التنصت على العالم: متى تطغى الخسائر السياسية على المكاسب الاستخبارية؟

"إنها كارثة.. وكل كشف جديد للأسرار يعزز الحاجة إلى إعادة كبح جماح الوكالة. هنالك عواقب سياسية تلحقها تبعات تشغيلية.."

التجسس بعمليات مختص مؤرخ ،إيد ماثيو

في عام 2001، رفضت شركة الاتصالات الأمريكية، كويست Quest، طلب وكالة الأمن القومي المشاركة في برنامجها للتجسس على العملاء دون إذن قانوني. وبعد بضع سنوات وجهت محكمة اتحادية إلى مديرها التنفيذي، جوزيف ناشيو، تهمة المضاربة اعتماداً على معلومات سرية حصل عليها بطريقة غير مشروعة، ثم تمكنت من أدانته وقضى أربع سنوات ونصف السنة من العقوبة قبل أن يطلق سراحه من السجن. وما يزال يصر إلى اليوم على أن العقوبة ظالمة وكيدية وسياسية الدوافع.

لا ريب في أن خبير المعلوماتية "المارق" إدوارد سنودن (29 عاماً) قد أثار، حين تسلل من الباب الخلفي لأكبر وكالة استخبارات في العالم حاملاً ملفاً ضخماً من أسرارها، عدداً لا حصر له من القضايا الإشكالية والأسئلة الشائكة التي تتجاوز نطاق التجسس والتنصت والترصد. فقد أثبت بعضها جملة من الحقائق التي ظلت محل شك واشتباه مدة طويلة، وصدم بعضها الآخر أنصار الحقوق المدنية ودعاة المبادئ الأخلاقية، وملأ غيرها نفوس الأصدقاء بالسخط والاستياء وصدور الأعداء

بالشماتة والازدراء، بينما سببت أخرى قلقاً عميقاً جراء تهديم المبدأ الجوهري الذي ارتكزت عليه الشبكة الإلكترونية.

ما هي الحدود الفاصلة بين متطلبات الأمن القومي وحقوق الخصوصية الشخصية؟ وهل يمكن قيام دويلة بوليسية سرية في بلد ديمقراطي يعتمد مبدأ الشفافية؟ هل ألحق التعاون –إن لم نقل التواطؤ- بين الوكالة والشركات الأمريكية العملاقة، طوعاً أو كرهاً، الضرر بها في أسواق الاتصالات والتقانة الدولية؟ هل يؤدي جهد الوكالة السري لإضعاف أنظمة التشفير والترميز إلى جعل الإنترنت أقل أماناً للجميع؟ هل تبرر محاربة الإرهاب التنصت على أي إلكترون شارد في الفضاء يمكن أن يضيف أي معلومة، ولو كانت تافهة، إلى ما تعرفه الإدارة الأمريكية عن العالم؟ وهل يعد التجسس قانونياً ومشروعاً وضرورياً ومثمراً في مكافحته؟ وهل ما سمح به القانون الأمريكي للوكالة يمثل الحدود النهائية للمراقبة والتجسس، أم مجرد نقطة البداية؟

