي إشكالية جديدة في العالم ولا تقتصر فقط على لبنان. مذّك غيّرت الأجهزة الأمنية في العالم معادلة الأمن مقابل الحرية إلى الأمن مقابل الخصوصية. تحت عنوان «قويبا» الإرهاب، انتهكت المبادئ الديمقراطية التي وضعت قيوداً قانونية وقضائية للأجهزة تمنعهم من تجاوز حد السلطة وضمان حرية الأفراد وخصوصياتهم. فإذا كان الوضع في الدول التي تزعم أنها «ديموقراطية» وتضمن «الحرية العامة والفردية» مثيراً للقلق والخوف، فكيف سيكون في دول، مثل لبنان، تفتقر إلى الحد الأدنى من الضوابط القانونية وتفتقر أساساً إلى ثقافة عدم انتهاك خصوصية الناس؟

يقول نجم إن «الحكومة اللبنانية مساهمة في تغطية انتهاك الخصوصية، وهي أعطت شيكاً على بياض للأجهزة الأمنية لتحصل على كل داتا الاتصالات والإنترنت من دون أي تدقيق فعلي من قبل القضاء، وهذا مخيف ويؤسس لزيادة التجسس والقمع الإلكتروني، ما يؤثر سلباً بنحو غير مباشر في كل نشاطاتنا الإلكترونية».

لا توجد معلومات موثقة قبل تشكيل لجنة التحقيق الدولية بقضية اغتيال رئيس الحكومة السابق رفيق الحريري وإقامة المحكمة الدولية الخاصة بلبنان، ولكن منذ ذلك الحين تحصل أكبر عملية تجسس واختراق للخصوصية في لبنان عبر تسليم «داتا» الاتصالات كاملة لأشخاص أجانب وجهات خارجية وأجهزة أمنية محلية. في عام 2014 تخلى مجلس الوزراء عن صلاحياته بقبول أو رفض طلبات الحصول على بيانات الاتصالات وإعطائها للأجهزة الأمنية، شكل هذا الأمر خرقاً للدستور والقانون 140 الذي ينص بوضوح في أول مادتين فيه على أن المراقبة يجب أن تقتصر على عدد محدد من الأشخاص، ولفترة زمنية محددة، وأن تكون ممنوحة بموافقة قاضٍ، كما يرد في التقرير.

الأجهزة الأمنية: برامج بملايين الدولارات

يستند تقرير «رسم خريطة المراقبة الرقمية الجماعية في لبنان» إلى المعلومات المتاحة من التسريبات التي حصلت أخيراً. يقول نجم: «كمتابعة للنمط، نعتقد بأن التجسس يحصل أكثر من ذلك، لكننا لا نستطيع أن نثبت ذلك». حسب التقرير، إن المديرية العامة للأمن العام وقوى الأمن الداخلي يستخدمان برامج FinFisher التجسسية لنشاطات المراقبة في لبنان، مستنداً إلى تقرير «مختبر المواطن» Citizen Lab، وهو مختبر للبحوث الرقمية في جامعة

36% من اللبنانيين، المشاركين في استطلاع عن المراقبة الرقمية في لبنان، يشعرون بأن الحكومة تراقبهم على الإنترنت. فيما يشعر 19% بأن الشركات الخاصة تراقبهم، في مقابل 11% يشعرون بأن أفراداً يراقبونهم. النسبة الباقية، 34%، ليسوا متأكدين من تعرضهم للمراقبة، ليبقى السؤال معلقاً: هل نحن مراقبون؟

الجواب نعم، بحسب تقرير «رسم خريطة المراقبة الرقمية الجماعية في لبنان»، الذي صدر أواخر عام 2016 بالإنكليزية عن «منظمة تبادل الإعلام الاجتماعي» (بحث وكتابة محمد نجم)، وترجم إلى العربية في شباط 2017، من دون تسليط الضوء عليه جيداً. يتناول هذا التقرير الجهات الفاعلة الرئيسية في الدولة في حقل المراقبة الرقمية، ويوثق حالات استخدام تكنولوجيا المراقبة الشاملة، ويسمى أيضاً الشركات التي باعت تلك الأنظمة والخدمات في خلال السنوات الخمس الماضية.

المديرية العامة للأمن العام، قوى الأمن الداخلي، مخابرات الجيش، شركة IncoNet - Data Management المعروفة بـ IDM وشركة virtual isp المزودتان لخدمات الإنترنت، تمتلك برامج تجسس كشفت عنها تسريبات لفواتير ضمن «ويكيليكس» وتقارير أخرى. لا يعني ذلك أنّ هذه الجهات وحدها متورطة بالتجسس والمراقبة في لبنان، إلا أن هذه التسريبات كشفت عن تورطها في شراء أو السعي لشراء أجهزة تنصت بملايين الدولارات، وفق ما يكشف التقرير، في ظل غياب مبادئ توجيهية واضحة ومحددة تنظم هذه العمليات، ما يجعلها تشكل تهديداً جدياً لخصوصية الناس ويطرح ضرورة وضع أنظمة صارمة لحماية البيانات وتنظيم عمل الأجهزة الأمنية في هذا الإطار.

