

رقاقة المقراض

إن مبتكر رقاقة المقراض Clipper Chip ، كان شبحاً من حيث لم يقصد . كان كلينتون بروك شغوفاً بعلم الفلك . فدرسه في جامعة ييل في أواخر الستينات ، وأراد أن يتخذه مهنة له ، بعد أن ينهي خدمته الإلزامية في البحرية . وما عهد إليه بأداء واجبه العسكري في المحيط الهادي ، أخذ يعد لانتقال زوجته وأولاده الصغار إلى هاواي وأن يبحر على متن إحدى السفن ، بعد تعيينه ضابط اتصالات فيها . ولم يكن مدركاً يومئذ أن جماعة معينة في وكالة استخبارات ، كانوا يعدون له خطأً أخرى .

كان بروكس ، قبل بضعة أعوام ، قد عُيِّن في موقع مجهول بالنسبة له ليقضي خدمته الإلزامية الصيفية ؛ كان ذلك المكان فورت جورج ميد . فانتقل بسيارته إلى ماريلاند ، متوقفاً أن يجد قاعدة عسكرية نموذجية . غير أنه بدلاً من ذلك وجد حراساً غامضين يوقفونه عند مدخل مكان بدا وكأنه بناء من أبنية المكاتب الحديثو سط أرض قفراء . وأخبره هؤلاء أن دخول المكان محظور ، إلا لأولئك الذين يحملون تصاريح أمنية عليا . ومما فاجأه ، ورود مكالمات هاتفية تفيد بأنه قد منح لتوه هذا التصريح . أهلاً بك يا كلينت بروكس في وكالة الأمن القومي . ولعله حسب أن مهمته هذه مجرد فاصل في سياق خدمته العسكرية ،

ومن الواضح أن رؤساءه قد لاحظوا قدراته، وقدموا له بديلاً عن الخدمة في البحرية. وكان في هذا العرض ما فيه من الإغراءات، إذ لم يعد بوسعه البقاء في الولايات المتحدة فحسب، بل سيتاح له أيضاً إرضاء حاجاته على نحو أعمق، فرصة لإشباع أشواقه الكونية، إلى حد ما، بأن يعمل في أقطار ستطلاع في غاية السريّة. ولن يكون قادراً، بالطبع، على إطلاع الأصدقاء والجيران والأقارب على العمل الذي يقوم به، لأنه حتى اسم مؤسسة الأعمار الصناعية كان يحاط بالكتمان أكثر من اسم الوكالة [وكالة الأمن القومي] التي ينكر الجميع وجودها. غير أن العرض بدا جيداً لبروكس. وهكذا رفض المهمة المعهودة إليه على ظهر السفينة بوبيلو، سفينة التجسس التي قدر أن يستولي عليها الكوريون الشماليون بعد بضعة أشهر، في 23 كانون الثاني/يناير 1968. إذن لسوف يعمل في الوكالة التي لم يكن ليجرؤ على النطق باسمها.

بعد أربعة وعشرين عاماً، أصبح كلينت بروكس نائب المدير المساعد في الوكالة التي صار الآن يجاهر باسمها بالفعل. ووجد نفسه وسط أزمة تتصل بالمهمة التي تأسست وكالة الأمن القومي من أجلها: صعود الكريبتوجرافيا الشعبية. وفي أحد الأيام من أواخر بيع عام 1992، مضى الرجل إلى مكتب مستشار عام للوكالة، عُيّن حديثاً فيها، ليطلب منها المساعدة في حملة كان يأمل في أن تساعد الوكالة على اجتياز هذا التطور الخطير.

جرت العادة على أن يتم تجنيد، المستشار العام لوكالة الأمن القومي من خارج ملاكها، وكان هذا محام حسن الإطلاع على العمل الحكومي، لكن ليست له خبرة تُذكر في شؤون الاستخبارات، حسبه أن يتطوع للتلاؤم مع البيئة المغلقة داخل لسياج الثلاثي، ويظل على إدراكه بالعالم الواقع خارج السياج. وكان بوي إنمان أول من خطر بباله أن عقلاً قانونياً حصيفاً انتزع لتوه من وسط الإهمال يستطيع أن يرفع أعمال الوكالة على أحسن وجه، ويقدم مستوى من النظرة الشمولية قد يقصر عنها شبح موظف. ومنذ أن قام محامو نمان

بمسا عدته في تقصي المشكلات، المتصلة بأبحاث الشيفرة في الجامعات، كان ثمة سلسلة من المحامين الأذكياء، والشباب نسبياً قد شغلوا هذا المنصب مدة ستين، ثم انتقل كل منهم إلى عمل آخر.

كان ستورات بيكر يناسب هذا القالب. ولد بيكر عام 1947 ونشأ خارج ديترويت، والتحق بكلية الحقوق في جامعة كاليفورنيا بلوس أنجلوس، وعمل ككاتباً لدى قاضي فيدرالي، ثم مل س المحاماة في مكتب ستيتو وجونسون، وهو واحد من أبرز مكاتب المحامين في العاصمة. وعمل بضع سنوات في وزارة التعليم في عهد جيمي كارتر، ثم عاد إلى مكتب ستيتو. ولما تم ترشيحه لوظيفة وكالة الأمن القومي، تردّد في قبولها، وسأل أحد أصدقائه العسكريين: «هل أقبل بها؟» فأجابه صديقه: «هل ثمة عمل أفضل يمكنك القيام به من أجل خدمة بلادك؟».

لم يكن قد مضى شهر واحد على تسلّم بيكر لمنصبه الجديد عندما زاره كلينت بروكس. وكان جلياً أن لموظف العتيد في وكالة الأمن القومي والنحيل ذوالفك المربع - كان مؤمناً حقيقياً - لكن بماذا؟ وقبل أن يتحدّث، وضع بروكس قارورة كبيرة من شراب آدفيل على مكتب بيكر. وقال: سوف تكون بحاجة لهذا».

بعد ذلك، عرض بروكس قصة كيف أصبحت الكريبتوجرافيا شعبية بحذافيرها. وأخبر بيكر عن معيار تشفير البيانات، والشيفرة المنيعة التي غدت أكثر انتشاراً مما توقعت وكالة الأمن القومي، وتطورا لمفتاح العام، وخوارزمية رسا، والمشكلات التي تُعاني منها الوكالة مع جماعة المشتغلين بالكريبتوجرافيا الجُدد والتي أدت إلى تعرّض عملية مراجعة الأبحاث قبل نشرها للخطر. ثم قال: والآن إنا لفكرة القائلة بأنك تستطيع السيطرة على الأمور بالتدقيق في الأبحاث العلمية لم تعد مناسبة: فشركات مثل آر إس إيه تبيع الشيفرة على

نطاق تجاري. كان بيكر يستمع مشدوهاً. وأراد أن يعرف: كيف تركتم ذلك الأمر يفلت من أيديكم؟

أوضح بروكس أن الأمر لم يكن بهذه السهولة، فوكالة الأمن القومي تضطلع بمهمتين أولاً طبعاً، حل رموز الرسائل المشفرة، وتزويد بقية أجهزة الحكومة بالكثير من المعلومات الاستخبارية ذات الأهمية البالغة لها. أما المهمة الأخرى فهي تزويد الولايات المتحدة بأفضل ما يمكن من الشفرات. وداخل السياج الثلاثي كان يشار إلى هذه الثنائية بـ «التوازن»، وهذا يعكس، بلا ريب، تساوي كلتا المهمتين في الأهمية. وكان كلينت بروكس هو رجل التوازن في الوكالة. وكان تحقيق التوازن عملاً لا ثناء فيه ولا شكر، لأن التقدم في إحدى المهمتين، قد يضر بالمهمة الأخرى أحياناً. في الماضي، على الأقل، كانت النقاشات محصورة داخل القلعة، لكنها الآن تجري في قاعات الكونغرس وعلى صفحات النيويورك تايمز. وفي غضون ذلك، كان شبح التشفير الواسع الانتشار مثل قطار خرج عن مساره مندفعاً ليس نحو وكالة الأمن القومي وحسب بل نحو المجتمع بوجه عام أيضاً. ومثلما فعل زعران الشيفرة، أنعم كلينت بروكس النظر في المستقبل ورأى الشيفرة تنتشر في كل مكان. لكن بينما تقبل ثوار الشيفرة هذه الرؤية بسرور، فإن بروكس فهم أن هذا الواقع الجديد، ينطوي على كارثة محتملة، إذا لم تتكيف الوكالة معها.

تلك كانت حقيقة قاطعة لا ريب فيها، راح بروكس يبثّر بها لسنوات عديدة، وكانت تصطدم في البداية بأذان صماء. وخلال معظم فترة الثمانينات، بعد تلك المناوشات الأولى بين المدير إنمان وأكاديمي الشيفرة، فإن غالبية العاملين في الوكالة لم يكن يعينهم كثيراً احتمال أن يكون للكريبتوجرافيا الشعبية كبير أثر عليهم. وكانوا مطمئنين إلى أن الأمور ستظل تحت السيطرة بفضل قوانين التصدير الصارمة فهي الضامن ألا يغادر شيء بقوة معيار تشفير البيانات دون قيود. وفي أوج الحرب الباردة، كان الكونغرس يقدم للقلعة كل ما تطلبه

على الدوام. ومع أن الأمر لا يخلو من أن يطلع من أهل الدار، بين الحين والآخر بالندير بنبوء أحد العلماء بانتشار الشيفرة في أوساط التجارة على نطاق واسع في غضون عامين أو ثلاثة، دون أن يبدو أنها ستحقق. وهكذا كان من اليسير أن يعتقد المرء أن هذه النبوءة قد تتحققاً أبداً. لكن بروكس كان يعلم أن الأمور تجري عكس ذلك. وابتداءً من عام 1988، توصل إلى فهم الاتجاه الذي كانت تأخذه الإنترنت وأدرك أن الخطر مائل حقيقة هذه المرة. لكن و ساءه ضحكوا عندما حاول أن يعظهم حول الخطر القادم. وكانوا يقولون له: أي خطر تتحدث عنه؟! ننا الكريتوجرافيون لحو حيدون، وليس في الميدان سوانا! وهذه تكنولوجيا عسكرية، وليست شيئاً يرغب لنا س في استخدامه! ولكن حينما أضحت ثورة الإنترنت جديرة بالتصديق، وشرعت شركات مثل لوتس، بوضع برامج تشفير مثل رسا ضمن منتجاتها، تحققت الوكالة على أعلى مستوياتها من وجهة رأي بروكس. ولذلك كان تكليفهم إيّاه بإيجاد حل لهذه المعضلة. ولقد خرج بروكس بالحل.

كان هذا هو السبب الذي حمل كلينت بروكس، على القيام بزيارة لستيوارت بيكر، ومحاولة إشراكه في الخطة. وأوضح له أن ثمة مخرجاً من الورطة... وهو حل لا يقدم للجماهير شيفرة منيعة توفر حماية لا مثيل لها سابقاً وحسب، بل يحفظ للحكومة كذلك القدرة على حيازة النص الواضح الأصلي للمحادثات والمرسلات. والواقع، أنه خلال السنوات الثلاث الأخيرة، كشف بروكس، عن أن وكالة الأمن القومي تعمل على ابتكار مثل هذا البرنامج. وكان يقتضي ضمناً توفير تقنية تُعرف باسم وديعة المفتاح Key Escrow.

كان المشروع قد بدأ في عام 1989. وكان بروكس بوصفه رجل التوازن في فوت ميد يقدح زناد فكره ليكتشف طريقة للتوفيق بين مطلبين متعارضين: الحاجة إلى شيفرة عامة منيعة وحاجة الوكالة إلى طريقة للوصول إلى الرسائل

الواضحة. وكان جلياً أنه ليس هناك من حلّ كامل. وكان الهدف الذي يسعى إليه هو تحقيق التوازن المناسب، بما يتيح لمستخدمي المعلومات غير المحظورة سواء داخل الحكومة أم خارجها درجة قوية من الأمن، لكن ليس إلى حد انتهاك أمن الجمهور. وفي الوقت الذي كانت فيه وكالة الأمن القومي قد شكّلت مجموعة العمل المختصة بالكريبتوجرافيا بالاشتراك مع المؤسسة القومية للمعايير والتكنولوجيا وفقاً لمذكرة التفاهم الموقعة بينهما. وقد وجد بروكس في راي كامير مدير المؤسسة القومية للمعايير والتكنولوجيا بالوكالة أخاً روحياً له، فراحا يمضيان الساعات الطوال، في استعراض جوانب المشكلة معاً، ويسبران النواحي التقنية، وحتى الفلسفيّة لسة الشيفرة.

وفي إحدى مناقشاتهما الأولى، توصل كل من بروكس وكامير في وقت واحد إلى ما يشبه الكشف: إن استخدام التشفير سيكون له تأثير عميق على حفظ الأمن والنظام، وخاصة من حيث قدرته على مواصلة التنصت عبر الأسلاك. وشرعا في زيارة أشخاص معينين في وزارة العدل ومكتب لتحقيقات الفيدرالي، ولم يكن لدى أي من هؤلاء أدنى معرفة بالمشكلات التي ستعرض لهم مستقبلاً. وعندما كان بروكس أو كامير يخبرهم أن جميع إجازات التنصت في العالم قد لا تفيدهم عندما يستخدم المحتالون التشفير، كانوا يقابلون هذه الأقوال بالدهشة. والمسؤولون عن تطبيق القانون يسألون: أليس بإمكانك مساعدتنا؟

إفترض بروكس ذات مرّة، أن الحل ربما يكمن في عملية تضليل جبارة. فبإمكان الوكالة ابتكار نظام تشفير قوي، إلى الحد الذي يحمل لشركات التجارية على إدخاله بين منتجاتهم، وتصديره إلى كافة أنحاء العالم. لكن الوكالة ستبني في داخله «باباً سرياً»، ل يتيح لها استخلاص النصوص الواضحة من البث المشفّر خفية. لكنه بعد أن تروى في الأمر ضرب صفحاً عن تلك الفكرة الخطرة والمشكوك في قانونيتها. وإن مشروعاً كهذا يستلزم الحصول،

على رسائل غير مشفرة من مواطني الولايات المتحدة. وقد تكون قادراً على تبرير باب سري لتستطلع أخبار الأجانب وتتطفل عليهم، ولكن إذا ما اكتشف الكونغرس أو كاتب من كتاب التحقيقات، بأن وكالة الأمن القومي، قد أطلقت خطة مراقبة سرّية على الأمريكيين، فستبدو لجنة السيناتور تشيرتس أمراً سهلاً.

وهكذا قضى بروكس ليالٍ بكاملها لا يغمض له جفن، ليحضر في ذهنه فكرة أخرى. وفي إحدى تلك الليالي، لاح له وميض. فقد وجد أن بالإمكان الوصول إلى حل وسط يمكن أن يرضي الجميع. ففي العالم الحقيقي نجد أن مذكرة التفتيش، تجبر مشتبهاً به في جريمة على تقديم تركيبة مفتاح الخزينة للسلطات. ولماذا لا تتم ترجمة ذلك المفهوم في عالم الاتصالات والكمبيوتر؟ فإذا ما ابتكرت نظاماً يمكنك بصورة خاصة من الحصول خفية على نسخة طبق الأصل عن مفاتيح التشفير وتخزينها في مواقع مأمونة، فإنك ستكون بالضرورة محتفظاً بتركيبات الأقفال بشكل وديعة غير متاحة لأحد سوى أولئك الذين لهم الحق باستعادتها. وبإمكان هؤلاء بما لديهم من سلطة قانونية - مذكرة تفتيش من قاضٍ أو مجموعة مفهومة من معايير الأمن القومي - الحصول على المفاتيح من موقع التخزين الموثوق به. ومتى كان الوصول إليها مضموناً فليس ثمة مشكلة في أن يسمح للتشفير ذاته أن يكون قوياً مثلما يرغب الجميع. ولتجعله غير قابل للتفكيك! وإذا ما كان مكتب التحقيقات الفيدرالي أو الشرطة بحاجة للمفتاح، وتم نيل موافقة القاضي، عندئذ سوف يتوفر لديهم الشيء الذي يتمكنون به من حل الشيفرة، وكأنهم كانوا المتلقين المقصودين باستلامها.

وبالنسبة لبعض من في الوكالة، كان المشروع بدعة، فقالوا: «إنك سوف تضع باباً سرياً في نظام التشفير... ثم تخبر الناس عنه؟» لكن كشف السر كان جزءاً بالغ الأهمية في رؤية بروكس. لقد كان يريد حقاً لهذا المشروع الجديد أن يبدأ مناقشة شاملة في البلاد حول الكريبتوجرافيا. وكان يذهب إلى الاعتقاد بأنه

عندئذ وحسب، سيكون بالإمكان إقامة مشروع الوديعة، الذي يتطلب بنية تحتية معقدة. ولما كانت الحكومة غير حريصة على وضع يدها على الرسائل المشفرة، فإن الطريق سيكون حراً وواضحاً باتجاه غطاء عالمي من الشيفرة، مع تنظيم توزيع المفتاح العام، وتوقيعات رقمية معيارية، وتشفير آلي للرسائل. وسيشير المهورسون بالسريّة، وحبك المؤامرات جحيماً إزاء فكرة المفاتيح الوديعة. لكن إذا ما عرضت جميع القضايا على الملأ، وتمت مواجهة الأخطار جميعها، وحددت جميع الفوائد، فمما لا ريب فيه أن العقلاء من الناس بإمكانهم أن يروا أن هذه الخطة، هي الطريق الأفضل لحماية اتصالاتنا دون أن نضحى بأمننا. وعلى أية حال، ماذا كان البديل؟

وبالطبع، لو قُيِّض لمشروع كهذا أن ينطلق، فإن على وكالة الأمن القومي نفسها، عندئذ، أن تتغير، وتعُدّل من تركيز اهتماماتها بحيث تعمل في عالم ما بعد الحرب الباردة المحوسب والمشفر إلى أبعدا لحدود. فالشدة التي ما تزال القلعة تحتفظ ببرقعها من التكتّم والسريّة لم يعد مناسباً. وإذا ما كان الناس سيقبلون فكرة متطرفة كهذه، فينبغي على وكالة الأمن القومي أن تنال ثقتهم. وهكذا كان من الضروري عرض لمناقشات حول الكريبتوجرافيا أمام الجمهور، ليظاً مناطق كانت ذات مرة أرضاً محرّمة بصدق قاس ومؤلّم.

وفي آخر الأمر حصل بروكس على الموافقة لمتابعة خطته، لكن فكرته القائلة بوجود تعاون وكالة الأمن القومي مع الجمهور استقبلت بارتياح أو ما هو أسوأ من ذلك. ووجد نفسه يجادل كالمتشائم المشوش الفكر. وحالما قابل بروكس أعلى مسؤولين في وكالة الأمن القومي، قال: «يجب أن تكون هذه سياسة قومية». وعندما طلب منه المدير المساعد أن يزيد في الشرح، أجاب: «هذا ليس حكماً يمكن أن يصدره مدير وكالة الأمن القومي أو لجنة من المعاونين. . . إن تعريف مصلحة البلاد مسألة تقدير، حكم قيمة. ولا بد أن يكون رئيس الولايات المتحدة هو صاحب القرار فيها. المسؤول الذي يتحدّث

إلى ناخبه مباشرة! ولقد اعتقد أقرانه بأنه بالغ في تصوراته، إذ كان موقفهم؛ هذه وكالة الأمن القومي، ونحن لا نقوم بعمل كهذا.