تأسست وكالة الأمن القومي عام 1952، وضمت أكبر مجموعة من وكالات الاستخبارات في الولايات المتحدة. في الأيام المبكرة، لعب العلماء العاملون في الوكالة دوراً كبيراً في تطوير أوائل أجهزة الكمبيوتر التي كانت مجرد أدوات لفك رموز الشيفرة. وحين انتشرت الكمبيوترات الشخصية والمحمولة واللوحية والهواتف الذكية في أصقاع الأرض كلها أصبحت القرصنة المجال المتوسع لعمل الوكالة –التي تعد أكبر مستخدم للمختصين بالرياضيات في الولايات المتحدة. تركز الوكالة بؤرة نشاطها التجسسي على الإنترنت وأجهزة الكمبيوتر والهواتف وكابلات الألياف البصرية، فضلاً عن فك أنظمة التشفير والترميز، ولا تمانع في اقتناص أي معلومة مهما كانت عن التعاملات المصرفية وصفقات الشراء التي تتم بواسطة بطاقات الائتمان، ومعرفة أرقامها وأسماء أصحابها، والتجسس على صناديق البريد الإلكتروني الخاصة والمحادثات الهاتفية ومحركات البحث على الإنترنت، وخطط سير رحلات السفر، والمشتريات العادية، أو أي بيانات إلكترونية أخرى. وعبر الترهيب والترغيب والوسائل القانونية وغير القانونية، حولت شركات الاتصالات والانترنت الأمريكية العملاقة إلى شركاء في جمع المعلومات، عن طريق زرع المرشحات في مرافقها، واقتحام البرمجيات التي تستخدمها، والحصول على مفاتيح فك التشفير والترميز التي تملكها. على الصعيد القانوني، تخضع الوكالة لإشراف لجنة الاستخبارات في الكونغرس ومحكمة مراقبة الاستخبارات. تبلغ ميزانية الوكالة (الميزانية السوداء) 10,8 مليار دولار، وتوظف جيشاً جراراً من العاملين والمحللين والجواسيس يصل عدده إلى 35,000 موظف.

الهدف المعلن للوكالة حسب الخطة الخمسية الحالية هو "الرد على الأنشطة المهددة التي يعمل الآخرون على إبقائها مخفية.."، ثم تأخذ النبرة انعطافة أخلاقية لافتة ترفض بإباء مبدأ الوسائل المبررة بالغايات: "يجب على الخبراء العاملين لدينا التشبث بالمبادئ الأخلاقية السامية، حتى حين يسعى الإرهابيون أو [الحكام] المستبدون إلى استغلال الحريات التي نتمتع بها.. وسوف يقول أعداؤنا أو يفعلون أي شيء للترويج لقضيتهم؛ أما نحن فلن نلجأ إلى هذا الأسلوب".

تحدد الميزانية خمس مهمات للوكالة: تحذير القادة الأمريكيين من التهديدات، ومحاربة الإرهاب، والحد من انتشار الأسلحة، والعمليات الإلكترونية، ومكافحة التجسس.

في الحرب الباردة استهدفت الوكالة الدفاع عن الأمن المعلوماتي والتقاني الأمريكي، والهجوم على منظومات العدو بغرض اختراقها أو كشفها أو تعطيلها، لكن تشابكت المهمتان مع عولمة أجهزة الكمبيوتر والإنترنت. وأصبح من الصعب التفريق بين

الأنظمة التي يستخدمها العدو والصديق، لأنها مشتركة بين الجميع: ميكروسوفت ويندوز، ومسيرات ربط (Routers) سيسكو، ولغة رقم النص الفائق (HTML)، وأجهزة أي فون، ورقاقات إنتيل.. ومن المؤكد أن العثور على نقطة الضعف –أو إيجاد واحدة- وإبقائها سرية من أجل مهاجمة الأشرار يتركان الأخيار بالضرورة أكثر عرضة للخطر.

تكشف ملفات سنودن عدداً من برامج المراقبة والرصد التي استخدمتها وكالة الأمن القومي و"مقر الاتصالات الحكومية" البريطاني (النسخة البريطانية من الوكالة الأمريكية) للتجسس على العالم. تمكنت الوكالتان كلتاهما من الوصول إلى المعلومات المخزنة لدى شركات التقانة الأمريكية الكبرى، دون إذن قانوني غالباً، إضافة إلى تنصت واسع النطاق على بيانات مستمدة من كابلات الألياف البصرية التي تشكل العمود الفقري لشبكات الهاتف والانترنت العالمية. كما تشاركت الاثنتان في العمل على تقويض المعايير الأمنية التي تعتمد عليها شبكة الانترنت والتجارة الإلكترونية والعمليات المصرفية. من هذه البرامج:

بريزم PRISM (أداة التخطيط لتكامل الموارد والتزامن والإدارة)

يتيح هذا البرنامج التجسسي السري لوكالة الأمن القومي الحصول على المعلومات المتعلقة بالأهداف من مخدمات عدد من أكبر شركات التقانة الأمريكية: غوغل، آبل، ميكروسوفت، فيسبوك، ياهو.. دون الحاجة إلى طلبها (بإمكان وكالة التجسس البريطانية، "مقر الاتصالات الحكومية"، الحصول على بيانات برنامج بريزم).

