

براءات ومفاتيح

كان الأمر كله لراي أوزي مسألة بسيطة لا تستدعي من الفكر كبير عناء ليحيط بها. فهو رجل يعمل في ابتكار منتج يتبادل فيه لنا س معلومات، يحرصون على حمايتها من التسرّب أو عبث العابثين. أما إدخال التشفير بين مكونات المنتج فما كان إلا وسيلة لتوفير هذه الحماية. وإذن فالمسألة عنده محض عمل وتجارة تفرضها البدهة أما وقد أخذت شركة لوتس الآن تعد لجعل الخوارزمية ر سا جزءاً أساسياً من البرنامج «نوتس»، فإن الرجل وجد نفسه غارقاً حتّى سطره في دغل من الممنوع والمحظور في شؤون تصديره، وكأنه أصبح بذلك شبه عدو للدولة. ولقد فزع حين اكتشف أن برنامجاً قصد به التجارة ويهدف لمساعدة لناس في أعمالهم يعتبر، في منطوق أنظمة التصدير، سلاحاً، لا كالمسدس، أو حتّى الخنجر، وإنما سلاحاً للتدمير الشامل.

ولقد كان بوسع أوزي أن يتجنّب هذه الورطة كلها فلا يقوم بتصدير منتج. غير أن الأمر، إن أخذنا به على المستوى العملي، كان مؤداها اقتصار البيع على أمريكا، وهذا مما يرفضه العقل، لأن ذلك يختصر العائدات المتوقعة إلى النصف على الأقل. إذ أن سوق البرمجيات، لأجهزة الكمبيوتر الشخصي كانت سوقاً عالمية، وخاصة حينما يتعلّق الأمر بالشركات الكبيرة التي كانت

المستهلك الأول لبرنامج «نوتس». ولكن مثل هذه السوق، لم تكن قد وجدت، بعد، عندما وضعت أنظمة التصدير. فلما أخذ أوزي ومحامو شركة لوتس يقومون بأبحاثهم وجدوا أن إجازات تصدير برامج الكريبتوجرافيا، لا تمنح على وجه العموم إلا عندما كان المصدر (وهو عادة شركة ذات صلات بالمؤسسة العسكرية) قادراً على تقديم كفالة حسن الصداقة والنية الطيبة لدى المستخدمين، وجدارتهم بالثقة. وقد عرفت هذه العملية بـ «إجازة المستخدم النهائي» End-User Certification. ولكن البرنامج «نوتس» كان سلعة لسوق شعبية فهو مجرد علبة، فيها شريط ملفوف أشبه بشريط المسجلة. أما المستخدمون فهم... مجرد أناس عاديين. ولقد أصاب الضيق محامي شركة لوتس حين عجزوا عن العثور على سابقة بإصدار رخصة تصدير، لبرنامج يتضمن شيفرة في تلك الظروف.

وكان على المرء، إن أراد الخوض في الأرض المليئة بالألغام السياسية، والفنية والحافلة بالأشباح، أي أرض تلك الأنظمة والقيود، الإستعانة بمحام يعرف خفايا واشنطن وخبير في كسح الألغام. وهكذا مضت لوتس، وكلفت أحد هؤلاء بمتابعة المشكلة وتمهيد الطريق. وكان هذا المحامي هو ديف ورمسر، ونصيحته الأولى: المضي مباشرة إلى مصدر كل الاعتراضات: أي وكالة الأمن القومي. حقاً أن القانون لم ينص على هذا الاتصال فاقناة المعينة لهذا الغرض هي وزارة الخارجية - إلا أن ورمسر كان يعلم أنه من العبث الذي لا طائل منه أن يتقدم المرء بطلب الإجازة ما لم يكن يعلم، بما يجول في عقول هؤلاء القابعين وراء السياج الثلاثي، بشأن المنتج وأية علة قد يجدونها فيه.