وفيما كان ينتظر أن تتخذ المناقشة العامة شكلاً معيناً، كان بروكس يعمل بجد مع وكالات أخرى، من أجل إقامة بنية لخطوة وديعة المفتاح الطموحة التي يعدها. وبسبب من مذكرة التفاهم، طبعاً، فإن على الوكالة أن تطور الخطة مع المؤسسة القومية للمعايير والتكنولوجيا. لكن ذلك لم يكن مشكلة تُذكر. فقد كانت مجموعة العمل التقني المشتركة تعمل على وضع الشيفرة العامة، منذ أول اجتماع لها في آذار/ مارس من عام 1989، خاصة على خوارزمية التوقيع الرقمي. وكانت الشيفرة العامة تعرف ضمن المجموعة بالقضية الأولى.

أما الطرف الثالث في المناقشات فقد كان مكتب التحقيقات الفيدرالي. ذلك أن الإنذار المبكر الذي أطلقه كل من بروكس وكامير أيقظا اهتمام لدى المكتب: ففي عام 1991 كان المدير وليام سيشوننس قد كتب إلى وزيراً للدفاع ديك تشيني حول أمن الكمبيوتر، مشيراً بجلاء إلى أن وكالته ترغب في أن يكون لها صوت مسموع في تحديد السلسلة. واتضح أن مكتب التحقيقات الفيدرالي سوف يتخذ حقاً الخط الأكثر تشدداً في المسألة.

وبالطبع فإن وكالة الأمن القومي، نهضت بأعباء الجانب التقني. وبحلول عام 1990، كان ثلاثون مختصاً بالرياضيات لديها، يعملون على معالجة المسألة. وقد استقر ربهم سر يعاً على أساس الوطيد الذي يستند إليه النظام، خوارزمية تشفير متينة كانت موضع دراسة ونقاش من فورت ميد لمدة سنتين، يرمز لها باسم سكيجاك Skipjack الوثاب [نوع من سمك التونة هـ. م] وكانت كتلة تشفير مثل معيار تشفير البيانات (ديز) لكن أقوى منه. فطول مفتاحها الموصى به 80 بت مقابل 56 لمعيار تشفير البيانات؛ وكانت تستخدم 32 دورة استبدال بدلاً من 16 دورة التي استخدمها معيار تشفير البيانات. (ويلوح كذلك أن ثمة المزيد من الأسباب التقنية الحاذقة لتفوق الوثاب، لكن بالطبع، كانت

وكالة الأمن القومي، تنفر من الكشف عنها). ولئن حاول بروكس أن يبرهن أنه من المناسب في هذه الحقبة الجديدة أن يتم الكشف عن الخوارزمية - وأصر، في الواقع، على أنهم إذا ما أرادوا التغلب على منتقديهم، فسيضطرون إلى نشرها، إلا أنه لاقى مقاومة قوية. فلن تسمح الوكالة مطلقاً لأعدادها بالدخول، إلى ما هو أشبه بدورة متقدمة في كتابة الشيفرة. ذلك أن الأمور لا تسير على هذا النحو في القلعة.

كان الوثاب، مع ذلك، مجرد مكون واحد لما تطلق عليه وكالة الأمن القومي القمة Capstone، والذي كان نظام مفتاح عام كامل يتضمن معيار التوقيع الرقمي. وبالطبع، كان هذا المشروع بالأخص ينطوي على تعقيد إضافي آخر: كيف يمكنك أن تطبق نظام الوديعة؟ يجب عليك أن تكتشف طريقة تعزل بها نسخة من كل مفتاح وترسل تلك المعلومات إلى مكان آخر ليتم تخزينها. وبحلول عام 1991، استقر رأي وكالة الأمن القومي على أن محاولة القيام بهذا العمل في برمجيات محفوف بالكثير من المخاطر - وخشيت أن يتمكن عدو ما من تغيير الرمز لإضعافه من الداخل - وخلصت إلى استنتاج مفاده أن الطريقة الأفضل تتمثل بأن توضع المسألة كلها على رقاقة كومبيوترية لا يمكن العبث بها. وتم التعاقد مع مقال متمرس يقوم بمشاريع لحساب وزارة لدفاع في تورانس بكاليفورنيا يدعى مايكوترونكس، ليقوم بتصنيع الرقاقات.

وكان النظام ذاته، يعمل بإدخال عدة مكونات جديدة في المعادلة الكلاسيكية حيث تقوم أليس بكتابة الشيفرة وبوب بحلها. وكان أحد هذه المكونات «معرف الرقاقة الفريد» وهو عدد مكافئ لمفتاح الرقاقة الفريد المخصص لرقاقة واحدة. ولكل جهاز - سواء كان كومبيوتراً أو ربما هاتفاً - معرف الرقاقة الفريد ومفتاح الرقاقة الفريد الخاص به.

وحينما يرغب شخصان بالاتصال ببعضهما بصورة شخصية، فإنه يتعين على كل منهما أن يكون لديه إحدى هذه الوسائل، إذا شاء مثلاً إجراء مكالمة

هاتفية على نحو لا يدع مجالاً لأحد للتنصت عليها، فإن عليهما أن يمتلكا أجهزة هاتف ذات خصائص تكنولوجية معينة. ومتى تم الاتصال بين الطرفين، قام الجهازان بتحويل المكالمة بين الطرفين، إلى إشارات رمزية (بواسطة طريقة ديفي - هيلمان للتبادل) من أجل حساب مفتاح متماثل جديد، يدعى مفتاح الجلسة. وباستخدام الوثاب يمكن لذلك لمفتاح، أن يشفر الأصوات التي يطلقها كل متحدث عندما تغادر تلك الأصوات جهاز الهاتف، ويفكك تلك الأصوات عندما تنبثق من الهاتف الآخر. ولكن مع المحادثة المشفرة فإن أجهزة الهاتف سوف تبث مجموعة أخرى من البتات تدعى مجال مدخل حفظ النظام LIAF Law Inforcement Access Field. (وكان قد دعي أصلاً مجال استغلال حفظ النظام، لكن تم تغييره إلى عبارة أقل مدعاة للضيق). ويمكن توليد مجال مدخل حفظ النظام، بمجموعة من الحسابات تشتمل على مفتاح الجلسة، ومفتاح الرقاقة الفريد، وعمرّ ف الرقاقة الفريد، ملفوفة مع عنصرين هامين: نسخة مشفرة من مفتاح الجلسة، وعمرّ ف الرقاقة الفريد. وهذه المكونات جميعها سوف تخضع لمزيد من التشفير بواسطة مفتاح العائلة.

لذلك كيف بوسع المسؤولين الحصول على هذه المفاتيح؟ الحق أنهم يمتلكون أحدها أصلاً، مفتاح لعائلة، وهو مفتاح وحيد لا ثاني له في النظام كله. وإن الجزء الحرج في المشروع يتمثل في الحصول على مفتاح الرقاقة الفريد المناسب، وفي النهاية، مفتاح الجلسة. وهذا يمكن القيام به بواسطة مجال مدخل حفظ النظام.

لكن ماذا لو أن أحد المتنصتين تمكن من لتقاط المعلومات الخاصة بمجال مدخل حفظ النظام؟ إن جهوده سوف تذهب سدى، حتى ولو استطاع عزل عمرّ ف الرقاقة من المجال. ذلك أن كل ما سيقوم به المعرّف، حقاً، هو التعريف. إذ يشير إلى مفتاح الرقاقة الفريد ضمن قاعدة بيانات واسعة. لكن المتنصتين لدى الحكومة المزودين بكل مفتاح رقاقة فريد في الوجود، وخدمهم

الذين يستطيعون الوصول إلى قاعدة البيانات تلك. إن امتلاك ذلك لمعزف دون وجود طريقة للدخول في تجهيزات الوديعة سيكون أشبه بالحصول على بصمة أحد هم دون الوصول إلى سجلات الوقائع الجرمية: إذ لا طائل من إخبارك عن الشخص الذي تعرف عنه. لكن بمقدور موظف حكومي أخذ ذلك المعزف مع أمر قضائي، إلى تجهيزات الوديعة، ومطابقتها مع مفتاح الرقاقة الفريد. ومن ثم يضمه إلى المفتاح العائلي. إذن هاكم الحل! فلسوف يكون لديك مفتاح الجلسة - ويمكن لمحادثة مشفرة يكتنفها لغموض، أن تتحوّل إلى لغة واضحة مباركة، أو ربما شهادة إثبات جرمية.

وقد أدى هذا بدوره إلى تعقيد آخر: أين تخزن مفاتيح الوديعة؟ وإذا ما تم الاحتفاظ بها كألهافي مكان واحد، فستكون بمثابة منجم ذهب لكل نصّاب وجاسوس، بل وموظف فاسد، فحكومة الولايات المتحدة، وبمقدور أي شخص يملك الدخول أن يحصل على جميع الوسائل الكفيلة بانتهاك سرّيّة كل محادثة مشفرة في العالم. وهكذا قرّر بروكس وزملاءه أن يتم تقسيم مفاتيح الوديعة إلى قسمين يخزانان في مواقع مختلفة. ويمكن القيام بذلك بحيث أن الحصول على أحد أجزاء المفتاح لن يوفر أية فائدة رياضيّة لاكتشاف المفتاح بأكمله. وحينما يسمح قاض بالتنصّت، فإن الموظف المسؤول عن تطبيق القانون سيقدّم المذكرة إلى كلا موظفي الوديعة، ويركّب المفتاح، وبذلك يتمكن من الإستماع إلى المحادثات.

وفي أواخر تموز/ يوليو 1991، التقت الوكالات الحكومية ذات الصلة بالموضوع كافة لتعقد اجتماعاً خارج مقراتها في دائرة الأبحاث الهندسيّة التابعة لمكتب التحقيقات الفيدرالي في كوانتيكو، فيرجينيا، للبحث في البدائل لسياسة تشفير قومية. وقد ألقى كلينت بروكس كلمة الاستهلال في الاجتماع. وهذا ما سجّله أحد الموظفين من الحضور:

قدم هذه [البدائل] ضمن سياق هدف قومي يلبي الحاجة إلى أمن

كربتو جرافي تجاري وغير محظور بينما مصالح مسؤوليات الأمن لقومي ومنظمات حفظ النظام في أمان. وأطلق على إنجاز هذا الهدف اسم «نيرفانا». [مصطلح في الفلسفة الهندية، والبوذية يعني السعادة المطلقة ه. م].

لم تصل الوكالات إلى اتفاق تام. ومن الجدير بالذكر، أن مكتب التحقيقات الفيدرالي دعا على ما يبدو لامتلاك القدرة على فكّ التشفير الخاص به على الفور. أو في «زمن واقعي» وهذا نهج رأى فيه جماعة المؤسسة القومية للمعايير والتكنولوجيا «وحشية وتطفلاً». (إن من شأن اتباع نهج مكتب التحقيقات الفيدرالي أن يملئ أوامره بأن تسهيلات الوديعة يجب أن تكون مكالمة هاتفية في أي وقت من الأوقات، وسيرمى بالضوابط ضد سوء الاستعمال من النافذة). لكنهم تفقروا جميعاً أن النظام المقترح يجب أن يوفر التشفير للجمهور بينما يتيح لرجال لشرطة والأشباح الوصول إلى المفاتيح - ويشكل أساساً كان هذا هو الحل المقدم من وكالة الأمن القومي.

بقي مشروع الوديعة مجرد تكنولوجيا، تخطف الأبصار، معدة وراء السياج الثلاثي، إلى أن اكتشفت الحكومة كلها سره. ولكي يعمل، كان من الضروري، أن يكون كلي الوجود. وكما كان بروكس قد توقع - وأدرلثرو ساؤه أخيراً - فإن تغييراً شاملاً كهذا بحاجة إلى الموافقة والدعم الفعّال من أعلى مستويات الحكومة، وصولاً إلى الرئيس جورج بوش ذاته. ولكن موعد الانتخابات كان يقترب، والوقت ليس مناسباً لطرح أفكار جديدة قد تثير الجدل على الملأ. وعلى أية حال، بدا أن جماعة بوش لم يكونوا مقتنعين بضرورة القيام بعمل سريع. حسب بروكس أنه في عام 1993، بعد عودة بوش إلى البيت الأبيض، فإن الرئيس المعاد انتخابه، سيكون قادراً على معالجة المشكلة، وهو متحرّر من القلق إزاء ما قد يفكر به ناخبوه.

لكن في عام 1992، وقع حادثان لم يكونا في الحسبان، حدّدا مجرى الأمور بشأن مشروع وديعة المفتاح بشكل دراماتيكي. وقد تضمّن الأول مُنتجاً

مبتكراً على وشك أن يدخل السوق، صندوق زنته اثنتين وعشرين أونصة مرتبط بجهاز هاتف. ولقد أُنذِر ذلك الرطل والنصف من التكنولوجيا، بأطنان من المشاكل. أما التطور الثاني الذي طرأ، فكان انتخاب رئيس جديد للولايات المتحدة.

كان لا سم التقني للصندوق إيه تي أند تي جهاز الهاتف المأمون AT & T Telephone Security Device (TSD) 3600 (تي إس دي) 3600. ولعدسنا نتكانت تلك الشركة العملاقة في وسائل الاتصالات عن بُعد، تزود الحكومة بهواتف مأمونة، مستخدمة في ذلك خوارزمية خاصة صممتها وكالة الأمن القومي. وفي عام 1992، قرّرت الشركة توسيع سوقها إلى خارج الحكومة، وبذلك مبيعات محدودة لمشفّر بيانات صوتية. استخدام خوارزمية تشفير ابتكرها فريق الشيفرة الخاص بالشركة. وفي ذلك الخريف، قرّرت أن تواصل ذلك على نطاق أوسع أيضاً - بإطلاق هاتف مأمون مصنع ليبيع منه بالآلاف. وإذا ما كنت تشعر بالقلق إزاء متطفلين يتصوّنون على بيانات حساسة تتضمن ملكية فكرية، ومسائل تجارية، واستراتيجيات مشروعات عمل، فإنك ستكون بحاجة إلى واحد من هذه الأجهزة. ولا ينبغي أن تكون مهندساً أو جريئاً تتخذ منه. وتدققت أديبات الشركة معلنة أنه «يرتبط بسهولة بأجهزة الهاتف المكتبية أو... أجهزة الهاتف الخليوية، كما أنه سهل الاستخدام فإنه قابل للحمل والنقل أيضاً. ومن أجل حماية المكالمات، ما على المستثمر سوى أن يضغط زرّاً واحداً. فيتم تشفير المكالمة بشكل آلي، وتصبح المحادثة مأمونة». كذلك زعمت لشركة بأن نوعية الصوت على هذا الجهاز، بخلاف الهواتف المشوشة نسبياً التي يستخدمها الجيش، جيدة مثل جهاز هاتف عادي تقريباً.

وما هو أكثر من ذلك، أن الهاتف الجديد هذا يستخدم خوارزمية التشفير الأكثر ثقة لتشفير الصوت: معيار تشفير البيانات تلك الشيفرة التي كانت ما تزال موضوعاً ساخناً خلف السياج الثلاثي.

كانت وكالة الأمن القومي، غير راضية عن الاستخدام الجديد هذا للطفل المشكلة الذي كانت قد باركته ذات مرة. لكن أخبار خطة إيه تي أند تي كانت مصدر قلق أكبر لمكتب التحقيقات الفيدرالي. وكان سبق لوكالة حفظ النظام هذه أن تدمرت من الميزات الجديدة للهاتف، مثل الخدمة الخليوية كانت تزيد من صعوبة القيام بالتنصت. وارتأت أن الحل يكمن في اقتراح مشروع قانون جديد يُعرّف داخل ضاحية المكاتب ببساطة بـ «الإرسال الهاتفي الرقمي» Digital Telephony. وهذا القانون يلزم [الشركات] بأن يتم تصميم جميع معدات الاتصالات الجديدة بشكل يلحظ توفّر ما يساعد على التنصت. وأن يحظر القانوناً لمعتزم إصداره كل الأجهزة والخدمات الجديدة التي تحرم الحكومة من فرصة ميسرة للإشراف والمراقبة. وكان المنتقدون قد أخذوا يولولون في ذلك الوقت. فحسبك أن مشروع القانون الجديد سيكبد صنّاع التجهيزات مئات الملايين من الدولارات (تكلفة يفترض أن يتحمّلها المستهلك). ولأ سوا من ذلك الفكرة الأساسية التي كانت وراء التشريع، التي يقصد بها أن يلف ذنب المتنصتين كلب الاتصالات عن بُعد. وبدلاً من تشجيع واحدة من أكثر الصناعات ابتكاراً على إنتاج أنظمة تدعم نجاح التقنية المتطورة لأمريكا في السوق العالمية، تجد أن الكونغرس سوف يعمد إلى تقييد التجديدات بالسلاسل والأقفال. ومن أجل ماذا؟ لتبقى أذناه مفتوحتان على حوالي 1000 سلك تنصت فيدرالي سنوياً، لجمع معلومات يمكن الحصول عليها بوسائل أخرى، مثل أجهزة التنصت المخفية أو المخبرين؟

ومع أن الإرسال الهاتفي الرقمي، لم يأت إلى ذكر الكريبتوجرافيا على وجه التخصيص، فإن شبح قيود الشيفرة سيكون سفيراً مصلتاً على التشريع مثل سيف ديموقليس. وكما كان كل من بروكس وكامير قد بيّنا لمكتب التحقيقات الفيدرالي، فإن الشيفرة المنيعة تستطيع أن تستجمع مزايا القانون على أكمل وجه. وحتى إذا ما تم إقرار الإرسال الهاتفي الرقمي، والتزمت الصناعة

بقيوده بإخلاص، فيكون رجال الحكومة، ودوائر الشرطة الأخرى، قادرين على مراقبة البث المُرسَل عبر الأسلاك أو الجو، ولكن ماذا سيحدث بعد هذا؟ إذا كانت الاتصالات مشفرة فإن هذه الأجزاء المعترضة الغالية، لن تكون ما يزيد على تشويش عديم الجدوى. ولقد فهم مدير مكتب التحقيقات الفيدرالي وليام سيشونسلر سالة وتأكد من أن رجال الحكومة سيكونون مساهمين في الجهد، الذي ستبذله وكالة الأمن القومي، والمؤسسة القومية للمعايير والتكنولوجيا لمعالجة المشكلة.

أخذ مكتب التحقيقات الفيدرالي يتصرف الآن على نحو غريب. ها هو جهاز هاتف الإيه تي أند تي الجديد، المصمّم من أجل أن ينقل تكنولوجيا الهاتف لمأ مون من رمز يشير إلى المكانة في مكاتب مستشاري الأمن مجلس القومي إلى منتج تجاري شائع، يستخدمه مدراء لشركات والهيئات، ولمحامون، والعلماء، ناهيك عن المهووسينها لسريّة، والنصابين، والإرهابيين، ويعلم الله من سواهم. وسيكون وبالأعلى حفظ النظام... ما لم يكن ثمة وسيلة تمكّن الحكومة من أن تنصّت بطريقة ما على تلك المكالمات كما كان شأنها قبل التشفير. ألم يكن ذلك ما سبق لكلينت بروكس أن اكتشفه؟ وهكذا فقد سئل بروكس وفريقه ما إذا كان من المحتمل أن تدخل رقاقة لقمة في جهاز هاتف إيه تي أند تي. وكا نت رقاقة القمة في صورتها الأول أقوى من أن يتحمّلها جهاز إيه تي إس دي 3600 - [فالرقاقة] بكل ميزاتها، كالتوقيع الرقمي، تتطلب طاقة كومبيوترية تفوق ما يتطوّر الجهاز القيام به. لكن إذا ما نحتت وكالة الأمن القومي، بالجهد المتواصل خوارزمية التشفير ومفتاح الوديدة فمقدورها أن تخرج بشيء يمكن أن يثبت في جهاز الهاتف بدلاً من رقاقة معيار تشفير البيانات.