تمبورا TEMPORA

برنامج لجمع وتخزين حجم هائل من البيانات المتدفقة من وإلى بريطانيا. يخزن محتوى الاتصالات التي يلتقطها لمدة ثلاثة أيام، بينما تخزن الميتاداتا (البيانات الوصفية، أو بيانات البيانات: المرسل، المستقبل، مدة الاتصال..) لمدة ثلاثين يوماً. يضع البرنامج أجهزة تنصت على كابلات الألياف البصرية (داخل بريطانيا وخارجها) للحصول على كميات ضخمة من البيانات الشخصية لمستخدمي الإنترنت، وذلك بعلم الشركات التي تمتلك هذه الكابلات أو محطاتها. وأشارت وثائق سنودن إلى أن وكالة الأمن القومي تتقاسم مع الوكالة البريطانية البيانات المجمعة بواسطة البرنامج.

نظام جمع سجلات بيانات الاتصالات الهاتفية

أظهرت أولى الوثائق المسربة أن وكالة الأمن القومي تتابع برنامجاً مثيراً للجدل لجمع سجلات المكالمات الهاتفية لملايين الأمريكيين. بدأ العمل بالبرنامج في عهد إدارة بوش واعتقد كثير من المتابعين خطأً أنه ألغي قبل سنوات. لكن تبين أنه أجيز قانونياً مرة أخرى. أفرجت إدارة أوباما عن مئات الصفحات من الوثائق السرية حول البرنامج، وأظهر عدد منها أن بعض عمليات المراقبة مخالفة للدستور وفقاً لمحكمة سرية تشرف عليها.

أبستريم UPSTREAM

برنامج يضم مجموعة من برامج التجسس التي تستخدمها الوكالة، منها التنصت على الاتصالات التي تمر في كابلات الألياف البصرية العابرة للولايات المتحدة أو في المحطات المقامة في قاع البحر. يتيح النظام، الذي يعتمد على مساهمة شركات الاتصالات الأمريكية، للوكالة الوصول إلى مخزون هائل من بيانات الهواتف والانترنت، حين يكون أحد طرفي الاتصال على الأقل خارج الولايات المتحدة. كشفت وثائق سنودن أن الوكالة تحتفظ بجميع بيانات البيانات (ميتاداتا) التي تستخلصها بواسطة نظامي بريزم وابستريم في قاعدة بيانات تدعى مارينا MARINA لمدة 12 شهراً.

إضافة إلى ذلك كله تبذل الوكالتان الأمريكية والبريطانية جهداً منهجياً لفك أنظمة الترميز والتشفير، وهي تقانة مصممة لحماية الإنترنت، بما في ذلك حسابات البريد الإلكتروني والتجارة الإلكترونية والمعاملات المصرفية والسجلات الرسمية . كما تطبقان برنامجاً إضافياً يكلف 250 مليون دولار سنوياً للعمل سراً وعلناً على إضعاف برمجيات وعتاد الأمان، والمعايير العالمية للسلامة والأمن، الأمر الذي دفع الخبراء إلى التحذير من مغبة ترك جميع مستخدمي الإنترنت عرضة للاختراق.