وهكذا مضى راي أوزي، في منتصف عام 1986، وبعيد شيوع خبر الصفقة مع شركة الآر إس إيه، إلى فورت ميد، بولاية ماريلند، لاستطلاع الموقف ومعرفتها سوف يواجهه. وكان برفقته يومذاك كل من ورمسر وألان إلدريج مهندس إيريس المسؤول عن مكونات الأمان في برنامج «نوتس»؛ وكان

أوزي في الثلاثين من عمره يومذاك، أي أصغر سناً من أن يكون بين الذين اكتسحتهم ثورة الستينات، ولكنه كبير السن بما يكفي لأن يكون دامو قف مشكك إزاء العسكريين. غير أنه كمهندس ومبتكر متفرق في العمل لم يكن ليُدري تماماً أي أمر صادفه الآن.

كان راي أوزي يجهل، أمر رحلة مماثلة لهذه قام بها من قبله والت تكمان من شركة آر إس إيه، وهو، شأنه شأن أوزي، غريب طارئ؛ نما يحمل مخططاً من شأنه توسيع مجال الشيفرة [الإلكترونية] فتجاوز النطاق الذي حدّته «القلعة» لنفسها. وكانت وكالة الأمن القومي قد وجدت نفسها، وهي الواثقة من أن شركة مثل أي بي إم لا يمكن تحدي طلب باسم الأمن القومي، أنها تجاوزت التحدي، إلا أنه بدا واضحاً في السنوات التي أعقبت الموافقة على معيار تشفير البيانات أن المشكلة ظلّت قائمة ولم تتلاش. ولما أخذ التشفير يزداد توغلاً في القطاع العام - ومعيار تشفير البيانات يصبح أشد شيوعاً داخل حدود الولايات المتحدة - أصبحت قوى معينة في وكالة الأمن القومي ترى الآن في الموافقة على معيار تشفير البيانات، بالرغم من التنازلات الكبيرة من جانب أي بي إم خطأ عظيماً. فمن كان يعلم أن الناس جميعاً بدءاً من مدرء الحلقة الوسطى حتّى الجندات سوف يستخدمون حواسب قادرة على تنفيذ عمليات تشفير بالغة التعقيد؟ من العيار الثقيل؟ ولقد اعتبر البعض من أركان الوكالة أن زيارة فريق شركة لوتس قد تكون أقوى إشارة حتّى الآن على أن كتابة الشيفرة قد بدأت بالانتشار بين عامة الناس، وكان معنى زيارة راي أوزي لهؤلاء المعنيين في وكالة الأمن القومي أن برابرة الشيفرة قد بلغوا الباب.

كانت الأجواء المحيطة بفورت ميد والسياح الثلاثي من حولها، ومخفر الحرس، ثم الممر الطويل بما علق على جدرانه من صور لجنرالات مجهولين، والغرفة التي يقودونك إليها وهي غرفة عادية لا تختلف عن أي غرفة أخرى، وما فيها من مفروشات تبدو وكأنها كانت هناك منذ عهد [السيناتور جوزيف]

مكارثي، تشير أشد الضيق في النفس. وهذا ما جعل أوزي يفكر بأن هؤلاء القوم على قدر عظيم من السلطة وبيدهم زمام الأمور، وهم عازمون على استخدام سلطاتهم.

بدأ الاجتماع بدخول جماعة من مسؤولي الوكالة، وأخذ أحدهم، وهو على ما يبدو المسؤول المكلف بالقضية، يتحدث الرجال الثلاثة. (كشف هذا الموظف - الذي ينفر أوزي من الإفصاح عن اسمه - بأنه ظل يتابع تطور «لوتس» مدة تزيد عن عشر سنوات). وتتابع الأسئلة: «ما هو هذا المنتج؟ متى يكون جاهزاً؟ أي نوع من الكريبتوجرافيا تأملون باستخدامها؟ ورد أوزي وجماعته بعرض أسلوبهم المركب في التشفير: استخدام الخوارزمية (ر سا) لتبادل المفتاح وميعار تشفير البيانات لعملية التشفير ذاتها.