كان بروكس قلقاً، حتى حينما كان يوافق على إمكان القيام بذلك. فلقد كا نت رقاقة القمة حسنة التصميم، وتقدّم حلاً كاملاً. وكان في طرح حل جديد

مجازفة أكبر - وللقيام بذلك في الوقت المناسب لخرق هاتف إيه تي أند تي، ينبغي تنفيذه بسرعة كبيرة. ولن يكون هناك متسع من الوقت، لإجراء مناقشة قومية كان يشعر بأنها أساسية جداً.

لكن مكتب التحقيقات الفيدرالي لم يكن بمقدوره الانتظار. ففي 13 تشرين الأول/ أكتوبر 1992، أجرى القاضي سيثونس اتصالاً هاتفياً مع المدير التنفيذي في شركة إيه تي أند تي روبرت ألن، وأخبره بمواجهته مشكلة، ثم أوجز له المشكلة والحل: هل ستفكر الشركة في استخدام رقاقة تشفير وديعة، عوضاً عن نظامها المستند إلى معيار تشفير البيانات؟ وإذا ما وافقت الشركة على ذلك، فبمقدور الفيدراليين تقديم مكافآت كثيرة. وبإمكان إيه تي أند تي الادعاء بأنها كانت توفّر حقاً تشفيراً أقوى، بما أن تفكيك الدخلاء لرموز الوثاب كان أكثر صعوبة من حل رموز معيار تشفير البيانات. علاوة على ذلك، فالمرجح أن الولايات المتحدة، سوف تسمح بتصدير هاتف وديعة للمفتاح هذا. والأفضل من هذا كله كان وعلاً للشركة ببلوغ المراد: أي أن تشتري الحكومة آلاف الوحدات لاستخدامها الخاص.

إن الوجه الآخر، طبعاً، سيكون على المشتركين المحتملين، أن يشتروا في ظلّ التسوية لأساسية التي استلزمها الوديعة: سيكون التشفير قوياً، لكن طرفاً ثالثاً ليس موضع ترحيب بالضرورة سوف يكون لديه نسخة من المفتاح.

هل يبدو ذلك مألوفاً؟ إنه الوضع ذاته الذي كان هويت ديفي قد وجد، أنه لا يمكن تحمّله على الإطلاق قبل عقدين من الزمن: الصعوبة التي يجدها شخصاً ينشُدان علاقة حميمة في حين أن شخصاً آخر في الفراش. ولقد ابتكر ديفي المفتاح العام لتفادي إساءة استعمال العلاقة الكريبتو جرافية. والواقع، أن هاتف إيه تي أند تي كما تمّ تصوّره أصلاً، كان تجسيدا لرؤية ديفي. فلن يكون مستخدمو الهاتف بحاجة لتبادل مفاتيح سرية سلفاً. وعوضاً عن ذلك، سوف يقوم جهازا الهاتف كل منهما في مكانه الخاص بإعداد الحسابات لتبادل المفتاح

حسب طريقة ديفي - هيلمان، للاتفاق على مفتاح ما مون من معيار تشفير البيانات يشق، ويفك تشفير المحادثة الفعلية. لن يكون ثمة حاجة إلى أي شخص آخر. إنك لن تحتاج إلى شخص آخر. لكن المنحة السخية المقدمة لشركة إيه تي أند تي - والفرصة السانحة لتفادي المواجهة مع الحكومة - كانت رابحة أكثر مما ينبغي بما لا يدع مجالاً لرفضها. ولقد وقّعت شركة الهاتف على اتفاق: إذا تبنت الحكومة خطة لجعل وديعة المفتاح معياراً لها، فإن إيه تي أند تي سوف تتخلى عن مشروعها الذي يستند إلى معيار تشفير البيانات. وتضع في أجهزتها بدلاً منه رقاقة من تصميم لحكومة. وستكون هذه [الرقاقة] هي النسخة المخففة من رقاقة القمة، مستخدمة خوارزمية الثواب وميزات الوديعة، لكن بدون التوقيع أو خوارزميات التجميع. ولها اسم رمزي جديد: المقراض.

قالت محدثة باسم الشركة: «إنا نعلم أن أي قرار لن يحققوا لسعادة للجميع. لكن بصراحة، لقد وفّرت رقاقة المقراض، مسألة هامة تتصل بحفظ النظام وزادت في مستوى الحماية». وعلى نحو أكثر صلة بالموضوع، فإنها ضمنت كذلك قدرًا من المبيعات، والرضا للدائم لأحد زبائن إيه تي أند تي الرئيسيين، أي حكومة الولايات المتحدة (في ذلك الوقت، كانت الشركة تفاوض على عقد حكومي تربو قيمته على عشرة بلايين دولار). وإذا ما أضحت وديعة المفتاحيات حكومية، فإن إيه تي أند تي سوف تكون قد استقرت بسعادة على متن السفينة.

لكن المقراض كان ما يزال أبعد ما يكون عن اعتماده من الحكومة سياسة رسمية. وكان كلينت بروكس ووكالة الأمن القومي بحاجة إلى فرصة أخرى قبل بدء الرحلة نحو لنيرفانا. ولقد تحققت الفرصة لمنشودة في 3 تشرين الثاني/نوفمبر 1992 حينمطو جهت الولايات المتحدة إلى صناديق الاقتراع وانتخب وليام جيفرسون كليتون رئيساً لها، وألبرت جور نائباً له.

وقد يبدو أمراً منافياً للبداهة الاعتقاد بأن نتائج الانتخابات، جاءت في

صالح وكالة الأمن القومي . فبعد كل شيء ، كان كليتون ديمقراطياً قضى سني حرب فيتنام ، يتحدث مناهضاً الصراع بدلاً من أن يقاتل فيه . وإبان الحملة الانتخابية ، كان كليتون قد زار [مجمع الصناعات الإلكترونية] سيكون فالي ، وفي الوقت الذي لم يقطع فيه أي وعود ، إلا أنه أشار إلى أن حكمه سيكون صديقاً للشيفرة الخاصة . ويتذكر المدافع عن السريّة مارك روتنبرج : « لقد عرض لنا مبلغ سخف ، بفرضه قيوداً على تصدير البرمجيات الجاهزة على الرفوف . ولم يقل «التشفير على وجه التخصيص» ، لكن هذا ما كان يشير إليه بكل وضوح» .

ثمة إشارة أخرى إلى أن كليتون ، قد لا يكون صديقاً لوكالة الأمن القومي وهذا يعود لطبيعة الأشخاص المحيطين به . مثلاً ، كان رئيس فريق ترتيب إجراءات انتقال الرئاسة ، عضواً سابقاً في جماعة ضغطتعمل لصالح الصناعات الإلكترونية يدعى جون بوديستا ، الذي كان مؤيداً متحمساً لبرنامج لصناعة لتحرير قوانين التصدير . وإلى جانب بوديستا كان في عداد المحظيين عند كليتون عدد من الأشخاص الذين بدوا متناغمين مع العلماء وعالم التحكم الآلي المناصر للشيفرة .

وكان الأبرز من بين أعضاء الفرقة تلك ، نائب الرئيس ذاته ، أحد المهورسين بلكو مبيوتر والذي أناط به كليتون مهمة اتخاذ القرار النهائي في مسألة الكريبتوجرافيا . والواقع أن وجود آل جور بوصفه الثاني في قيادة الأمة كان ينوّه به على أنه دليل . على أن فريق القيادة الجديدة كان فرقة تناصر الجراءة وتطلع إلى المستقبل ، و«فهمت» نموذج الإنترنت الجديدة . وكانت خطب حملتهم تدور حول إقامة جسور إلى المستقبل ، لكن رؤية جور كانت لطريق معلومات سريعة لنقل البلاد بل الكرة الأرضية إلى حال أخرى . ورتّب جور إحصار بعض مستشاري مجلس الشيوخ الأكثر معرفة بالتكنولوجيا إلى البيت الأبيض للمساعدة في الشؤون الرقمية ، مثل مايك نيلسون ، وهو جيوفيزيائي ، وأستاذ سابق في معهد مسلتشوسيتس للتكنولوجيا ، وخبير متمرس في شؤون

طريق المعلومات السريعة. ولقد كتب جون بيرى الذي تعرف إليهم بحكم كونه مؤسساً مشاركاً في مؤسّسة الآفاق الإلكترونية قائلاً: لقد كانوا «عشاق حرية واعين وأذكياء إلى أبعد حد. إن الكثير منهم لا يسهل قيادتهم. وكنت واثقاً من أنهم بعد انتقالهم إلى مواقعهم بشكل تام، سوف يواجهون وكالة الأمن القومي، ومكتب التحقيقات الفيدرالي بجسارة».

كان بارلو قد افترض على نحو خاطئ، أن أعوان كليتون قد عرفوا افتتاحية «المغنوليا الحلوة»، فإنهم سوف يكونون معفيين من جحيم لمحاضرات السريّة التي اعتاد صبية الشيفرة المزيّنين بالنجوم، على إلقاءها في فورت جورج ميد. وخلفنا لسياج الثلاثي، كما نت التوقعات على النقيض من ذلك تماماً. فقد أدرك الأشباح أن بيل كليتون وفريقه من التقنيين المزهوين بأنفسهم كانوا نعمة من الله من أجل خطة الوديعة. ولم تكن المشكلة إلى حد بعيد أن جماعة بوش كانوا بشكل خاص ضد هذا المشروع على وجه التحديد. فقد كانوا يهضون كل ما يتطلب شيئاً من روح المبادرة. وقال أحد المطلعين يصف الوضع: «كان جماعة بوش [الجمهوريون] قد قضوا اثنتي عشرة سنة في السلطة، معظمها مع كونجرس ديمقراطي، وعلموا أن كل ما يمكن أن ينفجر، سوف ينفجر. وعندما تقدم لهم شيئاً، لن تحصل منهم إلا على عيون تحدّق... يمكنك أن تشعر بأن كل واحد منهم كان يفكر: «ما مدى تأثير هذا على وضعي؟»».

وعلى النقيض من ذلك، كما نت جماعة كليتون من السياسيين المغامرين، أشبه بمراهقين سلم لهم القيادة خيراً. لقد كانوا يشعرون بسعادة غامرة، أنه بعد اثنتي عشرة سنة من حكم الديناصور، سنحت لهم الفرصة لإصلاح الأمور. كذلك كانوا مهووسين بالتفاصيل، وتواقين لاستيعاب الركام الهائل من البنود والهوامش والتوافه التي تجتد عملية الحكم. اعرض لهم فكرة لتجدهم قد أحاطوا بها، وداعبوها، ومزّ قوها إرباً إرباً، واختبروها حتى وجدت أجزاءها

تفرقع، وراحوا يتساءلون كيف بوسعهم جعلها تعمل لصالحهم. كانوا يستمدون الثقة بأنفسهم من إيمانهم بأن نواياهم واضحة، وأنه حتى ولو لم تكمل جهودهم بالنجاح، فإن الجمهور سوف يقرّ لهم بالفضل لمحاولتهم القيام بالعمل الصائب.

لم تنتظر القوى التي تدفع وديعة المفتاح، وصول الإدارة الجديدة إلى البيت الأبيض، قبل أن يصدوا كلاً من كليتون وجور بمشكلة التشفير. وقد وفّرها تف إيه تي أند تي زخماً وقوة دفع لذلك. وفي هذا الصدد يقول ستيوارت بيكر: «فجأة وجدنا أن هذا ليس بالأمر الذي يحتمل انتظار، إعداد بيان موجز منهجي للإدارة الجديدة، وأن ندعهم يلتفتون لتدبير شؤونهم، ويعينوا الوزراء، ويصدروا قراراً في عام 1994». وكانت فكرة جعل جورج بوش يعلن انتهاء البرنامج قبل إخلائه البيت الأبيض قد أخذت بعين الاعتبار، لكنها رُفضت». وكتب مسؤول في مكتب التحقيقات الفيدرالي إلى المدير سيشونس في مذكرة أعدّها في أواخر عام 1992: إننا نعتقد بأن المضي قدماً في تركيب رقافة المقراض بناء على موافقة الإدارة الحالية أمر يعتوره عقبات محتملة. فماذا لو تسرّبت الأنباء عن رقافة «قالبلا ستشار» قبل أن توافق جماعة كليتون على لسياسة بشكل رسمي؟ «وقد يفضي ذلك إلى دفعهم إلى لتصل من منهج إدارة بوش السابقة للحيلولة دون وقوع جدل». كان القاضي سيشونس ذاته، الذي بلغ به الخوف من أن يفقد عمليات التنصت الأثيرة على قلبه حد الاهتمام أو من يبلغ مدينة ليتل روك. [عاصمة ولاية أركنساس، مقر الرئيس المنتخب كليتون هـ. م] ويقول مسؤول حكومي مؤيد لوديعة المفتاح: «لقد أصبحت هذه تتصدّر سلم أولوياته. وكان مقدماً في مخاطبة الفريق الذي يتولّى ترتيب إجراءات انتقال السلطة، فخاطبهم بقوله: «أيها الشباب، لعلكم قادمون في كانون الثاني/يناير، لكن يجب عليكم أن تسمعوا هذا الآن». على أية حال، فإن وكالة الأمن القومي، كانت راضية تماماً عن تصدّره لحملة. ففي

النهاية، لم يكن الدور المعلن المناط بفورت ميد في الحكومة دعم القرارات السياسية، بل توفير خلفية تقنية ومعلومات استخباراتية من ملفاتها.

ولتأطير القضايا، قام مكتب التحقيقات الفيدرالي، بمساعدة من وكالة الأمن القومي، بإعداد بحث بعنوان «التشفير، حفظ النظام، والأمن القومي». وحفلت هذه الوثيقة بسيناريوهات ذات وقع شديد لما قد يحدث، إذا ما تحررت الشيفرة من القيود. وتعرض البحث إلى جهاز إيه تي أند تي، بوصفه محرضاً لهذا الهجوم الضاري. لكن البحث ذهب مع ذلك إلى إمكانية تفادي الكارثة المقبلة. «إن الحل يتمثل في رقاقة تشفير، توفر مزيداً من الحماية للسرّية (قوتها تفوق قوة معيار تشفير البيانات بمليون مرة على الأقل)، غير أنها تسمح لمسؤولي حكومة الولايات المتحدة قراءتها متى أجاز لهم القانون ذلك... إن من شأن نظام «وديعة المفتاح» هذا حماية شركات ومواطني الولايات المتحدة، من انتهاك الأمان الذي يتمتعون به على يد الراصدين المأجورين والمنافسين والحكومات الأجنبية. كما يتيح في الوقت ذاته، للأجهزة القائمة على حفظ النظام ممارسة التنصت على خطوط الاتصال في الظروف ذاتها السارية الآن بمقتضى القانون». ولئن بدا الوصف أشبه ما يكون بدواء عام لمشكلة إن لم نحتاط لأمرها الآن أنت فيما بعد بأعظم الكوارث، فإن البحث عرض لنتيجة واحدة تحمل نذيراً بالشؤم، إن استمرت السياسة الراهنة: إن هذا المفهوم سوف يُهاجم بقوة، من أولئك الذين يخشون إساءة تطبيق القانون وبالتالي فإنهم سيؤثرون الاعتماد على التكنولوجيا على اللجوء إلى المحاكم من أجل حماية سرّيتهم». لكن ذلك بدا تزييناً لمقايضة لا تخلو من التبيط في معالجة الأمور. فكأنما أراد الكاتب أن يحدّد الحل بالخيار بين اثنين: فأيهما تفضل قليلاً من نيران المدفعية المضادة للطائرات من المهووسين بالسرّية، أم سلاحاً قوياً بأيدي المختطفين والإرهابيين؟

كان ستيوارت بيكر الشخص المسؤول عن القضية في وكالة الأمن

القومي، وانتهى به الأمر إلى التنسيق، بين الجهود الكثيرة المبذولة لإقناع القيادة الصاعدة بإقرار مبدأ الوديعه. ففي الوقت الذي كانت فيه فورت ميد حافلة بالعابرة، لم تكن مليئة بالقدر نفسه بلأس يرتاحون بالتعامل مع العالم الخارجي. وكان بيكر قد قطع شوطاً كبيراً في الارتقاء في سلم المراتب، منذ أن زاره كلينت بروكس في مكتبه وأخبره أول مرة عن التوازن. وقد تكونت لديه منذ ذلك الوقت صورة جيدة للمشهد الكريبتوجرافي من وجهة نظر وكالة الأمن القومي، ورأى كيف تتصل الأمور ببعضها وتتناسق. إنك لا تستطيع فرض ما يستخدمه الناس داخل البلاد ولا يمكنك كذلك إبقاء كل نسخة من برنامج مثل منتهى السريّة PGP بعيداً عن متناول أي كائن في هذا العالم. لكن في الواقع، لن نجد الكثير من الناس يكلفون عناء البحث عن برمجيات تشفير غريبة مثل منتهى لسريّة واكتشاف طرق استخدامها كما نت القيود المفروضة على التصدير هي الطريقة التي توسّلت بها لإيقاف الشيفرة الجيدة - كل شيء من مستوى معيار تشفير لبيانات فما فوق - منعت من أن تكون من مكونات الأنظمة التي يستخدمها الناس كل يوم، وبالتالي، بعيداً عن متناول معظم الأشرار.

كان بيكر يرى في مشروع رقاقة المقرض وسيلة تغنيها لحكومة عن الاعتماد على القيود المفروضة على الصادرات لاحتواء الشيفرة. وكان ثمة إشارات بأن لكونغرس قد لا يستمر في دعم الأنظمة تلك إلى الأبد، وراحت تتعالى لأصوات بين أو ساط رجال الأعمال في معارضتهم لها. وكانت المشكلة، أن صناعة البرمجيات كانت قد نمت في بيئة، الأنظمة فيها قليلة، وأضحى الآن صناعة ضخمة تقدّر بعدة مليارات من الدولارات. وكان الرأي السائد أن طبيعة الأمور تفرض حسمها بالقتال في السوق فيما تبقى الحكومة كياناً ينأى بنفسه إلى حد ما عن التدخل. وبدا أن سريعو الغضب كانوا يعتبرون وكالة التشفير الأولى في العالم خرفة بعض شيء، ونتاج مصطنع للحرب الباردة، لا علاقة له بواقع الحال اليوم. كانت فلسفتهم هاكم، التكنولوجيا

تتحقق. ولقد شعر بيكر بالهلع ذات مرة حينما أخبره أحد المدراء المساعدين في مايكروسوفت بابتهاج أن بيل جيتس كان سيدخل الشيفرة في نظام تشغيل مايكروسوفت، وأنها ستكون موجودة في كافة تطبيقاته. ومن يهتم إذا كانت ستقوي الإرهابيين أو تشرّد الأمم؟ كان موقفهم: «إن التشفير ممتاز، لنضعه في أي مكان».