يبدو من الوثائق المسربة أن أذرع الوكالة الأخطبوطية تمتد إلى أركان العالم الأربعة، بمساعدة سفن التجسس التي تلتقط كل ما تبثه الأجهزة اللاسلكية على البر وهي تبحر قبالة السواحل، وأطباق الأقمار الصناعية (في فورت ميد-ولاية مريلاند) التي تتجسس على الصفقات المصرفية في كل مكان، والطائرات التي تجمع المعلومات من ارتفاع ستين ألف قدم، والهوائيات الموجهة على أسطح مباني ثمانين سفارة أمريكية في بلدان العالم. وحين نأخذ بالاعتبار الزعماء الخمسة والثلاثين الذين تتجسس عليهم الوكالة بانتظام (ما زالت أسماؤهم مجهولة)، والهجمات الإلكترونية التي شنتها على إيران وروسيا والصين وكوريا الشمالية (بلغ عددها 231 في عام 2011 وحده)، والجهود الحثيثة لاختراق عشرات الملايين من أجهزة وشبكات الكمبيوتر في أنحاء شتى من العالم وقرصنتها ثم ترك أجهزة تجسس فيها تسمح للوكالة بتجاوز الترميز عبر اقتناص الرسائل غير المشفرة حين تكتب أو تقرأ، نكتشف الحقيقة المذهلة الصادمة: لا يمكن لإنسان أن يعيش بمنأى عن العين الساهرة والأذن المرهفة لـ"الأخ الكبير": لا العدو اللدود آية الله العظمى علي خامنئي، ولا الصديق المتعب حامد كرزاي؛ ولا أنجيلا ميركل وديلما روسيف، ولا حتى بان غي مون الطيب المحايد (تكشف إحدى الوثائق أن الوكالة تجسست عليه وعلمت مسبقاً بالنقاط التي سيتطرق إليها عند لقائه مع الرئيس الأمريكي). ووفقاً لمنطق الوكالة، من المهم التجسس على بعض الدول للحصول على ميزة دبلوماسية (ألمانيا وفرنسا) أو اقتصادية (الصين واليابان) أو استعداداً لمواجهة مقبلة (إيران وكوريا الشمالية) أو تقاسم المعلومات الاستخبارية مع دول هي نفسها هدف للتجسس (إسرائيل)..

من الحقائق المعروفة في ميدان التقانة المتقدمة أن الطريقة المثلى لتحسين الأمن هي كشف نقاط الضعف والاختراق. ولذلك ينشر الباحثون المعلومات عن نقاط الضعف والانكشاف في برمجيات الكمبيوتر وأنظمة التشغيل، وخوارزميات فك التشفير. لكن من الخطأ الاعتقاد بأن أي تقانة تستخدمها وكالة الأمن القومي ستبقى سراً مكنوناً ردحاً من الزمن. صحيح أنها تجري أوسع الأبحاث نطاقاً وأكثرها تقدماً وتطوراً، إلا أن أطرافاً أخرى لا تتخلف عن الركب كثيراً. وفي الحقيقة هنالك موجة "دمقرطة" جارفة تكتسح الميدان، وما تكتشفه الوكالة من تقانة سرية اليوم، ستصبح أطروحات لطلاب الجامعات غداً، وأدوات للمجرمين والقراصنة في الفضاء الإلكتروني بعد غد.

لا ريب في أن الوكالة حققت بعض النجاحات المشهودة، مستغلة التقدم الهائل الذي تحققه الشركات الأمريكية والغربية في ميدان

تقانة الكمبيوتر والاتصالات. على سبيل المثال لا الحصر، اقتفى المحللون في الوكالة الأثر الإلكتروني الذي خلفه أحد كبار قادة القاعدة في إفريقيا في كل مرة كان يتوقف فيها على الطريق لاستخدام حاسوبه. ثم توقعوا المحطة اللاحقة، وأبلغوا الشرطة المحلية التي كانت بالانتظار لاعتقاله. وفي محطة الوكالة الضخمة في فورت غوردون، طور الخبراء خدمة مؤتمتة يمكن أن تبعث برسالة عبر البريد الإلكتروني إلى محلل كلما انتقل الهدف من برج اتصالات للهواتف النقالة إلى آخر في إحدى البلدان الأجنبية. وتمكنت محطة الوكالة في تكساس من اعتراض 478 رسالة بالبريد الإلكتروني حين كانت تساعد في إحباط خطة لمجموعة جهادية تستهدف فناناً سويدياً رسم صوراً مسيئة للنبي. وقدم المحللون في الوكالة إلى السلطات المسؤولة في مطار كيندي في نيويورك أسماء مجموعة من العمال الصينيين الذين أرسلتهم إحدى عصابات تهريب البشر، إضافة إلى رقم الرحلة، فألقت القبض عليهم على الفور.