لكن مجرد ذكر معيار تشفير البيانات كان مبعثاً لفقدان جماعة وكالة الأمن القومي صوابهم. فقال أحدهم: «ها إني أخبركم الآن بأنكم لن تتمكنوا من تصدير معيار تشفير البيانات، في أي ظرف من الظروف... إنكم لن تستطيعوا تصدير المعيار أبداً». بدا هذا قولاً غريباً. ألم تصادق وكالة الأمن القومي ذاتها على معيار تشفير البيانات؟ يمنع تصديرك يا حبيبي إلى أي كان يحمل في جيبه مثني دولار. وهنا أخذ موظف الوكالة، يشرح لمستمعيه وضع معيار تشفير البيانات. إنه ليس مجرد نظام للتشفير، وإنما هو في حقيقة قضية سياسية ملتهبة تشغل «القلعة»، وللهلضا مين وأبعاد يصعب على مهندس في القطاع الخاص استيعابها ولا حاجة له بذلك.

لم يكن أوزي يعلم حينئذ، أن وكالة الأمن القومي كانت تمر بفترة ندم مبعثه موافقتها على DES معيار تشفير البيانات. بل أن الوكالة كانت في واقع الحال تقوم على مشروع خاص بها أطلقوا عليه اسم برنامج «دعم أمن الاتصالات التجارية» Commercial COMSEC Endorsement Program الذي يؤمل منه القضاء على الشيفرة المستندة إلى لوسيفر، ويحل محله نظاماً للشيفرة

خاص به، ويطلق عليه اسم «مشروع الغالب» Project Overtake. وقدم السبب المبرر لذلك أن شيوع معيار تشفير البيانات «قد يحفز منظمة استخبارات معادية على شن هجوم واسع النطاق» يمكنها من تفكيك الشيفرة. وكان هذا التبرير في حد ذاته ضرباً من المفارقة لأن وكالة الأمن القومي ذاتها هي التي أجازت الحجم الأصغر لمفتاح الشيفرة فجعلتها بذلك عرضة لمثل هذا الهجوم. ولكن المشكلة الحقيقية لم تكن تكمن في كون معيار تشفير البيانات، ضعيفاً، وإنما في شدة إحكامه، فهو أشد إحكاماً مما ينبغي لنظام شيفرة يستخدمه جمهرة الناس. وها هو معيار تشفير البيانات يهدد بأن يزداد شيوعاً وبأكثر مما قدرت له الوكالة، وإذا ما استخدمت أنظمة للمفتاح العام على نطاق تجاري واسع، مثل البرنامج «نوتس» معيار تشفير البيانات، فإن المشكلة ستزداد سوءاً. وهكذا أصبحت فورت ميد تنظر إلى الشيفرة كعنصر خطير يتهدد مهمتها العالمية. فكان الحل أن تخرج وكالة الأمن القومي بشيفرتها الخاصة التي تسيطر عليها سيطرة تامة.

ومع ذلك فقد كان «مشروع الغالب» مبادرة محكوماً عليها بالفشل منذ البداية، لأن الزبائن الذين تسعى إليهم في القطاع الخاص لم يقبلوا عليه، لعدة أسباب منها أن التكنولوجيا المستخدمة باهظلتكاً ليف ومعقدة. وكان هذا النظام يتألف من أجهزة بحجم أشرطة الاستماع Audio cassette تركيب في الكومبيوتر، بسعر يبلغ 1000 دولار لكل علبة. والأدهى من ذلك، أنه لم يكن يسمح للمصارفو سواها من المؤسسات المالية التي سلت أن تساهم في هذا المشروع أن يكون لها أي قدر من السيطرة على النظام المستخدم. ثم أن الخوارزميات ذلها كانت محمية داخل علب مصممة، على نحو لا يسمح بالعبث بها. بل إن المفاتيح ذاتها كان توليدها وتوزيعها حكراً على وكالة الأمن القومي وحدها. وكيف يمكن للمرء أن يطمئن بأن وكالة الأمن القومي لن تحتفظ بنسخ عن المفاتيح؟ وقد جاء الجواب على لسان ممثل وكالة الأمن