كان بيكر يعتقد في دخيلته، أن هؤلاء السريعو الغضب، ليسوا بعيدين عن الوطنية، وإنما يجهلون المخاطر الحقيقيّة في العالم. وكانوا يعدّون تصنيف الشيفرة بموازاة الأعتدة الحربية الثقيلة. لكن إن التنتصت على العالم بشبكة ولمعة تقدّر كلفتها بعدة مليارات من الدولارات من الأقمار الصناعية، وقواعد الرادار، وأجهزة التحسّس الأرضية السريّة، كان عماد السياسة الدفاعية للولايات المتّحدة. هل ثمة طريقة أخرى لتتبع البرنامج النووي لكوريا الشمالية أو استخدام العراق للأسلحة الكيميائية ضد الأكراد؟ إن الجمهور كان قد سمع تلميحات وحسب عن أهمية تلك «المعترضات»، مثل الإشارات المنتزعة من المكالمات الهاتفية، والتحويلات الرقمية، وحتى بثّ أجهزة التليفون المتنقل (الووكي توكي). وكان معظمها محظوراً، ويعتبر في غاية السريّة. لذلك لم يكن هناك صحفيون حينما تجرأ الرئيس بوش ذاته على زيارة فورت ميد (وكالة الأمن القومي) ليقدم تهانيه الشخصية إلى مفككي الشيفرة على ما قا موا به من أعمال أثناء حرب الخليج. لكن ما الذي فعله هؤلاء الأشباح على وجه التحديد؟ لو أن الجمهور يعلم . . .

اعتبر بيكر وزملاؤه المدافعين عن نظام الوديعة، أن من الضروري أن تكون النظرة التي أخذت بها الإدارة الجديدة عن العالم أكثر واقعية وقوّة. ولا ريب أن التشفير يجب أن يكون جزءاً هاماً من المجتمع المتشابك، لكنك تحتاج إلى ضوابط، تحتاج إلى حدود تحترم ولا يجوز خرقها، تحتاج إلى

طريقة لسمع الأشخاص الطيبون ما الذي يقوله الإرهابيون، والمحتالون لبعضهم البعض.

في وقت مبكر من الحملة للفوز بأفئدة وعقول جماعة كليتون، أطلع بيكر وسيثونس ليون فيورث، الذي أصبح مستشار آل جور لشؤون الأمن القومي، على الموضوع. ومع أن فيورث كان حذراً، فقد كان بالإمكان أن يرى مؤيدو الوديعة أن حجتهم أصابت هدفها. واعتقدوا أنه كان ظاهراً على وجهه: الإدراك بأن الحملة الانتخابية قد انتهت وأن جماعة كليتون سوف يكونون الآن في صراع مع بعض القضايا لعويصة جداً. وكانت هذه إحدى تلك القضايا العويصة التي بمقدور وكالة الأمن القومي، ومكتب التحقيقات الفيدرالي الفوز بها.

ومع تعاقب أيام شهر كانون الأول/ ديسمبر، تواصلت جلسات الإطلاع. وبعيد يوم التولية [حينما يتقلد الرئيس منصبه رسمياً في 20 كانون الثاني هـ. م] تعرّف آل جور بنفسه على عقيدة وكالة الأمن القومي من المدير مك كونييل وكلينت بروكس. وكانت ضربة موفقة للقلعة. وبسبب من ولع آل جور بالتكنولوجيا، كان يستطيع تقدير براعة مشروع وديعة المفتاح حق قدره. ولربما عمد محطّم آلات حديث من الجمهوريين إلى التشويش على تلك التفاصيل، لكن انفتاح جور تجاه الفكرة بدا مقيداً بإدراكه بأن أجهزة ورافعات البرمجيات قد تعمل فعلاً، وتوفّر حلاً يمنح لكل واحد شيئاً ما.

ما أن تبدّل حال فريق كلينتون - جور من الانتقال إلى الحكم، حتى ضاعف جماعة رقاقة المقرض من اجتماعاتهم. وكانت المذكرات تطاير ما بين وكالة الأمن القومي والمؤسسة القومية للمعايير والتكنولوجيا المناقشة أفضل السبل للتنبؤ بالاعتراضات المحتملة والاستجابة لها. وكانوا يعون وجود مشكلة محتملة واحدة، هي إصرار فورت ميد على إبقاء العمل في رقاقة المقرض سراً عن الجمهور. ولقد حاول بروكس إقناع زملائه بكشفها للجمهور، لكنّه أخفق في مسعاه. كانت خطته الاحتياطية الحصول بطريقة ما، على ضمانات بأن

وكالة الأمن القومي، لم تضعف الوثاب قصداً خدمة لأغراضها الخاصة. وكتب بسرعة مذكرة وجَّهها إلى مديره في 5 كانون الثاني/ يناير: «إعمل على عقد ندوة من الأكاديميين، من أوساط محللي الشيفرة المختصين بالرياضيات، لدراسة مستوى الوثاب المحظور، للتأكد من أنه خوارزمية جيدة. فمن هم يا ترى؟»

في غضون ذلك، كان تأثير هذا الوايل من الجلسات اليومية على البيت الأبيض، يزداد باطراد. وفي الأسابيع الأولى من الحكم، لم يكن كليتون وجور قلاً علنا انتهاء العمل بالمقراض. بيد أن أعوانهما كانوا قد اقتربوا من الاستنتاج أنه ليس ثمة بديل آخر عن هذه الأداة.

كان جون بوديستا في ذلك، الحين أحد أعضاء الإدارة. ولعل لحظته حانت في وقت مبكر جداً، بعيد بداية العهد الجديد حين جاء لزيارته بعض جماعات لضغط المدافعة عن تكنولوجيا المتقدمة. في ذلك الوقت، كان مؤيدو مبادئ الحرية المدنية وجماعة صناعة البرمجيات ما زالوا يأملون بأن تقوم الإدارة الجديدة بعمل مناهض للأشباح ورجال الشرطة وتحزّر أنظمة تصدير الشيفرة. (ولو أنهم كانوا يعملون بأمر رقاقة المقراض لانفجروا). أما بوديستا، فكان لا يزال منبهراً بالألعاب الجديدة في كتبه، عرض لهم جهاز هاتف STU-III الخاص به، وهو جهاز هاتف الشيفرة المعياري، الذي كانت الحكومة قد استخدمته منذ حوالي خمسة أعوام. فسخروا منه وقالوا: «حل حكومي نموذجي مجلجل كما هو عهدنا بها، ولكن هل تعلم ما هو الممتاز؟ إن إيه تي أند تي سوف تصنع جهازاً حجمه نصف حجم هذا الجهاز، وأرخص منه بكثير، وسيقوم بكل ما يقوم به هذا، إنما بصورة أفضل. إننا ننصحك بشراء هذه الأجهزة!» ومع أن جماعة التكنولوجيا المتقدمة لا يعلمون شيئاً، فإن تعليقاتهم كانت في الحقيقة ترجيح صدى للمذكرات التي كان يتلقاها بوديستا. وما لم تفعل الحكومة شيئاً، فعلى الأرجح أن الأجهزة اللعينة تلك سوف تكتسح السوق.

وليس مؤدى ذلك، عصابة مؤامرة المقرض في وكالة الأمن القومي، ومكتب التحقيقات الفيدرالي كانت تعول على ضربة خط لإعادة جماعة كليتون إلى جادة الصواب. فقد كانوا يرتبون أوراق اللعب بشكل أساسي، ويعرضون مجموعة محدودة من الخيارات للأغرار. لا تريد أن تفعل شيئاً، وتدع السوق تأخذ مجراها الطبيعي؟ رائع. إذا ما كنت تريد أن تطلق فوضى التشفير، من عقالها فهاكم هي. وحذروهم، لا تفعلوا شيئاً، يعني أن إيه تي أنتي سوف تبدأ ببيع أجهزة الهاتف وتعلمون بأن التكاليف سوف تنخفض وستجدون الناس يتحدثون على هواتف مأمونة ويتراسلون ببيمجيات مشفرة. وكان الدخان المنصاعد من تفجير مركز التجارة العالمية بالكاد قد تبدد. وماذا لو أن كارثة إرهابية أخرى وربما أسوأ منها، وقعت، وتبين أن الحكومة قد أخفقت في الحيلولة دون وقوعها لأن مرتكبيها كانوا قادرين على لا تُصال فيما بينهم بشيفرة غير قابلة للتفكيك؟ أتود أن تمنح صدام حسين القدرة على استعمال شيفرة ليس باستطاعتنا تفكيكها؟ هيا، ثابروا على ما أنتم عليه، ولا تفعلوا شيئاً. وسوف تتحملون وزر الدماء التي ستسفك. وقد أفرغ هذا الطرح جماعة كليتون.

أما البديل الآخر، والذي كان بعض المتشددين في مسألة حفظ النظام يطالبون به بالحاح، فقد كان أكثر تطرفاً: حظر الشيفرة داخل الولايات المتحدة. وفي إحدى المحاضرات التي قدمها مكتب التحقيقات الفيدرالي والتي رافقها عرض شرائح منزلة (سلايد) وجداول بيانية ومؤشر ليرسم خطأ يبرز النقاط الهامة، دمج رجال الحكومة أهدافهم المتصلة بالمقرض مع رؤيتهم للإرسال الهاتفي الرقمي. كان العرض يقول بشكل أساسي: إن عدم ضبط الاستخدام المحلي للشيفرة أدى إلى ظهور الحاجة إلى وضع سياسة قومية شاملة على مستوى البلاد تجيز للمستخدمين «الشرعيين» استخدام الشيفرة لإحباط جهود خصومهم، وكذلك «تكفل للأجهزة والأنظمة الكريبتوجرافية

القدرة على التشفير، في الوقت المناسب لتطبيق القانون». إن المعنى المتضمن والذي لا يمكن تفادي استخلاصه هو: يجب حظر أي كريبتوجرافيا غير مطابقة للمعايير، بما في ذلك الأجهزة والأشياء التي يوزعها المصنعون الأمريكيون على المستخدمين الأمريكيين. وإلا نشأ «ملاذ إلكتروني» لا يحتمل. فلتنسوا استولجية استخدام القيود المفروضة على الصادرات لتخفيف ما يستخدمه الناس داخل البلاد... لقد كانت أمتنا معرضة للخطر بسبب من أن أدوات كهذه، كانت متاحة قانونياً لمن يشاء، إذا كان لديه حافز للبحث عنها. ومن غير القانوني السماح بوقوع الأسلحة النووية بيد كل من هب ودب، كذلك يجب ألا يكون قانونياً وقوع الشيفرة، في أيدي أولئك الذين سيدمرون المجتمع بها. ونجد في هذا الرأي ترجيحاً، بطريقة عجيبة غريبة، لصدى قول فيل زيمرمان: «حينما تكون الشيفرة محظورة، فإن الخارجين على القانون وحدهم سوف يمتلكونها».

ولقد تدبر جماعة كلينتون مقاومة ذلك المطلب، الذي كان سيثير شغباً في سيليكون فالي، ولعله ما كان ليفلت من مقاضاته أمام المحاكم. وكان فريق جور على وجه الخصوص ذا حساسية إزاء الفكرة القائلة بأن طريقة المعلومات السريعة الآخذة بالنشوء كانت بحاجة إلى حماية لسرية مراسلاتها. ثم كيف لك أن تفرض حظراً كهذا؟ ماذا يريد هؤلاء من الحكومة أن تفعل، أتراهم يريدون منها الانتقال من بيت إلى بيت والتفتيش في الأقراص الصلبة للناس، بحثاً عن نسخ من برنامج بي جي بي؟

وبعد أن قُدم لجماعة كلينتون بديلين مقيتين، طرح عليهم طريقة ثالثة، بدت على النقيض من غيرها، تسوية يمكن للجميع التعايش معها. وفي استعادة للأحداث الماضية والتأمل فيها، راح أحد المطلعين في الإدارة ينظر إليها على أنها مماثلة للخيارات التي قُدمتها جماعة كينيدي بشأن غزو كوبا - وهي إما تفادي المشكلة وهذا ينم عن الجبن، وإما عملية عسكرية واسعة النطاق تشيع

الاضطراب وعدم الاستقرار، أو الخطة الأخرى، وهي عملية صغيرة في مكان ما يدعى خليج الخنازير.

تم عرض هذا المشروع على جماعة كلينتون على أنه مشروع جاهز للتنفيذ والدخول في العملية حالما يعطي الرئيس الأمر. حتى التراخي المؤقت كان يعني عند القوم فقدان احترام قاعد أنصار القانون والنظام الذين تحتاج إليهم الإدارة. كان أحد رجال مكتب التحقيقات الفيدرالي الذي يتولى اطلاع جماعة كلينتون على مجريات الأمور، رجلاً ضخماً أنيقاً هو المدير المساعد جيمس كالستروم. وقد سعد نجمه يوم كان رئيس فريق التكنولوجيا في المكتب، لنجاحه في عملية التنصت التي أوقعت جون جوتي. ووصفه بعض الناس بأنه نسخة مكتب التحقيقات الفيدرالي من كيو Q، الساحر الذي عرفناه يأتي بلا ابتكارات والاختراعات الخارقة في أفلام جيمس بوند. وكان أسلوبه في العرض الحديث المباشر والنظر في عيني مستمعيه، وتوجيه انتقاداته بشكل شخصي. فيسألك هل أنت متزوج؟ هل لديك طفل؟ ثم يندفع بجرأة إلى عرض سيناريو يصور فيه قيام أحدهم باختطاف أحد أولادك، واحتجازه في قلعة في منطقة البرونكس. وتذهب الظنون بالمكتب أن ولدك محتجز هناك؛ فيحصلون على مذكر قفتيش للعثور عليه. لكن الأوغاد قد شيدوا القلعة من معدن جديد ليمنعوا اختراقها. لذلك يقف الرجال المكلفين بإنقاذ ولدك عاجزين، عن دخول القلعة المنيعة. ويا له من كابوس رهيب: المختطفون، ومعهم رهيتهم الثمينة، يراقبونك ورجال الحكومة وأنتم تحاولون الدخول ويضحكون عليكم.

سوف يقول كالستروم بلهجته النيويوركية: «إن هذا هو الأساس الذي تقوم عليه المسألة. ومن وجهة نظر حفظ النظام هناك تهديد خطير - هذا لشخص سوف يقوم الآن ببناء هذه المنطقة المحصنة في برونكس، لأن لديه باباً فولاذياً ضخماً، ولا شيء لدينا من أدوات اللحم، والبومرنج boomerange [سلاح أسترالي يصيب هدفه ثم يرتد عائداً إلى صاحبه هـ. م] يفتح لنا الطريق

إلى داخل ذلك المكان. إننا بالتأكيد، نريد أن نمتلك تلك الأبواب الفولاذية الجديدة، لحماية مصارفنا، وأسرار التجارة الأمريكية، وحقوق الملكية، والتكنولوجيا. ولكن هل نرغب في طريقة رقمية فائقة السرعة، حيث يستطيع لمجرمون الكبار العمل، دون أن يتأثروا بالأوامر القضائية، أو يتضايقوا منها؟ إذا كنا لا نرغب في ذلك، عندئذ يجب علينا أن نتطلع إلى «المقراض».

أضحى كالستروم ومعه كل من بيكر، وبروكس، ومك كونيل، وجون دويتش رجل وكالة المخابرات المركزية (سي أي إيه)، جزءاً من فريق وديعة المفتاح يعرضون ظاهرياً للإدارة ما لديها من بدائل، لكنهم كانوا يجهونها حقاً، بيد واحدة على مؤخرة عنقها الديمقراطية، نحو القبول المحتوم بالمقراض. كان ثمة حليف أنت به الرياح على نحو غير متوقَّع هو رون براون وزير التجارة؛ ففي أول عرض حضره، ذكر براون أنه أمضى خدمته الإلزامية في دائرة التنصت بوكالة الأمن القومي، وكان مدركاً تماماً ما تتمتع به استخبارات الإشارة من أهمية حيوية. وفي هذه المرحلة أصبحت جلسات الاطلاع لا تقتصر على جماعة الأمن القومي بل اتسعت لتشتمل المستشارين العلميين لدى كليتون وجور مثل ميك نيلسون الذي يعمل في مكتب السياسة العلمية والتكنولوجيا، مهووسون بالمعلوماتية، متفهمون منسجمون مع قضايا مثل الحرية الشخصية وحاجة لصناعة إلى أنظمة مأمونة. (حصل نيلسون على تصريحه الرسمي لسري للغاية بسرعة البرق في غضون ثلاثة أسابيع). وفي عرض لمكتب التحقيقات الفيدرالي في 26 كانون الثاني/يناير، فسَّر كالستروم الكثير من النقاط الدقيقة في المشروع، لكن المدير المسؤول عن برامج الاستخبارات لدى جور، جورج تنيث طرح المزيد من الأسئلة حول منهج المقراض، مثل من سيكونون الوكلاء لوديعة المفتاح؟ كيف ستتم معالجة الجوانب الدولية؟ وتضمنت مذكرة مهبطة وضعها سيثون في 9 شباط/فبراير ملخصاً مفصلاً للخطة، والآثار الخطيرة التي ستنتج، إن لم يتم الشروع في عمل ما.

وهكذا، لم يكن قد مضى شهر على تولي إدارة كلينتون، حتى اشتد الضغط للإسراع في تنفيذ المقرض. وكان مفترضاً، أن تشحن إليه تي أند تي عشرة آلاف جهاز هاتف، مزودة بمعيار تشفير البيانات، بحلول الأول من نيسان/ أبريل ما لم يمنع ذلك إجراء ما. لكن بحلول ذلك الوقت، كان فريق الشيفرة لدى الإدارة للمؤلف من أعضاء مجلس الأمن القومي، وخبراء في الإنترنت - قد انتقلوا تدريجياً من صنع القرار إلى تنفيذه. كانت تلك المبادرة الكبيرة الأولى لهم، وكانوا يرغبون بالقيام بها سريعاً: وظلت الكلمة «إنهاء» تبرز في مراسلاتهم. في مذكرة داخلية من النوع المعهود، مؤرخة في 5 آذار/ مارس، وجهها جورج تينيت إلى ليون فيورث، مستشار جور لشؤون الأمن القومي وزميله ويليام وايز: تصدرت الرأسيّة عبارة «النجدة، النجدة، النجدة». ثم «إن الحاجة ماسة لأن يمنحنا نائب الرئيس بعضاً من وقت، لعقد اجتماع مع مدراء وكالة الأمن القومي السابقين والحاليين. حول مسألة التشفير. «أظن أنني أعلم ما يرغب نائب الرئيس في سماعه من حديث مك كونيرو ستوديمان»، وأنهى تينيت مذكرته بخاتمة غريبة: «رعاكم الله جميعاً!».

تواصلت الاجتماعات طوال شهر آذار/ مارس، وفي غضون ذلك، كانت جماعات لصناعة والحريات المدنية تمارس ضغوطاً على القادمين الجدد، وهم ما يزالون يأملون من الإدارة الجديدة القبول بإجراء إصلاح كبير في موضوع الشيفرة. وصرخ أحدهم بجماعة جور قائلاً: «إنكم تعرقلون التجارة الإلكترونية، إنكم تعرّضون أمن الشبكات للخطر، وإلى جانب ذلك، فإنها خرجت جميعها عن نطاق السيطرة». ولكن جماعة كلينتون كانوا لتوهم قد انحازوا ذهنياً إلى المطلعين على مواطن الأمور في الحكومة داخل وكالة الأمن القومي، ومكتب التحقيقات الفيدرالي، ووزارة العدل، ووكالة المخابرات المركزية. ولقد أدت جلسات الاطلاع السريّة الغرض المطلوب، وعلى وجه الخصوص لتحذير، بأنّه ما لم يتخذ أي إجراء فإن «الناس سوف يقتلون، ولقد

سُئلوا: هل أنتم على استعداد للتضحية بحياة البشر، من أجل زيادة جزء من فاصلة عشرية في مجمل الناتج القومي؟» وكانت الخطة مؤثرة على نحو مدمر: فقد حُلَّت المعضلة بشكل جوهري بوصفها خياراً بين مقتل آلاف من الناس وزيادة ثروة بيل جيتس بنسبة عشرة بالمئة. ويقول مسؤول في الإدارة: «كان هذا قراراً سهلاً إلى حد بعيد».