لكن في خضم الضجة الكبرى، وصخب أصوات التأييد والاعتراض والتبرئة والإدانة، تضيع عدة مفارقات تدعو إلى السخرية حقاً، منها فشل المؤسسة المسؤولة عن أمن المعلومات في الحفاظ على أمن معلوماتها!! واقتحام الشبكة الإلكترونية من الدولة التي تنادي بحمايتها من اختراق الأنظمة القمعية والحكام المستبدين، فضلاً عن إخفاقات وعثرات مهمة لم يتطرق إليها أحد: تنصتت الوكالة على كل ما يحدث في أفغانستان، من الاتصالات بين البيروقراطيين في دواوين الحكومة في كابول إلى المكالمات بين قادة طالبان الميدانيين في الجبال، لكنها فشلت في تحقيق نصر حاسم على عدو جاهل بالتقانة المتقدمة. ورصدت جميع مراحل بناء الترسانة الكيماوية في عهد الأسد الأب والابن خطوة خطوة وقذيفة قذيفة، إلا أنها لم تمنع مذبحة خنق الأطفال الرضع بالغازات السامة في غوطة دمشق. وجمعت مسودات الرسائل في حسابات البريد الإلكتروني لزعماء دولة العراق الإسلامية، لكنها ما حالت بينها وبين التوسع ومد نشاطها إلى سورية المجاورة. واخترقت، عبر برنامج متطور للقرصنة، كمبيوترات بعض قيادات حزب الله اللبناني، ما جعل من الممكن اقتناص رسائل الحزب الإلكترونية من بين السيل الدافق من الاتصالات العالمية، لكن ظل الحزب يمثل خطراً إرهابياً متوسعاً ومهدداً للمنطقة.

هل نعاني تبعات العيش في عصر المعلومات وأخطاره؟ ربما تكون القصة كلها مجرد علامة أخرى على تغيير جوهري يحدث تحت السطح في المدركات السائدة عن الحكومة وأجهزتها وصلاحياتها، إشارة دلالية أخرى إلى نهاية مفهوم "الأبوية الأمنية" إذا جاز التعبير. لقد أصبحت الحدود الفاصلة بين الحكومة والمواطنين في العقود الأخيرة أكثر قابلية لـ"لاختراق"، حيث يريد هؤلاء مزيداً في المشاركة في صنع السياسة. وربما تمثل تسريبات سنودن هجوماً مقصوداً على أكثر المحرمات (التابوهات) التي تستخدمها الحكومة تأثيراً في القلوب والعقول لفرض رأيها وتخويف المعارضين: الأمن القومي. وما فعله سنودن هو جر آخر معقل من معاقل النموذج الأمني الأبوي في صنع السياسة من ظلام السر إلى نور العلن. لكن ما يحدث الآن فعلاً –فوق السطح- هو استقطاب حاد بين الجماعات المدافعة عن الحريات المدنية والحقوق الأساسية، ومجتمع الاستخبارات والمسؤولين الأمنيين، استقطاب قد يعطل الحراك في المستقبل المنظور.

تباينت المواقف حول إدوارد سنودن، وتراوحت بين ضرورة تبرئته وتمجيده بوصفه بطلاً فضح الأخطاء والتجاوزات، وتجريمه وإدانته باعتباره خائناً أفشى الأسرار والمعلومات وعرض الأمن القومي الأمريكي للخطر. لكن جوليان أسانج، مؤسس موقع ويكيليكس، وشريكه (الأسترالي) في فضح أسرار الأبوية الأمنية (والعسكرية)، دافع بأسلوبه اللاذع عن سنودن ضد متهميه بالخيانة العظمى، فكلاهما في الهم سواء: في الحقيقة، ينتمي إلى "جيل الشباب المتفوق في الذهنية التقنية" الذي خانه

باراك أوباما.