القومي، إذ قال بلهجة متعالية، في مقابلة نادرة في صحيفة وول ستريت جورنال: «لدينا أمور أفضل تشغلنا». ومؤدى ذلك بعبارة أخرى: لتثقوا بنا. وقد تضمن المقال عرضاً لتكتيكات وكالة الأمن القومي في لتسويق تنحو فيها نهج الستالينية الجديدة. وها هو ذا أحد مدراء المصارف يعرض زيارة عمل من النوع المألوف للترويج لمشروع الغالب: «يقف رجل من رجال وكالة الأمن القومي ويشرع في إلقاء الأوامر: «عليكم يا شباب أن تفعلوا هذا». إنه توجيه. ولك أن تتخيل أي نجاح يمكن أن يلقى هكذا أسلوب». وكانت النتيجة أن المصارف أعرضت عن اعتماد النظام الذي تروج له الوكالة، مؤثرة الاستمرار بالعمل بمعيار تشفير البيانات.

ومع أن رأي أوزي كان يجهل كل هذا، إلا أنه أخذ يدرك أن تصدير الشيفرة مسألة شديدة الأهمية لهؤلاء ويأخذونها على محمل الجد. وأصبح واضحاً مع استمرار الاستجواب الودي في ظاهره أن جماعة وكالة الأمن القومي يفتقرون للمفردات اللازمة للتعامل مع منتج صمّم لسوق واسعة ذي مكوّن أمني قوي مثل اللوتس نوتس. ويصف أوزي حال هؤلاء الناس بأنهم «كانوا يتعاملون مع أناس يعرفون زبائنهم ويضمنون لهم إجازة المستخدم النهائي. أما نحن فكان علينا أن نبين لهم أن صناعتنا لا تسير على هذا النحو». ولما حاول أوزي أن يستر سل في الشرح بدأ محاميه يضرب ساقه تحت الطاولة بقدمه محدثاً إيّاه من أن وكالة الأمن القومي لا ترتاح لسماع مثل هذا الكلام. غير أن أوزي كان يرى في تلك اللحظة أنه من الأهمية أن يتولى الدفاع عن مكوّن الشيفرة في برنامج «نوتس»، على أساس أن من يستخدم المنتج إنما يجازف بكل تجارته ووسيلته للطمأنينة فهي الأمان الذي يكفله البرنامج وعدم افتراق الشيفرة. ولكن هذه الحجة لم يبد أنها راقية للأشباح.

أخذ أوزي يتساءل، وهو في طريق عودته إلى بوسطن، بعد ذلك الاجتماع الأول، إن كان ثمة ضير حقاً في الاقتصار في توزيع برنامج نوتس

داخل الولايات المتحدة، وتفاهي الدخول في هذه المعركة؟ بيد أنه وجد هذا النهج بمثابة انتحار مالي، إذ ليس بوسعك أن تتنافس مع الشركات المنتجة الأخرى إن تجاهلت السوق العالمية.

وهكذا طلب أوزي من المحامين ترتيب اجتماع آخر، في كمبردج هذه المرة. فهل أصبح موقف وكالة الأمن القومي أكثر ليناً؟ لقد جاءه الرد حين قال أحد ممثلي وكالة الأمن القومي لفريق شركة لوتس: «أقول لكم على سبيل توضيح موقفنا أننا على معرفة منذ عهد طويل، بأنكم قد ضمتتم برنامج اللوتس 1 - 2 - 3 برنامج شيفرة، وهذا يقع من وجهة نظرنا في نطاق سلطاتنا. ولو شئنا لكافؤ سعنا فرض حظر على تصدير برنامج اللوتس 1 - 2 - 3».

لقد كان برنامج اللوتس 1 - 2 - 3، الجدول الإلكتروني الذي يشكّل الجانب الأعظم مرعاتات الشركة. وكان هذا البرنامج أكثر البرامج شعبية في العالم وكانت نسبة عظيمه من مبيعاته، إنما تتم خارج الولايات المتحدة. فما هو «التشفير» الذي تشير إليه وكالة الأمن القومي؟ لقد كان برنامج الجدول الإلكتروني في لوتس يحتوي على إضافة كلمة سر بسيطة، تمنع تدخل كل من لا يعرفها في البرنامج. والآن، من المستبعد أن تجرؤ حكومة الولايات المتحدة فتفرض حظر شحن جميع البرمجيات التي تحتوي على كلمات سر إلى الخارج، وهو تصرف كفيل بأن يؤدي إلى انهيار صناعة برمجيات الحواسب الشخصية برمتها. ومع ذلك فقد فعل التهديد فعله. فعندما نظر أوزي إلى محاميه من طرف عينه رأى على وجهه ملامح الذعر واضحة جلية.