ومؤدى ذلك أنه لم يكن ثمة ارتياب داخل البيت الأبيض. فقد كان السؤال الكبير الذي طرحه مساعدو كليتون على أنفسهم: «لماذا يرغب أي شخص بالمقراض؟» (ففي النهاية، «كان» يفترض بالخطة أن تكون طوعية). وكان ثمة مشكلة أخرى، بعد، وهي المطلب بأن تكون خوارزمية الثواب محجوبة. وكان من المحتم أن سريتها سوف تقود النقاد إلى القول بأن المشروع كان بمثابة حصان طروادة لإدخال شيفرة فيها عيوب إلى البنية التحتية. لكن وكالة الأمن القومي ما كانت لتترجح عن موقفها من السريّة.

أخيراً كانتمة مشكلة، كيف سيعمل مشروع وديعة المفتاح فيما وراء البحار؟ فإذا لم يكن الحل التشفيري عالمياً، فإنه سيكون عديم الفائدة. وإذا لم تحظ منتجات الولايات المتحدة مع خطة الوديعة بثقة المشتريين في الخارج، فإنهم سوف يعرضون عنها ويلتفتون لشراء احتياجاتهم من المصنعين في سويسرا أو ألمانيا أو حتى روسيا. ثم كيف بمقدورك أن تعالج وديعة المفتاح في البلدان الأخرى؟ هل يجب على الولايات المتحدة أن تسمح لدول تفتقر لحرية التعبير عن الرأي مثل سنغافورة والصين بالوصول إلى المفاتيح المخزّنة؟ وهل ستكون نسا ومصر واليابان ودول أخرى سعيدة بما سمح لمواطنيها باستخدام منتجات تتيح لأشباح في الولايات المتحدة حل شيفرا لمكالمات، بينما لا تستطيع ذلك وكالات الاستخبارات وأجهزة حفظ النظم في تلك البلدان؟ إن هذه الأسئلة لم تكن لتجد لها إجابة بسبب من أن المخططين للمقراض لم يوجدوا أبداً حلاً لآثاره العالمية - وتلك نتيجة أخرى تأت مع الإسراع بطرح لمقراض.

إن هذه الاعتراضات كلها لم تكن كافية لإغراق الخطة . ففي السادسة من مساء 31 آذار/ مارس 1993 ، وفي غرفة إدارة الأزمات بالبيت الأبيض ، قام نائب الرئيس جور بمراجعة للتوجهات المقترحة في اجتماع ضم المجموعة بأكملها من قادة أجهزة حفظ النّظام والاستخبارات و الأمن القومي . وبعيد ذلك ، عرض للرئيس توصيته . فوافق بيل كليتون .

وجاء الأمر بتنفيذ المقرض .

منذ تلك اللحظة ، تحوّلت العمليّة إلى ما أطلق عليه أحد المساهمين فيها اسم «تسويق على طريقة البيت الأبيض» . ووضعت مسودات البيانات الصحفية . وأخذ مايك نيلسون بكتابة توضيح للاقتراح بشكل سؤال وجواب . ومن ثم عشية الإعلان ذاته ، أطلع البيت الأبيض مسبقاً عدداً من ممثلي الكونغرس والصناعة ، وجماعات الحريات المدنية على الموضوع ، ولم يكن ذلك بقصد الحصول على تغذية راجعة ، بقدر ما كان لمنع توجيه التهم التي كان جماعة كليتون قد تعاملوا عنها مع التحوّل المفاجئ في مجرى المشروع .

ومع ذلك ، لم يتوقع أحد في البيت الأبيض ، قيام ضجة حول المقرض . لكن كلينت بروكس رأى مشكلة قادمة ، كانت هذه المسألة عرضة لاحتمال أن تتسرّب إلى خارج وكالة الأمن القومي ، لتجعل من المتعاطفين المحتملين أعداء حقيقيين . وذات مرة ، أثناء تنقله بالسيارة مع ستوببكر بين فورت ميد والبيت الأبيض قال له متذمراً : «إنهم قاصرون عن إدراك المسألة» . وفي أحد الاجتماعات ، تساءل : «من الذي سيعالج هذا الموضوع في برنامج لاري كينج الذي يبثّ على الهواء مباشرة؟» ولقد تجاهل الحضور هذا السؤال . فكّرر من جديد بعد بضع دقائق . فأخبره مسؤول كبير في الإدارة بصراحة : «يا كلينت ، إننا نقدر موهبة الدعاية عندك . لكن هذا أمر جدي فعلاً . عليك بمعالجة الجانب التقني من الموضوع ، ونحن سنعالج الجانب السياسي» . (بعد بضعة أشهر عمد ما ظهر آل جور في برنامج لاري كينج ، ليتحدّث عن طريق المعلومات

السريعة، كان أول سؤال وجه إليه يتمحور حول... رقاقة المقراض).

مضت جلسات الإطلاع مع الكونغرس، وأرياب الصناعة على نحو كان متوقفاً تقريباً: فقد استقبل الاقتراح بحذر بل حتى بالشك لكن دون أن يصرف النظر عنه. وتدمر أحد المستشارين في الكونغرس بأنه عندما جرى تحدي جماعة كليتون ردوا بموقف هجومي. فقد تساءلوا: «هل ترغبون في أن تكونوا مسؤولين عن الخاطفين؟» فتهاوى المشرعون. ولم تكن الجلسات التي عُقدت مع جماعة الحريات المدنية بعيدة كل البعد عن الود والمجاملة. ولقد حضر جون بيرري بارلو من مؤسمة الآفاق الإلكترونية إحدى الجلسات الاطلاعية المفاجئة ولم يستطع أن يصدق ما يسمع. إذ شعر بأن أصدقاءه الجدد في البيت الأبيض كانوا يشربون ما تقدمه لهم وكالة الأمن القومي. وما أزعجه بشكل خاص ذكر مايك نيلسون للمعلومات السريّة التي بلغت ولم تكن قد بلغت بارلو. قال نيلسون: «لو كان بإمكانني أن أخبرك بما أعلم، لشاطرتني الشعور ذاته» وأسّر إليه بأن الآلاف يمكن أن يلقوا حتفهم. ف شعر بارلو أنه كان يسمع الموسيقى الزائفة ذاتها التي كان يعزفها مثيرو الحرب الفييتنامية. وأن ما يعنيه المقراض حقاً، كان خطة سوف «تبدأ عملية قد تشكل نهاية الحرية في أمريكا».

وقام كلينت بروكس، ببذل جهود كبيرة، ليفهم الخبراء في الخارج المعلومات الضرورية لشرحوا للجمهور الطبيعة غير الخطرة للنظام. وفي الليلة التي سبقت الإعلان، قام بروكس بالمجازفة بقيادة سيارته تحت وابل من المطر ليطلع دوروثي دينينج، ساذة علم الكمبيوتر في جامعة جورجيتاون، ويعرض عليها خياره الأول لعقد ندوة لدراسة خوارزمية الوثاب السريّة. وكان ذلك خياراً ملهماً. ذلك أن دينينج كانت خبيرة في الشيفرة وأمن الكمبيوتر لكن سلوكها كان من الرقة مثلما كانت عليه بيتي كروكر. (وصف كاتب الخيال العلمي بروس ستيرلينج ذات مرة المرأة الدقيقة الحجم هذه بأنها «أشبه براهبة حاجة خلف زجاج من الرصاص») وكانت في ذلك الحين معروفة بدعمها لضبط

الكريبتوجرافيا، وبمحض الصدفة، وبالتزامن مع زيارة بروكس، كانت لتوها قد خبرت وضعا مزعجاً عجزت فيه عن فتح خزانتها بعد سباحتها في مجبج الجامعة المغلق؛ ولم ينقذها سوى رجال الصيانة، ذوو الخبرة والقدرة ومعهم القاطعات المتينة (المرادف لعملاء الوديعة!) من خطر التعرض لطقس [بارد] تبلغ درجة حرارته أربعين درجة [فهنها يت] في ملابس سباحة مبللة. ولذلك فإنها لم تكن على استعداد للدفاع عن وديعة المفتاح فحسب، بل إنها أصبحت تشعر بأنه كان قدرها.

في 16 نيسان/ أبريل، كشف لرئيس كلينتون النقاب عن المبادرة الجديدة. وفي إعلان سكرتيره الصحفي عن الخطة، عرضت القضية للجمهور على أنها حل وسط بين أمرين أحلاهما مر، مثلما عرض الوضع للإدارة من وجهة نظر وكالة الأمن القومي إلى حد بعيد. وبالنظر إلى الوضع عبر تلك المصفاة، تم اعتبار رقاقة المقرض هبة من الله:

إن الرقاقة خطوة هامة في مواجهة مشكلة سيف التشفير ذي الحدين: فالتشفير يفيد في الحفاظ على سرية الأفراد ولصناعة، لكنه بإمكانه أيضاً حجب المجرمين والإرهابيين عن الأنظار. إننا بحاجة إلى «رقاقة المقرض» وطرق أخرى تتيح للمواطنين الملتزمين بالقانون بلوغ ما يحتاجون إليه من التشفير وتحول دون استخدام المجرمين له، لإخفاء أنشطتهم غير القانونية سواء بسواء.

إن الإعلان الفعلي عن المقرض لم يجعل منه معياراً، لكنه أكد التزام الحكومة بشراء الآلاف من أجهزة شركة إيه تي أند تي التي وضعت رقاقة المقرض داخلها لتزود بها دوائرها. وكان الأمل أن يؤدي تبني الحكومة للمقرض وتزكيته أن يحدث تحولاً في السوق مما يجعل المقرض يبيع ويتشر، وإن ظل اختياره معياراً طوعياً. أما التوصية النهائية فستأتي بعد تلقي كلينتون نتائج مراجعة واسعة النطاق على مستوى رفيع لسياسة التشفير التي

ستعتمدها الولايات المتحدة، بعد تفحص مبادرة الوديعة بعناية وتقوم قوانين التصدير.

وبذلك الإعلان، شعر بيل كلينتون وجماعته بأنهم قد قاموا بخطوة كبيرة نحو تفادي ما بدا وكأنه تصادم ينذر بكارثة في عالم الشيفرة، تصادم بدا مقدراً سلفاً منذ اليوم الذي اكتشف فيه هويت ديڤي طريقة تقسيم مفتاح الشيفرة. والواقع أن رقاقة المقراض اعتبرت بحق نقطة التحول في المعركة، لكن ليس بالطريقة التي كانت تريدها إدارة كلينتون على الإطلاق. فبا لترويج للمقراض باعتباره سفينة القيادة لمفتاح الوديعة، ارتكبت الحكومة خطأ فادحاً. فعوضاً عن التدرج في مناقشة موضوع التشفير أصبحت فضائل هذا المشروع - ومثاله - هي ساحة القتال الرئيسة في معركة حامية الوطيس حول التشفير. كان المقراض ذاته هو القضية، وكان المقراض كما تم اقتراحه عرضة للانتقاد. وقد رأى مهندسه كلينت بروكس، أكثر من أي شخص آخر، ما كان يجري، لكنه كان عاجزاً عن منعه.

في البداية، لم تبدو الأمور سيئة إلى حد كبير. ومن الموقع الممتاز للبيت الأبيض وفورت ميد، بدا أن أي اهتمام شعبي ضئيل نسبياً حظيت به رقاقة المقراض، كان متوازناً بكل معنى الكلمة. وقد حُدثت مقالة النيويورك تايمز، المنشورة يوم الإعلان بلهجة معقولة في تناول الموضوع من مقدمتها، إذ قالت أن إدارة كلينتون «على وشك إعلان خطة لصون السريّة في وسائل الاتصال الإلكترونيّة... فيما تتضمن كذلك حق الحكومة بالتنصّت لأسباب تتعلق بحفظ النظام و الأمن القومي». التوازن. وبالطبع، فإن المقالة أوردت قولاً لأحد ممثلي الوسط لصناعي: «إننا لحكومة في سبيلها لأن تُخلق وحشاً».

وفي الأيام التالية، لم يكن ثمة أي استعجال لقبول الخطة، من مختلف أصحاب المصالح الذين قد يتأثرون بها. وارتاح الفيدراليون، مع ذلك، لأنهم

تفادوا بهذا القرار، نشوب حركة تنديد عنيفة. وأخذت الإنترنت، تضج بمخاوف من تفشي إجراءات الدولة البوليسية ولكن من الناحية الأخرى، أعلنت دوروثي دينينج على الفور وصفاً صادراً عن فكر صاف للنظام ذاته مما اعتُبر في ذلك الحين مثلاً على أن مجتمع الشيفرة لم يكن مناهضاً للمقرض على وجه الإطلاق. والأفضل من ذلك، أن مارتي هيلمان طلع بوصف مؤيد للخطة لم يكن متوقفاً أن يصدر عنه، وكان بروكس قد عرض له الموضوع على الهاتف عشية الإعلان. كان تفسير هيلمان للمشروع حياً وحادراً (مع أنه نَبه حقاً إلى ضرورة أن يرافق هذا ضوابط للعملية القانونية تؤدي إلى استرداد المفتاح)، وقامت الشبكة ذات النفوذ التي يديرها ديفيد فاريير بإدراج اسمه ضمن قائمة «الشخصيات المشيرة للاهتمام»، ليكون في عداد من يتلقون رسائلها البريدية.

في 20 نيسان/ أبريل وضع كلينت بروكس، مذكرة تعكس تفاؤله كتب فيها: «إن ردود الفعل التي تردني من الأكاديميين والصناعيين تفيد بأنها قد تصادف النجاح». كذلك كان هؤلاء الأشخاص يقولون له بأن الحكومة ربما لم تعين عدداً كافياً من الأرقام في حقول تعريف الرقاقة لتعالج جميع رقاقات المقرض التي ستدخل في الاستعمال. إن مئة مليون لن تكون كافية!

لكن ذلك النجاح الأولي كان وهماً، وأشبه بفريق بيسبول من الدرجة الثانية احتل المرتبة الأولى بعد أن صادف سلسلة من الانتصارات في شهر نيسان/ أبريل. وقد جاءت أولى الأصوات المتذمرة الجدية من صناعات المعلومات الدقيقة. وبعد القيام بمراجعة الخطة، خلصوا إلى أن الفرصة التي أتاحتها لبناء شيفرة منيعة قابلة للتصدير في أنظمتهم قد نال منها كثيراً وجود مجال مدخل حفظ النظام LEAF، الذي زود متطفي الحكومة الذين لديهم الترخيص بالمفاتيح. وكانت الغاية من تصدير الشيفرة، بعد كل شيء، خدمة الزبائن فيما وراء البحار. لكن ما هي الشركات الأجنبية التي ترغب في شراء

نظام أمني، مفاتيحه مودعة في خزائن حكومة الولايات المتحدة؟ وانضم كبار رجال الأعمال، إلى جماعة الحريات لمدينة المرتابين أصلاً، والذين ردتهم مجموعة الإنترنت الأساسية بالطاقة. ثم أخذوا جميعاً قضيتهم إلى وسائل الإعلام. ومع أن بناء رد الفعل قد استغرق بضعة أشهر، فإن التغطية التي نالها المقراض في وسائل الإعلام، تجاوزت كل دعاية جماهيرية نالها سابقاً أي تطور في علم الشيفرة.

كان بعض هذه التغطية إيجابياً. وكان مبتكرو الوديعة يعتقدون ضمناً، طوال الوقت الذي كنا نت فيه الحكومة تخطط لمبادرة الوديعة، بأن قلة ضئيلة منعزلة فقط هي التي متشكك في دوافعهم. ونظروا إلى الترويج للمقراض على أنه عملية ستحمل إلى العقلاء قدراً من الهموم، وأن الحكومة سوف تستجيب لها، ومن الهموم الرئيسة كما حسبوا، الخطر بأن الجانب التقني من مشروع الوديعة، سوف يعرض أمن التشفير ذاته للخطر، مما يبسر على المحتالين والجواسيس من دول أخرى أمر فك الشيفرة، وهناك، بعد، هم آخر هو احتمال أن تكون تسهيلات مفتاح الوديعة ذاتها ضعيفة، والذي لم يأخذه هذا التفكير بعين الاعتبار هو الأساس الذي بني عليه هذا المشروع من حيث أنه وسيلة الحكومة لتقر مفتاح «فك التشفير» لأغراضها الخاصة، وقد وجدته معظم لنا س كريهاً مقرفاً. كل ما كان على الخصوم القيام به هو إجراء عملية مقارنة بسيطة، ماذا لو أنك كنت مضطراً لأن تترك نسخة مفتاح باب بيتك في مخفر الشرطة؟ فحتى الساذج من الناس الذي لا يعرف الفرق بين التشفير وتمرير الكرة سوف يتحول إلى مناهض للمقراض. وقد بين جيرري بيرمان من مؤسسة الآفاق الإلكترونية بأن «الفكرة القائلة بأن الحكومة تمتلك المفاتيح لجميع الأقفال، حتى قبل أن يتهم أحد بارتكاب جريمة، قول لا يفهمه الجمهور، إن هذه ليست أمريكا».

ولم يكن الآخرون بحاجة إلى عقد مقارنة كهذه. ذلك أن أحد الأسباب

الرئيسة وراء رغبة الكثير من لناس في استخدام الشيفرة، إبقاء المعلومات بعيداً عن متناول الحكومة ذاتها. وليس لكونهم قد انتهكوا القانون بالضرورة، بل إن الأمر بكل بساطة أنهم لا يمحضون الحكومة ثقتهم. فالبيروقراطيون الذين أعدوا الخطة كان يفصلهم جيل عن ووترجيت، ولكن أي شخص كان موجوداً في السبعينات، ربما كان يعرف الوضع بصورة أفضل.

كان مدير وكالة الأمن القومي السابق بوبي إنمان، مثلاً، قد اطلع في وقت مبكر على رقاقة لمقراض وأدرك على الفور ألا أمل لها بالنجاح. فمن تراه الذي أراد أن يعطي الحكومة سبيلاً مباشراً لا ستقاء أخبارك؟ وقد فهم زعران الشيفرة ذلك، وبدأوا على الفور بشن حرب غير تقليدية تستهدف وسائل الإعلام والسكان عموماً لحملهم على منا صرتهم في حربهم هذه ضد رقاقة المقراض. وفي الاجتماع الشهري، ألخ إريك هيويز على أن يتضمن جدول الأعمال كل الأعمال المحتملة بدءاً من توزيع مواد إعلامية لكسب تأييد جماعات الصحفيين إلى الدعوة إلى إجراء تعديل في لدا ستور ينحو إلى تأييد الشيفرة. واقترح تيم ماي القيام بعمل تخريبي فعال للمقراض، أو مقاطعة شركة إيه تي أند تي. وقد أنجزوا حقاً مزحة مؤثرة، بتوزيع أشكال صغيرة لتلصق على الملابس. وقد صممت بحيث تشابه البرمجية الشهيرة إنتل في الداخل، لموضوعة بلغة لوجو، وتقرأ عليه عبارة «الأخ الكبير في الداخل». وهذه العبارة أجملت كل ما يمكن أن يقال تقريباً. (هددت إنتل سريعاً بمقاضاتهم لانتهاكم علامتها التجارية، فأوقف زعران الشيفرة توزيع اللصاقات).