يوضح معدّ التقرير، محمد نجم، لـ«الأخبار» أنّ «التجسس يحصل في كل البلدان، لكن المخيف في لبنان أنه يحصل من دون دور قضائي جدي للجم أي تعدّ على الحقوق المدنية للمواطنين المكفولة بالدستور، ولا سيما الحق بالخصوصية». ويشير نجم إلى أن «عدم وجود قانون لحماية البيانات الشخصية يساهم بزيادة هذا التعدي (عن قصد أو عن غير قصد) من قبل الأجهزة المعنية». وبلغت إلى «أننا مقلوبون على مرحلة البيانات الديمترية في لبنان، سواء الباسبورات التي بدأ العمل بها، أو دفاتر السوق وتسجيل السيارات التي سيبدأ العمل بها قريباً، لذلك يجب أن نعرف ماهية هذه البيانات وأين تُخزن وكيفية حمايتها ومن لديه القدرة على الوصول إليها، وما هو دور القضاء في ذلك؟».

الأمن مقابل الخصوصية

عالمياً، تُعدّ قضية حماية خصوصية الأفراد من أكثر القضايا المطروحة، خصوصاً في الولايات المتحدة

الأمن العام وقوى الأمن الداخلي يستخدمان برامج FinFisher التجسسية

أنه «في شباط 2015، تواصل المكتب (الأمن العام) مع هاكينج تيم، طالباً تفاصيل عن برنامج الشركة الجديد غاليليو (Galileo) لنظام التحكم عن بُعد وعن ميزات و ثمنه والشخص الممكن التواصل معه وعن معلومات إضافية. وكشفت التسريبات عن دليل على إجراء عرض تجريبي للفكرة في بيروت. وأجرى المكتب

تورونتو، «وقد سُجّل انخراط المديرية العامة للأمن العام وقوى الأمن الداخلي نظراً لارتباطهما بمخدم بريد بسجلات تحمل اسم نطاق كلا الوكالتين».

لكن ما هي برامج FinFisher؟ في تقرير لمختبر Citizen Lab، يوجد شرح أن هذا البرنامج طوّره شركة «عاما الدولية»، ويجري تسويقه على أنه أداة قوية للوصول إلى أجهزة كمبيوتر المجرمين والإرهابيين سراً. بمجرد استهداف جهاز الكمبيوتر الخاص بالشخص المعني، لا يمكن كشف البرنامج من قبل أي برنامج لمكافحة الفيروسات والتجسس. أما قدرات هذه البرنامج، فهي: سرقة كلمات المرور من أجهزة الكمبيوتر الخاصة بالأشخاص، ما يتيح الوصول إلى حساباتهم الإلكترونية الخاصة والتوصّل على المكالمات الهاتفية ومكالمات سكايب، إضافة إلى تشغيل كاميرا جهاز الكمبيوتر الخاص بهم وميكروفون لتسجيل المحادثات والفيديو من الغرفة الموجودين فيها.

يشير التقرير إلى أنه في «عام 2015، نشرت ويكيليكس رسائل إلكترونية مسربة بين الأمن العام وشركة هاكينج تيم (Hacking Team) للمراقبة الهجومية، أظهرت أنّ التواصل بين الفريقين بدأ في أوائل عام 2012، إلا أنه غير الواضح إذا ما نشأت علاقة عمل بينهما في نهاية المطاف أو لا. يتضح في تسريبات «ويكيليكس» لأكثر من مليون وثيقة تعود إلى شركة هاكينج تيم، وفق ما ينقل التقرير، لم يقتصر الأمر على جهاز الأمن

العام، إذ يرد في التقرير أنّ مخابرات الجيش أجرت مثل هذه الاتصالات أيضاً. فقد كشفت التسريبات عن فواتير صادرة عن شركة هاكينج تيم موجهة إلى مخابرات الجيش اللبناني، بلغ مجموعها أكثر من مليون يورو، مستحقة عن شراء نظام غاليليو للتحكم عن بُعد إلى جانب معدّات أخرى. ولكن لم تُحدّد الأهداف أو المحتوى الخاضعان للمراقبة».

إنّ ما هو برنامج Galileo؟ تقدّم شركة «هاكينج تيم» برنامج «غاليليو» على أنه أداة لتجاوز التشفير، جمع البيانات من أي جهاز ومراقبة الأفراد المستهدفين أينما كانوا، حتى عندما يكونون خارج نطاق المراقبة الخاص بالمراقب. يمكن من خلال البرنامج التحكم بالمستهدفين ومراقبتهم مهما كانت أنواع أجهزة تهم، وهو برنامج لا يمكن رصده من قبل المستخدم أو برامج مكافحة التجسس كما أنه لا يؤثر على أداء الجهاز المراقب أو بطاريته.

تعلّقاً على هذه المعلومات، يقول ناشط حقوقي إن «هناك ما يكفي من المبررات لاستخدام الأجهزة الأمنية وسائل تجسس، بدءاً من رصد عملاء إسرائيل، وصولاً إلى استباق الهجمات الإرهابية، وهي نجحت في هذا الأمر أكثر من مرة، وتمكنت من تجنّب البلد هجمات عدة. لكننا بالمقابل نعيش في بلد تشويه صراعات كثيرة وتدخلات خارجية واتهامات لأجهزة دول عربية وأجنبية بالتجسس على اللبنانيين

فواتير صادرة عن شركة هاكينج تيم إلى مخابرات الجيش بقيمة مليون يورو لشراء نظام «غاليليو»