ولقبها ت واضحاً لراي أوزي، أثناء ذلك الاجتماع والاجتماعات الكثيرة التي عقدت خلال السنوات الثلاث اللاحقة، أن كل موافقة يحصل عليها لتصدير البرنامج ستكون رهناً بإرادة الحكومة، بالغاً ما بلغت أهمية النوتس لشركته أو حتى للاقتصاد الأمريكي. ولكئنه كان قد ارتاح إذ علم أنه ما من

شخصٍ كلفته وكالة الأمن القومي، بتمثيلها في التعامل بفرض نوع الشيفرة التي تُباع «داخل» حدود الولايات المتحدة. (وجدير بالذكر أن فرض شرط كهذا مخالف لقانون أمن الكمبيوتر. ولكن من يدري ما هي الحدود التي يقف عندها هؤلاء القوم؟). وكان المفاوضات عن جانب الحكومة يردون على أوزي كلما ألمح إلى أن القيود المفروضة بموجب أنظمة لتصد ير قد تقسر شركته على توزيع نسختين من برنامج نوتس، واحدة ذات تشفير عالي المستوى للتداول الداخلي ونسخة أخرى تمثللما صفت الموضوعة للصادرات، بلا مبالاة قائلين: «ذلك خيارك وشأنك». كذلك كان يراود أوزي خاطر بأن وكالة الأمن القومي ربما كانت تحث لوتس على وضع هيكل مفتاح سري يفيد منه الأشباح في تفكيك الرسائل التي يقوم نوتس بتشفيرها بسرعة. ولقد حاول ذات مرة جس نبض القوم لمعرفة إن كانت هذه غايتهم. فسأل جلاوذته: «ماذا تريدون بحق الجحيم؟» هل تنتظرون مني أن أقدم لكم باباً سرياً لتدخلوا منه؟» فجاء الرد فوراً: «لا، إننا لا نريد لك أن تجازف بأمن المنتج». فعاد أوزي يسأل: «إذن فماذا تبغون» فيبقى سؤاله معلقاً بلا جواب. ويظل هذا الوضع على حاله.

وفي النهاية حصل أوزي وفريقه، حوالى منتصف 1987، على تنازل من وكالة الأمن القومي وأساسه أن الحكومة تجري تقييماً لقوة لشيفرة، وتسمح بتصدير برنامج نوتس. ويتقرر طول المفتاح في مفاوضات بين الطرفين، شرط أن تتخلى لوتس عن معيار تشفير البيانات وتستخدم شيفرة بديلة. فعمدت لوتس إلى تكليف رون رايفست فوراً ليأتي بخوارزمية جديدة. لقد طلع رايفست بعد بضعة أسابيع من العمل المضني بشيفرته الخاصة التي تحمل الرمز RC-2، اختصاراً لـ «شيفرة رايفست رقم 2». (وكانت الأولى قد نسقت). وكان النظام الذي خرج به رايفست شبيهاً بمعيار تشفير البيانات، بمعنى أنه شيفرة متكاملة تقوم على بدائل معقدة، إلا أن مفتاحه، على العكس من معيار تشفير البيانات،

يقبل الإطالة والاختصار. وقد قامت شركة لوتس بدفع كافة تكاليف أعمال التطوير، إنما سمحت لشركة الآل س إيه بالاحتفاظ بحقوق الملكية الفكرية. ثم سلم رايفست الشيفرة، في 1987، إلى وكالة الأمن القومي؛ ولم يمض إلا بعض الوقت حتى بلغه أن عباقرة الشيفرة وراء السياج الثلاثي نالوا تقريعاً من المسؤولين لعجزهم عن معالجتها.

وقد سأل أوزي رايفست: «كيف لك أن تعلم أن هؤلاء الجماعة لن يعبثوا بالشيفرة لإضعافها؟».