جاءت المعارضة من كافة الجهات. ووجد مناھضو المقراض أنفسهم يتفقون مع راش ليمبو الذي هاجم المقراض في برنامج الإذاعي. كذلك أعجب هيبو الديجيتال بالعمود الذي كتب ليام سافاير بعنوان «أغرقوا رقاقة المقراض» حيث أشار إلى أن اسم الحل المقراض Clipper قد تم اختياره بعناية، إذ أنه يقص Clips أجنحة الحرية الفردية.

كثيراً ما كان تيم ماي يعرض لنظرية تقول، أن للأمريكيين عقليين عندما يتعلّق الأمر بالسريّة. أحدهما يؤثر المصلحة العامة، وهو مناهض للشيفرة في الجوهر: «ماذا لديك لتخفيه؟» أما الآخر فيعبر عن الأخلاق الفردية كما يجسدها ميثاق الحقوق، وهو مؤيد للسريّة: «لا شأن لكم بما يخص سواكم». ولا بد لأي سياسة ناجحة من السير في طريق وسط بين هذين الاتجاهين المتعارضين. لكن المقرّاض، بإصراره على ألا يخفي شيئاً عن الحكومة، لم يحقّق التوازن لمنشود. وما أن بدأ الناس يطلقون عليها اسم رقاقة الأخ الكبير، حتى انتهت اللعبة.

بذلت الحكومة قصارى جهدها للدفاع عن المشروع. وقام ستيفورات بيكر بعرض الأمر لرجال الأعمال لصناعة، بما في ذلك مؤيد الشيفرة بيل جيتس، ولكن دون جدوى. كذلك دخل إلى عرين الأسد، متحدثاً في مناسبات أقيمت تأييداً للشيفرة مثل مؤتمر «الكومبيوتر والحرية والسريّة» حيث قلّل من شأن القوى المناهضة للمقرّاض في وجوههم، معتبراً ما يقومون به: «انتقام أناس لم يستطيعوا حضور احتفالات وود ستوك لانشغالهم بواجبات مدرسيّة ثقيل كاهلهم». وعمد إلى توبيخهم والسخرية منهم، بقوله: «لو أنكم تعلمون ما أعلم». وجادلهم إن نظرتكم إلى السريّة تعكس رؤية للعالم ساذجة وميؤس منها. ومضى بيكر محذراً: «إننا بإصرارنا على حق المطالبة بسريّة تتجاوز نطاق النّظام الاجتماعي، ونُخلق عالماً يزدهر فيه [المحتالون والإرهابيون]، وهم قادرون على القيام غداً بما هو أكثر مما يستطيعون القيام به اليوم».

لكن لم تكن جميع الأخبار سيئة بالنسبة للحكومة. ففي صيف 1993، اعتبرت خوارزمية الوثاب منيعة، في نظر فريق من «الخبراء المستقلين» بقيادة دوروثي دينينج ويضم كلاً من والت تكمان (الذي قاد فريق معيار تشفيراً لبيانات لدى شركة آي بي إم) وإيرني بريكيل (الذي فاز بجائزة الألف دولار، لقيامه بتفكيك شيفرة الحقبة المتعددة التكرار لميركل). وأصبحت دينينج شديدة

الضراوة في دفاعها عن الحكومة، مبينة بوضوح موقفاً يثبت الأخطار الناجمة عن فوضى التشفير، حتى أن النقّاد كانوا يطلقون عليها اسم «القراضة الحسنة» وقد جعلتها نزاهتها أشد تأثيراً في المتدييات العامة من الفريق التقني للإدارة المنهك والذي أخذ ظهوره في المؤتمرات ذات الصلة بالإنترنت يلقى من الحضور ما تلقاه عملية جراحية في الأسنان من ابتهاج وترحيب. فمن تراه يلومهم والأسئلة تنهال عليهم سؤالاً بعد سؤال وكلها تحفر في الحقيقة بأن نصارهم الطبيعيين من الراسخين في التكنولوجيا كانوا ينظرون إليهم على أنهم أشبه بأصحاب القمصان السمراء؟ [فاشيون. ه. م] وأصبح مايك نيلسون من البيت الأبيض يشير إلى الشيفرة بوصفها «بوسنة الاتصالات عن بُعد».

وما زال المقراض كما يبدو شيئاً ملعوناً. فعند كل منعطف كانت تبرز مشكلة جديدة على نحو غير متوقع. مثلاً، بعيد الإعلان عن الخطأ تصل بالحكومة أستاذ في معهد ماسا تشوستس يدعى سيلفيو ميكالي. وكان ميكالي الذي عمل في مجموعة الكريبتوجرافيا والرياضيات في المعهد (بقيادة رون رايفست)، قد ابتكر بضعة بروتوكولات رياضية، أطلق عليها اسم «أنظمة شيفرة عادلة» بدت مماثلة لمشروع وديعة المفتاح الحكومي. وكان قد نشر بحثاً حولها عام 1992 وحصل على براءة اختراع عنها. فدعت الحكومة لميكالي مليون دولار لقاء إجازة استخدام اختراعه.

كما ثبت أن اسم الرفاقة كان مشكلة أيضاً. وقد كتب بروكس في مذكرة وضعها في وقت مبكر من عام 1992، «كانا لمقراض الاسم الذي سترنا به في عمليات وكالة الأمن القومي العادية. وحاولت أن أحمل لنا س على عدم استخدامه خارج الوكالة، لكن صناع السياسة ومشاريهم وجدوا أن من الملائم جداً استخدامه إلى حد أنه صار ملازماً له». ومن المؤسف أن شركة تدعى انترجراف، كانت تباع في ذلك الحين معالماً مصغراً أطلقت عليها اسم «المقراض» فما اضطرت حكومة الولايات المتحدة أن تدفع لها مبلغاً كبيراً لقاء

استخدام هذا الاسم، الذي كان على وشك أن يصبح ما يطلق عليه المسوقون اسم مشؤوم.

أما المشكلات الأخرى فكانت محض تقنية. ومن ذلك ما صادف مصنع الرقاقات مايكو ترونكس، وكان مقاولاً حكومياً وتجارياً غير معتاد على طلبات السوق الاستهلاكية، ولم تكن الرقاقات مبنية لتتزداد بمعدلات مرتفعة من البيانات. وفي إسراعها لإدخال المقرض على هواتف إيه تي أند تي، كانت وكالة الأمن القومي قد ابتكرت منتجاً يمكن أن يلائم تكنولوجيا الاتصالات لعام 1993 لكنه كان غير كفاء على نحو يرثى له لأن يكون مناسباً للسرعة الكبيرة لتدفق المعلومات في المستقبل القريب الذي لا بد آت ربما بعد عامين أو نحو ذلك. وبكلمات أخرى، كما لاحظ النقاد بسخرية مريرة، بحلول الوقت الذي يستغرق في شركة ناجحة الأشهر الخمسة عشر إلى الثمانية عشر لبناء مُنتج حول المقرض سيكون العتاد قد تجاوزه الزمن.

«هل أحب أحدكم المقرض؟» كان قد طلب من المؤسسة القومية للمعايير والتكنولوجيا، معرفة تعليق الجمهور على الخطة، كجزء من العملية، فكان أن وجهت هذا السؤال. وقد استجاب ثلاثمئة وعشرون فرداً ومنظمة اثنتان منها فقط قابلت فكرة المقرض بالرضا. وهذا ما جعل لين مكنولتي المسؤول في المؤسسة القومية للمعايير والتكنولوجيا، يسلم بأن «ليس هذا بالتزكية الطيبة لبلاء مجيد».

لكن جماعة كلينتون لم يتزحزحوا عن موقفهم. ففي 4 شباط/ فبراير من عام 1994، صادق الرئيس رسمياً على المقرض - المعروف باسم معيار وديعة التشفير - بوصفه معيار معالجة المعلومات الفيدرالية. وسوف تشرع الحكومة على الفور في شراء هواتف إيه تي أند تي المجهزة بالمقرض لاستخدامها الخاص، وإيداع المفاتيح في المؤسسة القومية للمعايير والتكنولوجيا ووزارة المالية. (على الرغم من أن التكنولوجيا لم تكن متوفرة فعلاً، بعد، للقيام بلك

الشيفرة للمفاتيح المسترجعة من تسهيلات الوديعة غير الموجودة حتى الآن).

كتب تيم ماي: «إن إعلان الحرب علينا وشيك، فقد أظهر جماعة كليبتون وجور أنفسهم، بمظهر المؤيدين المفعمين حماسة للأخ الكبير».

وفي مجلس الشيوخ أقسم باتريك ليهي مع آخرين سواه، على محاربة المقرض، وألح على أنه دون موافقة الكونجرس لا يمكن تمويل المشروع (كلفة وضع البرنامج تبلغ 14 مليون دولار، إضافة إلى 16 مليون دولار سنوياً مخصصة لتسهيلات الوديعة). وفي أيار/ مايو 1994 عقد السيناتور ليهي جلسة استماع. وفي ظهور علني نادر عرض كلينت بروكس ومايك مك كونييل للمشهد، من وجهة نظر من وراء السياج الثلاثي، مهتماً الإدارة لاتخاذها الطريق الصحيح. وخلص مك كونييل إلى القول: «هنالك، بلا ريب، مسائل ينبغي تسويتها، لكنني على ثقة من أننا سوف نتخلص من الشوائب وتمتص الأمور».

ثم أظهرت مجموعة من المناوئين، أن تلك «الشوائب» بحجم حوض نهر كولورادو تقريباً.

وكان من بين الأسئلة العسيرة التي وجهوها: «من الذي سوف يقبل على استخدام المقرض، في حين أن هناك برامج جاهزة مثل بي جي بي؟» وكانت استجابة الحكومة «نظرية اللص الغبي»، التي شرحها جيم كالستروم من مكتب التحقيقات الفيدرالي على أحسن وجه، والذي زعم بأنه حُمل على سماع رجال عصابات كانت خطوطهم الهاتفية مراقبة، يسخرون من كونهم يخضعون للتفتيش، ويشاركون في أحاديث فيها إدانة لهم لتورطهم في أعمال إجرامية، لمجرد أنهم يجدون مشقة في الخروج واستخدام هاتف للعموم. وقال: «إذا ما راج المقرض في غضون خمس سنين، ووضعنا الناس في أجهزتهم، فإن نسبة عالية من المجرمين سوف يذهبون إلى راديو شاك، أو أي مكان آخر مشابه له لشراء مفكك تشفير من نوع ما. إنهم لن يتذكروا أنه في عام 1994 [ظهرت] مقالة هامة في مجلة وول ستريت جورنال [حول وديعة المفتاح]. ولربما وقعنا

في مكان ما من المطبوعة الراقية على أن المقراض شيء ذو شأن. لكن لن يكون ظاهراً لكل ناظرٍ [لبل] سوف يكون جزءاً من المشهد العام. وهذا مبتغاناً».

حسن، إذن فقد استخدمه اللصوص الأغبياء. ولكن الشهود المناهضين للحكومة لاحظوا أنه إذا ما أعرض المجرم الذكي عن المقراض، فإن الزبائن فيما وراء البحار الذين لهم أعظم الأهمية في تبنيه، سيفعلون ذلك أيضاً. فما الذي يحمل فرنسا، أو اليابان، أو إندونيسيا على التوقيع على خطة تجعل المفاتيح لمحادثات مواطنيها الخاصة - التي ربما تتضمن أسراراً تجارية لا تقدّر بثمن - بيد فرعين من أجهزة حكومة الولايات المتحدة؟

ولربما كان هويت ديفي الشاهد الأكثر إقناعاً. وقد شهد ليس بوصفه أحد مبتكري المفتاح العام وحسب، بل بوصفه أيضاً مثلاً لإحدى جماعات الضغط المناوئة للمقراض، جماعة العمل من أجل الأمن والسريّة الرقمية. حاول ديفي أن يضع المسألة في منظور تاريخي. فالحكومات كانت معنية على نحو مماثل بالثورات السابقة في مجال الاتصالات، مثل الكيبل الممتد عبر الأطلسي وشيوع الراديو. وبالرغم من المخاوف التي كانت تتاب الحكومات من أن تفقد سيادتها، فقد ثبت في النهاية أن هذه لتطورات كانت ذات فائدة عظيمة لها. والآن يُرجّح أن تزيد الاتصالات بالكمبيوتر إجمالاً في قوة الدولة. لكن الولايات المتحدة بدت كارهة لأن يكون لمواطنيها أيّ من تلك القوة. وفي حين أن الحكومة تدعي الرغبة في الاحتفاظ بقدرتها على التنصت وحسب، فإن الحقيقة أنه في عهد الآباء لمؤسسين، كان من السهل الحصول على السرية، بمجرد الابتعاد عن مدى سمع الآخرين. وقال ديفي: «يبدو أن حق المجتمعين في اتخاذ التدابير لضمان سريّة للحدوث كان أمراً يكاد لا يقبل الشك، بالرغم من أن حق سريّة الحديث قد يُسَاءل استعماله فيكون في خدمة الجريمة». واليوم، يتصل الناس ببعضهم، بطرق إلكترونية، إلى حد بعيد، تراوح بين الها تف

والكومبيوتر. فهل يمكن أن يكون للحكومة، الحق في منع السريّة في هذه المحادثات؟ وأخبر ديفي أعضاء مجلس الشيوخ: «إن شرعية القوانين في المجتمع الديمقراطي تنشأ عن لسيرورة الديمقراطية. وما لم يكن الناس أحراراً في مناقشة الآراء المطروحة حول القضايا - والسريّة مكون أساسي للعديد من هذه المناقشات - لا يمكن لتلك العملية أن تتحقّق».

بعيدانتهاء جلسات الاستماع في مجلس الشيوخ، تعرض المقراض لضربة قد تكون الأسوأ بين جميع الضربات التي تلقاها. ولم تأت كخطبة سهبة عنيفة في الكونجرس، أو هجوماً شتّه أحد ممثلي لصناعة، أو مقالة غير رسمية من أحد زعران الشيفرة، بل كانت نتيجة لتجربة علمية أجراها عالم باحث مغمور يدعى ماثيو بليز. وكان ما فعله هو أنه جعل رفاة المقراض، تبدو غبية.

كان بليز من أبناء نيويورك، وباحث جريء في العلوم الكلاسيكية، وقد انقطع عن الدراسة في إحدى المدارس الإعدادية الخاصة، وعمل حيناً ممرضاً (أول شخص توظفه مصلحة الإسعاف الطبي للمدينة بدون رخصة قيادة سيارة)، ثم انتقل إلى الدراسة الجامعية، وحصل على إجازة في علمين متعارضين في ظاهرهما: الكومبيوتر والعلوم السياسيّة، وأثناء قيامه بالدراسات العليا في جامعة كولومبيا، بدأ يفكر جدياً بالشيفرة. وخلال حديث له مع أحد زملائه في المكتب، ويدعى ستوارت هابير، الذي كان قد ابتكر طريقة لاستخدام المفتاح العام لتاريخ الوثائق رقمياً (مقدماً مرادفاً إلكترونيّاً للعادة القديمة بختم الرسالة بخاتم البريد لتحديد تاريخها)، أدرك بليز أن الشيفرة كانت طريقة لمعالجة مشكلات هامة في الرياضيات ورافعة عمليّة لتغيير المجتمع على حد سواء. وكان بليز كذلك شديد الإيمان بحق الإنسان بالسريّة.

بعد انتقاله إلى جامعة برنستون، وحصوله على الدكتوراه، مضى ليعمل مع مجموعة تشفير صغيرة في مخبر بل للبحوث التابع لشركة إيه تي أند تي.

وبدأ بليز العمل في مجالات تشفير أخرى، ما عدا الخوارزميات. وكانت مجموعته معنية بالبحث الأساسي، أكثر من مجموعة نظام الأمان، لشركة إيه تي أند تي في نورث كارولينا، التي كانت قد أنتجت جهاز تي إس دي 3600، الذي وقع الاختيار عليه ليكون جهاز الهاتف ذي المقراض. والواقع أنه اكتشف موضوع المقراض أثناء قراءته الصحفية مثل أي شخص آخر.

لكن إدارة كلينتون، فيما هي تعدد للمصادقة على معيار الوديعية في شباط/مارس 1994، أجرت سلسلة من الجلسات الإطلاعية الفنية، ضمت في عدادها مجموعة الشيفرة في مختبر بل. كذلك حضر العديد من العلماء لدى وكالة الأمن القومي، إلى نيوجرسي للاشتراك في إحدى الجلسات الإطلاعية. ومع أنه يمكن وصف مجموعة الشيفرة عموماً، بأنها مناهضة لرقاقة المقراض فضلاً عن مضامين السريّة، وبوصفهم كريبتوجرافيين، فقد شعروا بالضيق من المخاطر الأمنية التي ينطوي عليها إرسال المفتاح إلى فريق ثالث، ويقول بليز: «لقد تدبرنا أن نحسن التصرف، وألأندع اللقاء يهبط إلى مستوى مناقشة ما إذا كانت هذه فكرة جيدة أم لا». وفيما بعد، سأل إن كان بإمكانه أن يرسل ملخصاً لما جرى في الاجتماع عبر الإنترنت، وكان أن التزم بليز بالوقائع في ذلك أيضاً.

وقد أثار هذا إعجاب من كانوا خلف السياج الثلاثي، الذين زين لهم الفكر على ما يظهر أنه يمكن الاستفادة من بليز مختبر آخر من الخارج لتكنولوجيا المقراض. فتمت دعوته مع أحد زملائه إلى فورت ميد لدراسة نموذج أولي لتيسيرا Tessera وهي النسخة التي تعتمد على البطاقة الذكية من نظام الوديعية (كان مقيضاً أن تكون تيسيرا نسخة قابلة للحمل من نظام تشفير القمة بكل محتوياته الذي كان كلينت بروكس يفضل على رقاقة المقراض المحدودة). وهناك شعر بالإثارة إذ لم يسبق له أن دخل المكان من قبل. وقد أعطي شارة الزائر المعتادة مع جهاز حسّاس لتعقب خطواته في البناء: وحينما اصطحه مضيفه معه، كان عليه أن يظل في مواجهة آلات التصوير الأمنية،

ويطمئن حارساً غير مرئي بأن بليز برفقته، وقال صوت يستحيل تبين صاحبه: «حسن، شكراً». حتى بين قاعة الاجتماع والحمام تكرر هذا الأمر مرتين. ويقول بليز: «لكنهم لم يتبعوني فعلاً إلى الحمام»، وحين غادر علماء مختبر بل، قدمت لهم بطاقات تيمسيرا ومجموعة من الكتيبات الشارحة وأباريق قوة خاصة بوكالة الأمن القومي.

شرع بليز على الفور في اختبار النظام، مركزاً على الجوانب المتصلة بالمقراض في الجهاز. وبخلاف فريق دوروثي دينينج، الذي ركز على الوثاب، تساءل بليز ما إذا كان ثمة طريقة، لاستخدم التشفير المنيع فعلاً بينما يجري التغلب على مقومات الوديعة. وبكلمات أخرى، هل بإمكان لص، أو إرهابي، أو شخص ما يرغب في السريّة وحسب أن يستخدم شيفرة المقراض دون أن يتم اكتشاف شخصيته؟ وقد ركّز جهوده على دراسة مجال مدخل حفظ النظام. يقول: «لم أكن لأفكر حتى أن أعتبرها موطن ضعف محتمل، لكن اتضح بأن الطريقة الواضحة للتغلب على مجال مدخل حفظ النظام كانت أول ما ينبغي أن يخطر ببالك».

بدأ في إجراء الاختبار، مستخدماً في ذلك قارئ بطاقة وبرنامجاً صغيراً يحاكي التنصت عبر الأسلاك. وجرب أبسط الأشياء - مثل تغيير الرمز بحيث لا ترسل المعرف، أو إرسال رقم ما آخر محل المعرف - لكنها لم تنجح. إلا أن الأمر استغرق قدراً من التفكير وطرقاً أكثر تعقيداً بقليل حتى تحقق له النجاح. وجاء الاختراق حينما لاحظ بليز، وهو منكب على مطالعة هذه الكتيبات، بأن «ضبط المجموع» في مجال مدخل حفظ النظام كان مداه 16 بت فقط. (ضبط المجموع طريقة للثبث من أن مجال مدخل حفظ النظام، بما في ذلك معرف الرقاقة ومفتاح الجلسة الذي قام بتشفير المحادثة، قد تم إرسالها إلى المراجع فعلاً. إن العدد المناسب في ضبط المجموع أشبه بعباراة «كل شيء واضح»، التي تعني أن الأمور على ما يرام. وإذا ما كانت هنالك طريقة لتزييف مجال

مدخل حفظ النظام، مع ضبط مجموع صحيح، فإنك ستكون في الواقع قد ألحقت الهزيمة بنظام المقراض. إن التشفير سيعمل، لكن المتنصتين عبر لاسلاك لن يتوفر لهن مفتاح الجلسة المناسب لفك شيفرة المحادثة).

يقول بليز: «إن ست عشرة بت ليست عدداً كبيراً جداً في هذه الأيام، لإجراء العمليات الحسابية». وفي غضون ساعات قليلة وضع «منفاخاً لمجال مدخل حفظ النظام» وهو برنامج سريع يمكن أن يصدر كل تركيبة ممكنة (2¹⁶) من أعداد ضبط المجموع، ثم قام بربطه بنظام الاختبار الخاص به، والحق أنه لم يكن يتوقع أن ينجح، لقد بدا سهلاً جداً. لكنّه نجح فعلاً، في كل مرة كان يجربه فيها. وفي ما لا يزيد على اثنتين وأربعين دقيقة، كان قادراً على إرسال ضبط مجموع يخدع نظام الوديدة بأن جعله يفترض خطأ أنه كان يرسل البيانات، التي ترشد المحققين إلى المفتاح المودع، في حين أن هذه البيانات مضللة، ولا تقودهم إلى أي شيء. بل إن المتنصت سوف يواجه، عوضاً عن ذلك، محادثة مشفرة بخوارزمية الثواب القوية الفعالة، التي تعتبرها وكالة الأمن القومي ذاتها غير قابلة للتفكيك. (كذلك وجد طريقة تمكن شخصين متآمرين من التغلب على مجال مدخل حفظ النظام بسرعة أكبر أيضاً).

وما كان يجهله بليز هو أن المدى الصغير لضبط المجموع لم يأت مصادفة بل جاء نتيجة الاستعجال في أعداد المقراض. ذلك أنه أثناء عملية التصميم المتعجلة، تشاور مهندسو وكالة الأمن القومي، مع مختلف الخبراء الفنيين في شركات الهاتف، الذين حذروهم من أنه بعد نزول الهواتف اللاسلكية، فإن أي نظام يتطلب بث الكثير من البتات سوف يعتبر غير عملي. وهكذا حدّد مجال مدخل ضبط النظام بـ 128 بت منها، 32 بت تستخدم لتعريف الرقاقة، بينما تتركس الـ 96 بت الباقية لمفتاح التشفير وضبط المجموع. وكانت وكالة الأمن القومي ترغب في ضبط مجموع كبير، لكن مكتب التحقيقات الفيدرالي أصرّ على استخدام 80 بت، بحيث يمكن بث مفتاح

الجلسة بالكامل. (ولربما كان ثمة بديل، يتمثل بالكف عن استخدام بعض بتات المفتاح، والسماح لمكتب التحقيقات الفيدرالي، بإتمام فك التشفير بواسطة هجوم بالقوة الغاشمة. وإذا ما تم، مثلاً، تحويل ثمانية بتات من مدى المفتاح إلى ضبط المجموع، أمكن لمكتب التحقيقات الفيدرالي أن يتفحص مجرد 256 بديلاً مختلفاً ليجد المفتاح، لكن محاولة بليز لحل ضبط المجموع سوف تستغرق أكثر اثنتين وأربعين دقيقة، بل ما يزيد على أسبوع. وفي ذلك ضياع وقت طويل).

وفي غضون بضعة أيام، أرسل بليز مسودة أولية بنتائج بحثه إلى زملائه في مختبرات بل. لكن معظمهم لم يستطع تصديقها، وسألوه: هل أنت متأكد من هذا؟ واقترحوا ضرورة مراجعة عمله من جديد. ولقد قام بذلك. ثم بدأ عملية مراجعة أكثر تدقيقاً وتمحيصاً بالاستعانة بشخص من الخارج. وذات صباح شمر بليز عن ساعديه وأرسل مسودة ما قام به بالفاكس إلى فورت ميد. وبعد الغداء مباشرة أتاه الرد الذي يؤكد صحة استنتاجاته من الناحية التقنية.

سأله الشخص، الذي اتصل به من وكالة الأمن القومي: «ما الذي تخطط له فيما يتصل بهذا العمل؟»

أخذ بليز نفساً عميقاً. «أود أن أنشره».

ولقد أدهش أنه لم يجد معارضة لذلك. بل إن القارئ في وكالة الأمن القومي، أشار إلى خطئين وقعا عند نسخ الأرقام وخطأ نحوي واحد. والآن كان كل ما على بليز القيام به هو الحصول على موافقة الشركة التي تستخدمه، التي كانت تراهن بملايين الدولارات على الهواتف ذات المقرض. وبرغم وجود البعض الذين كانوا يرغبون في دفن البحث، استطاع بليز في النهاية إقناع رؤسائه، أنه من المستحيل إبقاء نتائج بحثه طي الكتمان، وبالتالي يجب ألا يفكروا حتى بمجرد محاولة التكتّم عليها. على أية حال كما نت أخبار هذا العمل قد تناهت إلى سمع جون ماركوف، من صحيفة نيويورك تايمز. حصل

بليز على الموافقة بإرسال مسودة له، ليضمن دقة الرواية، مهما تكررت لقصة التي بلغته. واتصل ماركوف به ليحصل على بعض لإيضاحات. وبعد بضع ساعات عاد يتصل من جديد ووجه سؤالاً غريباً لبليز: هل يعتبر قصته تستحق الاهتمام؟ لقد كان بليز يشعر بأنها كانت قصة جديرة بالاهتمام فعلاً إذ أظهرت كيف كانت وكالة الأمن القومي مستعجلة لإخراج نظامها، وأكدت على مدى خطورة إكراه الناس على قبول شيء لم يبلغ النضج بعد. لكنها ليست قصة لتصدر الصفحة الأولى أو شيء من هذا القبيل. وبعد وقت قصير، اتصل ماركوف مجدداً، وهو يعتذر تقريباً، وقال أن اليوم فقير بالأخبار ولذلك فإنه سوف يخصص للقصة مكاناً أكثر بروزاً. وبناء على ذلك حسب بليز، أن للموضوع سيتصدر صفحة الأعمال التجارية.

كان قد سمع أن بوسع المرء الحصول على صحيفة اليوم التالي في التاسعة مساءً من مبنى التايمز، ولشدة فضوله ذهب إلى هناك في ذلك الموعد. بعد أن تصفح الصحيفة بدقة وعناية، أصيب بخيبة أمل إذ لم يجد شيئاً. «لم يخطر ببالي حتى أن أنظر إلى الصفحة الأولى إلى أن خرجت من المبنى». لكنها كانت هناك تتصدر الصفحة كلها في المكان الأبرز من الصفحة الأولى، بعنوان «اكتشاف خطأ، في الخطة الفيدرالية للتنصت على المكالمات الهاتفية».

وكان لهذا مغزاه من عدة وجوه. أولاً، مع أن الخطأ ذاته يمكن إصلاحه - ويمكن المجادلة بأنه لم يعرض الأمن للخطر إلى حد بعيد - فإن الحقيقة القائلة بوجود ضعف كهذا لحقت وصمة دائمة بنظام يعتمد على ثقة الجمهور. ولربما كان الأهم من ذلك أن حالة الركود السابقة، والكلام غير المفهوم عن الشيفرة قد أبرزوا هذه الناحية بحيث أن تطوراً معتدلاً مثل تفكيك بليز للشيفرة يمكن لمحوري التايمز النظر إليه على أنه لقصة الأكثر أهمية في العالم ذلك اليوم. وما جعل هذا الموضوع الجاف مثيراً، كان ما فاح من رائحة الأبخ

الكبير، الذي لم يستطع حتى، وضع برنامج بشكل صحيح. وقد أوقعت الحكومة نفسها في هذا الدور عن غير قصد، حينما أصدر مسؤول متعجرف في وكالة الأمن القومي، بأن هجوم بليز، بالرغم من أنه معقول، فإن تطبيقه عملياً بعيد الاحتمال، وهذا ليس ضماناً واضحة بشكل خاص، للقائمين على الشيفرة في البلاد. وكان أقوى من ذلك تأكيد مارتي هيلمان: «إننا لحكومة تخوض معركة عسيرة».

وفي غضون ذلك، وبعد عدة مشكلات تتعلق بالتجهيزات الأولية، شرعتا لحكومة في استخدام الهواتف ذات المقراض. (كانت رقائق القمة الأكثر شمولاً، والمصممة لضمان لا تُصّلات عبر الكمبيوتر، قد دخلت خط المعالجة منذ عهد قريب). وجرت العادة على أن يقوم أربعة رسل مزودين بتصاريح أمنية، اثنان من المؤسسة لقومية للمعايير والتكنولوجيا واثنان من وزارة الماليتبالا نتقال بالطائرة من واشنطن العاصمة إلى تورانس في كاليفورنيا، مرة كل أسبوع، إلى ما يسمى بمنشأة البرمجة بمقر إدارة مايكوترونكس. (كانت الوفرة مقصودة شخصية لسلامة وتتفق مع بروتوكولات المستخدم في رقابة الأسلحة النووية). حين يصبح في الداخل فإنهما ينتظرن محطة التشغيل صن حتى تنجز عملها، حيث تولد أولاً مفاتيح التشفير الفريدة التي سيتم إدخالها في رقاقت إم واي كي MYK-78 (المقراض) ثم تقوم بتقسيم المفاتيح إلى جزئين وابتكار مجموعتين من الأقراص المرنة، في كل منها مجموعة من المفاتيح الجزئية. وإن تكويناً لمفاتيح الكاملة داخل الرقاقت يتطلب كلتا المجموعتين من الأقراص.

وإن إنتاج مجموعة الإسناد يتم بالطريقة نفسها. ثم يتم فصل الأقراص، وتذهب كل مجموعة منها ممهورة بخاتم بلاستيكي، مع اثنين من الرسل. وعندما يعود الرسل كل اثنين إلى الهيئة التي أرسلتهما، توضع الأقراص في خزائن مزدوجة الجدران وفق مقاييس الحكومة للمواد المحظورة. ويتم إدخال

مجموعات الإسناد إلى خزانة أخرى. حيث تنتظر هناك، نحو 20,000 مفتاح مجزأ بحلول شهر أيار/ مايو عن عام 1994، وهي آمنة مطمئنة فيما حرب المقرض مستمرة.

في أواخر كانون الثاني/ يناير من عام 1994 وجّه العاملون في الكمبيوتر من أجل لمسؤولية الاجتماعية رسالة إلى الرئيس يحثونه فيها على إلغاء الاقتراح الداعي للأخذ بالمقرض، وشاركهم في التوقيع عليها خبراء في السرية، ورجال الأعمال لصناعة، وأكاديميون، وكريبتوجرافيون، وأضيفت إليهم توقيع أخرى تم جمعها عبر الإنترنت. وفي غضون بضعة أشهر، فاخرت العريضة - إحدى أوائل الاحتجاجات السياسية عبر الإنترنت - بأنها جمعت ما يزيد على 47000 توقيعاً. وفيما قد يرفض مرتاب هذا بالقول بأنه جاء نتيجة حماس مبالغ فيه من الشبكة، فإن استطلاعاً للرأي أجرته النيويورك تايمز والسي إن إن أظهر أن الحكومة قد عانت هزيمة منكرة بحجم الهزيمة التي لحقت بالجنرال كستر [قائد عسكري أمريكي حارب الهنود الحمر وقتل بسبب سوء تقديره. ه. م.] في ميدان لعلاقات العامة. إذ أن ثمانين بالمئة من الجمهور الأمريكي حالياً، يعارض المقرض.

لكن ذلك لم يكن له أثر يُذكر. فقد كانت الإدارة تراهن، على أن تحول أنظمة التصدير، دون إدخال الشيفرة المنيعة، في المنتجات التي يستخدمها الناس عادة، وستكون وديعة المفتاح هي الخيار الوحيد المتاح في الولايات المتحدة. لكن الكونجرس كان يملك السلطة لتغيير تلك الأنظمة. وأكثر من ساهم في الضغط في هذه المسألة، كانت امرأة عازبة في الثامنة والثلاثين من عمرها، تدخل الكونجرس للمرة الأولى.

كانت ماريكاكا نتويل ابنة سياسي من إنديانا. انتقلت إلى ولاية واشنطن في العشرينات من عمرها، حيث عملت في المجلس التشريعي هناك، وفي عام 1992 فازت رغم الصعاب بمقعد في الكونجرس لتمثل المنطقة التي تتألف من

جزء من سياتل، والمدن الواقعة شرقي بحيرة واشنطن، وهي منطقة زاخرة بشركات التكنولوجيا المتقدمة، من نيتندو إلى مايكروسوفت. ولذلك انصب اهتمامها، عند اختيارها لعضوية إحدى اللجان، على أحد المشاغل الرئيسة لصناعة البرمجيات، وهو التصدير، فتقدمت بطلب للانضمام إلى لجنة الشؤون الخارجية - وعلى وجه التحديد لجنيتها الفرعية، للسياسة الاقتصادية والتجارة والبيئة.

وكانت بالكاد قد ألفت الكونجرس لتجد حجرة إيداع المعاطف عندما وصلت أنباء الإعلان عن المقرض. وكان هذا مدعاة لإثارة غيظ ناخبها من أصحاب كبريات شركات التكنولوجيا المتقدمة، وأخذت تمعن النظر في المشكلة وتعمق في دراستها، وخاصة ما يتصل منها بأنظمة التصدير. وراحت تعمل عندئذ بشكل وثيق مع شركات البرمجيات التي تأثرت بالإعلان، لا تلك التي في منطقتها وحسب مثل مايكروسوفت بل شركات أخرى أيضاً مثل لوتس. وكلما ازدادت اطلائاً على أنظمة تصدير الشيفرة، كلما بدت لها شدة سخافتها في عصر الكمبيوتر. وقالت لسام جيجدينسون، رئيس اللجنة الفرعية وأحد ناصحيها التشريعيين: «لا يمكن أن يكونوا قصيري النظر إلى هذا الحد ليحسبوا أن الكريبتوجرافيا سلاح حربي. وإذا ما استمروا على هذا المنوال فإنك لن تكون قادراً على الحصول على حماية على الإنترنت».

وفي غضون ذلك، كان وضع التصدير قد بلغ حالة العطالة تماماً. وقام بعض قادة الصناعة الجديدة، مثل راي أوزي من لوتس وناثان مرفولد من مايكروسوفت ببذل جهود جبارة، في عام 1992، وهم يتفاوضون مع وكالة الأمن القومي. وكانت تلك المفاوضات عبارة عن صدامات بين ثقافات متعارضة. وقد اعتبر رجال البرمجيات سعي الحكومة لإبقاء أجزاء من الشيفرة داخل الولايات المتحدة نفسها موضوعاً مثيراً للسخرة، في حين أن خوارزميات الشيفرات تنتشر دون أي قيد في دول من ألمانيا إلى روسيا. إن

الخطيئة الأكثر سوءاً هي التصرف غير المنطقي. أم أنه كان منطقياً؟ وفي إحدى المناسبات وجّه مرفولد سؤالاً إلى أحد الأشباح، في جلسة من جلسات المذاكرة: «ألا تدرك أنك في هذا أشبه ما تكون بصبي هولندي صغير، تحاول استخدام أصابعك لتسد خرقاً في سد أمام بحر من الشيفرة المنيعه؟».

ابتسم الرجل المشاكس، وقال بتؤدة: «إن كل يوم يستمر فيه السد دون أن ينهار هو نصر». وكان ذلك صحيحاً. لا ريب في أن عفريت الشيفرة قد أفلتت من الزجاجة. لكنك إذا ما ألقيت في طريقه، مقداراً كافياً من العقبات، فإنه سيحتاج إلى وقت طويل حتى يتمكن من الإتيان بعمل سحري.

أخيراً، أدت تلك الجهود التي بُذلت إلى تسوية مؤقتة. فقد حصلت الشركات بالتعاون مع جماعة صناعية تُعرف باسم اتحاد ناشري البرمجيات، على الموافقة «لاعتبارات ملحة» لتصدير برمجيات على أن يتم تقليصها وتغليفها لتباع للزبائن التجزئة. وكان الشرط الأساسي أن التشفير في تلك المنتجات سوف يكون بشيفرات رون رايفست آر سي - 2 أو آر سي - 4، واستخدام مفاتيح لا يزيد مداها على 40 بت. على أن يزداد هذا، كما يزعمون، في السنوات اللاحقة لمجاراة الكومبيوتر الأسرع. وفي المقابل، حصلت وكالة الأمن القومي على قيود خاصة بها. لن يكتب هذا النظام صفة رسمية بأن يعتمد معياراً بصورة صريحة. واضطرت شركة آر إس إيه والشركات الأخرى التي تستخدم الشيفرة لأن توافق على إبقاء تفاصيل تصميمها سراً.

ولم يلق هذا الاتفاق من يميل إليه بشكل خاص. إلا أن المطروح أمام الشركات أحد خيارين: الأول أن تقدم، مثلما فعلت لوتس، للزبائن الأمريكيين نسخة بتشفير (64 - بت) المنيع، ونسخة أضعف للتصدير. عندئذ سوف يتساءل الزبائن الأجانب لماذا كانت برمجياتهم تقتصر على شيفرة من الدرجة الثانية، وفي بعض الأحيان، يشترون منتجات أخرى. وقد ذهب راي أوزي إلى الزعم، بأن هذا ما كان يحدث مع لوتس في ذلك الوقت. (وأطلق على الـ 40 بت كحد

أقصى اسم التشفير القابل للتجسس). أو الخيار الثاني مثلما فعلت مايكروسوفت ويتضمن تجنب متاعب التصنيع وشحن نسختين، بأن تقدم للجميع تشفيراً ضعيفاً. وفي غضون ذلك، شعر المتشددون في الحكومة، أن إعطاء الضوء الأخضر للسماح بالتصدير، مهما يكن طول المفتاح، فإنهم يكونون على منحدر زلق باتجاه شيفرة منيعة. قدموا لشركات مثل لوتس ومايكروسوفت أربعين بت الآن، فسوف تجدونهم يطرقون أبوابكم مطالبين بأجهزة من ثمان وأربعين بتاً، وأكثر.

لكن عندما ذهب كانتويل وجيجدينسون إلى البيت الأبيض، للمطالبة بالسماح بتصدير شيفرة أكثر قوة، ارتطما بجدار من الآجر. فقد وجدوا جماعة كليتون ثابتين على موقفهم.

وفي تشرين الأول/ أكتوبر من عام 1993 عقد جيجديسون وكانتويل جلسة استماع للجنة الفرعية، ليلفتا الانتباه إلى المشكلة. قال جيجديسون: «إن جلسة الاستماع هذه مخصصة لمحاولات وكالة الأمن القومي الحسنة النية للسيطرة على ما لا يمكن التحكم به». كان يتحدث عن قوانين التصدير، لكنه ربما كان يتحدث عن أمر آخر - الدعم من الكونغرس الذي اعتبرته فورت ميد ذات مرة أمراً بديهياً. وبينما قبلت الأغلبية من أعضاء الهيئة التشريعية مزاعم وكالة الأمن القومي، كما قدمها أصحابها، وكان ثمة تنافر معرفي أخذ يبرز بين ما كانت تسوقه من حجج وما بدا أنه نظرة للواقع أكثر قوة وإفحاماً. وقد عبرت كانتويل عن ذلك بوضوح في بيان الاستهلاك: «إننا هنا لتبادل الآراء، حول رؤى متعارضة للمستقبل». من جهة كان ثمة مجموعة من العقول أسيرة الأوضاع التي كانت سائدة أيام الحرب الباردة إلى حد أنها تجاهلت ما هو محتم ولا يمكن تجنبه. ومن جهة أخرى كان هناك الحالمون التقنيون الذين زودوا مستقبلنا بالقوة المحركة، والتواقون إلى تدعيم الهيمنة الأمريكية في السوق العالمية.

كان أول شاهد في جلسات الاستماع راي أوزي، الذي جاء مجهزاً بنسخة عرض برمجية. وكانت لثيافة متصلة عبر خط هاتف بكمبيوتره في ماسا تشوسيتس، الذي كان يستخدمه لاقتحام لإتترنت وتنزيل واحد من «مئات الآلاف» من نسخ تطبيقات معيار تشفير البيانات المتوفرة وراء البحار. وقد وقع اختياره على واحد في ألمانيا، وقام بتنزيله في آلتة خلال ثوان، كما يقوم بذلك أي شخص في العالم. لكنه، لاحظ، أنه إذا ما عمد عندئذ إلى إعادة البرمجيات ذاتها إلى ألمانيا، فيجرم لقيامه بتصدير الشيفرة المنيعة، التي يعاقب عليها القانون الفيدرالي.

أما لشاهد التالي فكان ستيف والكر، وهو مسؤول سابق في وكالة الأمن القومي ويتراس الآن ترستيد أنفورميشن سيستمز، وهو مكتب استشاري، يساعد الشركات التجارية على تطبيق الشيفرة. وقد عرض نتائج دراسة قام بها اتحاد ناشري البرمجيات حددت 264 منتج تشفير، يتم إنتاجها وراء البحار، 123 منها تستخدم معيار تشفير البيانات. وبما كان الأجانب والشركات الأجنبية شراء أي منها، ولكن ليس منتجات مماثلة بتكرها الشركات الأمريكية لأن وكالة الأمن القومي لا تجيز تصديرها. وقال: «لا يمكن أن يكون الأمر أكثر وضوحاً. إن وجود منتجات تشفيرية واسعة الانتشار ومتاحة في الأسواق حقيقة ماثلة لا تقبل الجدل... إن حكومة الولايات المتحدة نجحت في الواقع في شل قلتر صناعة أمريكية حيوية، وحسب». ثم أورد أمثلة معينة على صفقات تجارية أضاعتها شركات أمريكية، مثل إحدى الشركات التي أضاعت نصف زبائنها الأوروبيين بسبب عدم استطاعتها تزودهم بشيفرة منيعة ومأمونة.

وبين فيل زيمرمان في شهادته، أن محاولة تقييد الكريبتوجرافيا، أشبه بمسعى لـ «تنظيم أمواج البحر والطقس». وشدد دون هلمر، المدير التنفيذي لشركة ديجيتال إكويمنت كوربوريشن على القول بأن من الضروري أن تعدل

قيود التصدير في الولايات المتحدة المفروضة على التشفير بحيث تتفق مع الواقع».

وكان أحد أعضاء اللجنة شخص لم يسبق أن عرف عنه الاعتراض على الحكومة، وهو محافظ من كاليفورنيا، يدعى دانا روه باتشر، وقد نبه بصورة رسمية إلى أن ذلك لو وقع قبل خمسة أعوام، لقام بمعاقبة الشهود، لاستغلالهم وضعاً يحتمل فيه فقدان الأمن القومي. لكنه الآن يقول: «إن الحرب الباردة قد وضعت أوزارها. وحن الوقت لكي نتقدم».

بعد الجلسة العامة، تفحص خبراء الأمن، القاعة بشكل دقيق، بحثاً عن أجهزة تنصت، قبل جلسات المتابعة لمحتومة، التي تمس مصالح وكالة الأمن القومي، وقال جيجدنسون: «إن جلسة الاطلاع هي المكان الذي تجيب فيه وكالة الأمن القومي على جميع تلك الأسئلة سراً». وكانت مطالعات وكالة الأمن القومي ذات صيت سيء في دوائر الكونغرس. حيث تشتمل على عرض مؤثر توضح فيه الوكالة الأسباب التي تجعل قدراتنا على التنصت الدولي، أمراً حيوياً إلى حد بعيد، وتتضمن كما هو مألوف تمجيداً بانتصارات تتحقق بالتطفل الخفي (انتصارات لم تكن ليتم التفكير بها دون رصد اعتمادات ببلابين الدولارات)، وأوضاع دولية محفوفة بالمخاطر تتطلب يقظة ودعمًا متواصلين. وكان بوبي إنمان، قد تولى إيصال الوكالة إلى حد الكمال حين كان مديراً لها، ومنذ أيامه أدخلت الوكالة أعضاء من الهيئة التشريعية في عضوية جمعية لري للغاية» فحولوا تحالفهم الضمني من المواطنين إلى وكالات الاستخبارات. وخلاصة الأمر أن عضو الكونغرس المنضم حديثاً إلى الهيئة التشريعية سوف ينال جرعة صريحة ومروعة من المعرفة بحقائق العالم، يفترض به أو بها بعد ذلك دعم أي مطلب تتقدم به وكالة الأمن القومي وإلا نال «الهنون البرابرة» من حريتنا بصفقة تجارية. وقد عرف عن أعضاء مجلس النواب والشيوخ دخولهم القاعة المنظفة من أجهزة التنصت، والخروج منها بوجوه متجهمة، ليفاجئوا

مستشاريهم المتقدين حماساً، بقولهم: «حسن ربما يجب علينا أن نعيد النظر في الأمر».

لكن هذا لم يكن شأن ماريّا كانتويل. إذ كانت بين عدد متزايد من أعضاء الهيئة التشريعيّة الذين وجدوا مطالعة الوكالة مؤثرة إنما غير مقنعة. فالمسألة بالنسبة لهؤلاء المرتابين لم تكن مبلغ أهمية الشيفرة وحسب، أو النجاح الذي تحقّق لنا بفك الشيفرة، بل ما إكالا نت المحافظة على قوانين التصدير مثمرة حقاً. ثم ماذا لو أفلت العفريت من القمقم، ولم يكن بوسع الشركات الأمريكية بالتالي القيام بتصدير مُنتجاتها؟ فإن المحتالين سوف يحصلون على الشيفرة من أماكن أخرى!

بدأت كانتويل، بإعداد تشريع لعلاج هذه لمسألة. فيما كانت لجنة الشؤون الخارجية، عاكفة في عام 1994، على وضع خطة للفحص الدوري الدقيق لأنظمة التصدير. وقدأ عدت كانتويل مسودة التشريع إتش آر H.R. 3627، «تعديل قانون إدارة لتصدير لعام 1979»، وهو مشروع قانون يضيف قسماً جديداً إلى القوانين القديمة، التي لها آثار معينة على الصادرات من البرمجيات، بما في ذلك التشفير. وبموجب هذا التشريع، يتم نقل سلطة القرار، من وزارة الدفاع إلى وزارة التجارة، وتجعل البرمجيات التي تم تقليصها وتغليفها والبرمجيات العامة مستثناة من أنظمة التصدير. وهذا سوف يضع حداً للعبة وكالة الأمن القومي بضبط الشيفرة الأمريكية باستخدام قوانين التصدير.

بطبيعة الحال، لم يكن بوسع الإدارة، أن تسمح بتمرير هذا التشريع المقترح. وعندما كانت كانتويل تتأهب لتقديم مشروع القانون أعلمها مستشاروها بورود مكالمة هاتفية من نائب الرئيس. وكان قد سبق لها أن اشبكت لمرّة واحدة، مع آل جور أثناء مناقشة الموازنة، حينما أيدت كانتويل، رغم تحفظاتها الشديدة، الإدارة (وسوف يتهي بها الأمر أخيراً إلى خسارة حملة إعادة انتخابها جزئياً بسبب ذلك). فما الذي يريده هذه المرّة؟

قال: «أود أن توقي مشروع القانون هذا». وكثر الكلام الذي يتردد في جلسات الاطلاع، بشأن الأمن القومي وما إلى ذلك. تثبتت كانتويل بموقفها. وقالت: «إنني آسفة، يا حضرة نائب الرئيس، إنني أحترم رأيك، لكنني لن أبدل رأبي».

وبطريقة ما، كما نت تلك المحادثة، نقطة تحول لماريا كانتويل. فعملت على تمرير مشروع القانون إلى اللجنة الفرعية ثم واصلت الضغط ليفوز بالموافقة، على الرغم من أن الزملاء في اللجنة كانوا في ذلك الحين يحاولون حملها على التخلي عنه. ولم تكن قد غادرت القاعة بعد التصويت - بل لم تكن نهضت من كرسيها بعد - حين صعد إليها أحد النواب وقال لها بصراحة: «إذا لم توقي هذا، فإن الأمور سوف تصبح مزعجة جداً». وقالت ماريا كانتويل في نفسها: «لن أتوقف».

في 24 تشرين الثاني/ نوفمبر 1993، قدمت كانتويل مشروع القانون في قاعة المجلس. وكانت تعليقاتها فظة، إذ قالت: إن نظام ضبط صادرات الولايات المتحدة مفلس. وكان قد صمم ليكون أداة في الحرب الباردة، للمساعدة على محاربة أعداء لم يعودوا موجودين. ولا بد أنه لدى الوكالات الفيدرالية التي لا عد لها ولا حصر والمسؤولة عن ضبط تدفق الصادرات من بلادنا، شخصية جديدة تدرك حقائق يومنا هذا».

استمر الضغط، بالرغم من التعاضد، بين معظم الأعضاء في محاولاتهم لإقناعها. وثمة مثال على ذلك، حين صعد أحد زملائها الديموقراطيين إلى مكانها في قاعة اجتماعات المجلس وبدأ يوبخها بقسوة لتجاهلها مسائل الأمن القومي. فشعرت حينذاك بالرهبة لكنها كانت على قناعة أكثر من أي وقت مضى بأن عليها مواصلة التقدم. ومع جميع القوى المحتشدة لمساندة قوانين التصدير العجيبة هذه ورقاقة المقرض الخيفة، وجدت الأمر تجلياً لسلطة لا تحدّها حدود ضد المتهلك.

ومع ذلك، كانت تعلم أنها في المقدمة فيما يتعلق بهذه المسألة. وبرغم أنها كانت تؤدي خدمة جليلة، لقليلي الصبر الذين تمثلهم، فإن معظم ناخبيها في الدائرة الانتخابية الأولى بولاية واشنطن كانوا يفضلون أن يكون تركيزها على قضايا مثل الرعاية الصحية، إلا أنها كانت هنا، حبيسة اجتماعات مع مستشار الأمن القومي توني ليك. وبلغ مسا معها ذات يوم أن بيل جيتس سوف يزور المدينة. لذلك طلبت من شخص من مايكروسوفت ممن كانوا يعملون معها - ناثان مرفولد وبيل نيوكوم مستشار الشركة - إقناع رائدا لتكنولوجيا الأشهر في العالم بأن يمارس ضغطاً على زملائها من أجل القضية. وناشدتهما بالقول: إنني هنا في وضع حرج سياسياً. ودون دعاية إعلامية، جعلت بيل جيتس يخاطب لجنة الاستخبارات. وبدأت أدوات الأمن القومي تشرح للملياردير مدى أهمية قوانين التصدير، لكن مثال الاقتصاد الجديد كان قليل الصبر عند سماع المحاضرات. فأعلمهم أن ما بلغه منهم إن هو إلا تبرير سخيف. ولم يشعر أعضاء اللجنة بالاستياء، كانت متعة من نوع ما، أن يلقوا معاملة مزرية من أغنى رجل في العالم. ولا ريب بأن المرء لا يملك إلا أن يأخذه على محمل الجد، حينما يتحدث بشأن ما هو مفيد للفعاليات الاقتصادية.

وكانت لكانتويل مواقف مع البيت الأبيض أيضاً. فقد طلبت من القوم هناك ألا يحاربوا مشروع القانون الذي اقترحته، بل أن يدعوه يأخذ مجراه في الكونجرس. وكانت الاستجابة غير متوقعة، وجاءت قبل التصويت بيومين وكانت عبارة عن صفقة. وأراد جماعة جور معرفة موقفها: إذا ما بدلنا موقفنا، فهل تحسبن مشروع القانون؟ واقترحوا أنهم بدلاً من فرض رقابة المقرض على الناس، سوف يؤيدون مشروعاً مختلفاً يقوم على إيداع المفتاح طواعية. وربما يكون مبنياً على تطبيقات برمجية، أكثر مرونة من الموجودة حالياً؛ وكذلك عوضاً عن أن تكون تسهيلات الوديعة لدى الحكومة وحدها يمكن أن يكون بعضها في القطاع الخاص، الذي هو موضع ثقة أكبر، مثل المصارف أو شركات التأمين.

كان ذلك تراجعاً كبيراً، لكنه لا يزال في جوهره يتعلّق بمشروع الوديعة، وليس الحل النهائي الذي ترغب به كانتويل وناخبوها. ومن الناحية الأخرى، كانت حظوظ تمرير مشروع القانون الذي اقترحتته من غير اعتراض، تعادل حظوظ شحن مايكروسوفت نظام تشغيل دون أجهزة تنصّت. (حتى في ذلك الحين سيواجه رفضاً شبه محتم). عادت كانتويل إلى الأشخاص الذين كانوا يخوضون المعركة زمنياً طويلاً قبل أن تنتقل إلى واشنطن. وتشجع بروس هايمان من المجموعة الصناعيّة التي تدعى اتحاد صناعة البرمجيات، على القول أن الحكومة كانت بذلك تقدم إطاراً لتسوية. واحتفل نااثان مرفولد بلا تردد. وقال لاحقاً: «لقد وهنت أعصابهم». واتفق مستشارو كلينتون جميعاً، مع ذلك، على أنه قبل سحب المشروع، يتعين عليها الحصول على وعود مكتوبة بما تم الاتفاق عليه.

في عصر 20 تموز/ يوليو 1994، قبل التصويت، وصلت رسالة من آل جور وبعد الادعاء الفارغ المعتاد (لأنني أكتب [هذه الرسالة] لأعبر عن تقديري الصادق لما تبذلينه من جهود، لدفع النقاش على المستوى القومي إلى الأمام...») ثم دخل جور في صميم الموضوع.

إن الإدارة تتفهم ما يساور [أرباب] الصناعة من قلق، فيما يتصل برقاقة المقراض. وإننا نرحب بالفرصة للعمل مع الصناعة لتصميم نظام متعدّد الاستعمالات، وأقل تكلفة. وإن نظام وديعة مفتاح كهذا سوف يكون قابلاً للتطبيق في البرمجيات، والبرمجيات الثابتة، والعتاد، أو أي مركب من هذا القبيل، ولا يعتمد على خوارزمية محظورة، وسوف يكون طوعياً، وسيكون قابلاً للتصدير... كذلك فإننا ندرك أن نظام تشفير وديعة مفتاح جديد، يجب أن يجيز استخدام وكلاء لوديعة الصفحات من القطاع الخاص كواحد من الخيارات.

ومن الواضح، أن البيت الأبيض كان يعتبر تلك الحركة، مجرد وسيلة

لتهدئة عاصفة محتملة من الغضب. (وفي وقت لاحق من الصيف، قيل لمسؤول في وزارة الدفاع كان يطلب توضيحاً عن الآثار المترتبة على تحوّل لسياسة، بأن الرسالة إنما بقصد «استرضاء كاتويل الجمهورية وتجنب طرح الموضوع للنقاش العام»). لكن حينما وجدت محتويات رسالة جور طريقها إلى الصفحة الأولى من الواشنطن بوست في اليوم التالي (إحراج طفيف لكاتويل، التي لم تكن تود أن تظهر وكأنها تؤدي مشهداً لإثارة الإعجاب)، وقد كشفت جماعة جور من جديد بأن «بوسنة» الاتصالات [رقاقة المقراض] كانت شائكة كعهدهم بها دائماً. لقد قطع البيت الأبيض وعوده، دون أن يتم الاتفاق عليها مع وكالة الأمن القومي ومكتب التحقيقات الفيدرالي. (وكانت المرة الأولى التي سمع بها كلينت بروكس يوم نشرتها الواشنطن بوست). تلقت كاتويل اتصالاً هاتفياً من أحد رجال جور. وسألها هل لديك مانع إذا ما، ألغينا الرسالة؟

أجابت قائلة: «أتعلم كم ستبدو سخيلاً؟ وبعد، لقد كانت تلك رسالة جور وكلماته و وعدت بالأمتثال الحاد في الإعلام، لكن الأخبار كانت قد خرجت إلى العلن، ولم تكن لديها لسلطة لأن تدعه يلغي الاتفاقية. فظلت الصفقة قائمة. وهكذا أسقطت كاتويل مشروع القانون الذي اقترحت، على الرغم من أنه في السنوات القليلة التالية سيكون الأول في عدد من مبادرات شعبية متزايدة في الكونغرس لإصلاح قوانين التصدير. وفي الوقت ذاته، فإن رسالة جور، سواء عن قصد أم لا، كانت برنامج العمل الأساسي الذي ستعتمده الإدارة في التعامل مع رقاقة المقراض سيئة الحظ. خطوة إلى الوراء. رفض، خطوة أخرى إلى الوراء. عرقلوا اضطراب، بينما النقاش العظيم الصادق الذي تخيله كلينت بروكس بشأن سياسة تشفير قومية، لم يتقدم إلى الطليعة قط. وفي الوقت ذاته، فإن الخطة التي اعتبرها بروكس أساسية جداً، حلاً تشفيرياً كاملاً لحماية السرية مسيسة ستولنسياسة التوقيع الرقمي لشامل، لتقوية التجارة الإلكترونية ومنع التزوير الإلكتروني، ومدخل لتطبيق القانون، لم تلق الدعم الصريح.

أراد كلينت بروكس أن يخرج من الصراع . فبعد سنتين من التردد بين ما ريلاند والعاصمة، والدخول في المناقشات ذاتها مع الأشخاص أنفسهم، سأل المدير الجديد لوكالة الأمن القومي إن كان بإمكانه، القيام بأي شيء يفيد من مواهبه بكفاءة أكبر. ولقد قبل طليقلا شت التيرفانا.