وكان رد رايفست أن في تعليقات للحكومة وجهة نظر منطقية، وذلـك فهو مطمئن لما سيقومون به من تغييرات. وقد استغرق الأمر شهراً أو يزيد قليلاً ثم ستؤنفت المفاوضات من جديد، ولكن ذلك لا يعني أن الطرفين كانا يقتربان من الاتفاق. ويصف أوزي الوضع بقوله: كان محتوى تلك الاجتماعات يزداد فقراً وشحاً، وفي اعتقادي أن الجماعة كانوا يبددون الوقت تأخيراً للقرار. كان الانطباع لديه: أن ثمة صراعاً يدور داخل وكالة الأمن القومي ذاتها، حول الأسلوب الذي ينبغي اتباعه في المفاوضات. فلم يكن الافتقار لإجازة تصدير يمثل أزمة ذات شأن لشركة لوتس خلال العامين 1987 و1988، لأن برنامج نوتس كان أحد المشاريع الطموحة لإنتاج البرمجيات، وقد تأخر إنتاجها عدة سنوات. وإذن لم يكن موضوع التشفير هو ما يعرقل صناعة المنتج. ولكن في بداية عام 1989 بدت الأمور تعد بقرب إنجاز المنتج وتصنيعه. فبات حل مشكلة التصدير مسألة ذات أهمية.

كان الأمر الوحيد الذي تستند إليه لوتس، وتفيد منه هو ما تمتع به من دأب ومثابرة. والحقيقة، أن أوزي لم يكن لديه خيار آخر سوى أن يظل على دأبه ومثابرته. فكان كلما أشار إلى احتمال طرح المنتج في أسواق الولايات المتحدة وحدها وجد أن المختصين بالتسويق يصرون على أن هذا الحل غير ذي جدوى من الناحية المالية. وهكذا تابع الرجل لضغط، وكان لا يتقطع عن

طلب مزيد من الاجتماعات مع وكالة الأمن القومي، وعمل جهده على تقديم كل ما تطلب من معلومات. وكان ما يحمله على هذا هو قطع طريق الإعتراض، حال نيله إجازة التصدير، بحجة كتمان معلومات تتصل بالنظام وأسلوب عمله. فلو وقعت على تقصير منه لوجدت ذريعة لمنع شحن البرنامج. ولذلك حرص أوزي، على أن تلبى لوتس حتى أدق طلبات وزارة الدفاع مهما تكن عارضة.

ومع أن أوزي كان لطر فالمتو سل في هذه العلاقة، إلا أنه كان لديه بعض الثقل في الأمر. فقال ذات مرة للقائمين على شؤون التصدير: «أتراكم تقولون: أن عليّ الذهاب إلى من يمثلني في لكونغرس، لأخبره بأنكم تمنعونني من تصدير إنتاجي إلى الأسواق الخارجية؟ هل تراكم تدعونني لإثارة ضجة لن تهدأ بسبب هذا الموضوع؟». حقاً أن لوتس قد لا تكون إحدى الشركات العملاقة من ذوات رؤوس الأموال، التي تُعدّ بالبلايين من الدولارات، إلا أنها كانت مع ذلك، أكبر شركات صناعة البرمجيات في ذلك الوقت، ولم يكن من المناسب قيام بعض الأشباح الذين لا ملامح لهم، بإغلاق الباب في وجه محبوبة لصحافة الاقتصادية.

وفجأة ودون مقدمات ذاب الجليد في منتصف عام 1989. ويعتقد أوزي عن اقتناع بأن الصراع داخل وكالة الأمن القومي انتهى أخيراً بتسوية، «بين جماعة تناصرنا وأخرى معارضة لنا»، حسب قول أوزي: «في البداية كانوا يلتقون بنا، لأن ذلك من طبيعة عملهم، ثم أنهم كانوا يريدون معرفة توجهاتنا، نحن الذين نعمل في صناعة الكمبيوترات الشخصية الطارئة. وأعتقد أنه دارت معارك داخلية طاحنة بين الطرفين، بعضهم يحبذ شيئاً من الشيفرة في السوق للتخلص منا، وبعضهم لا يريد طرح سابقة، بل يحرص على ألا يخرج إلى التداول شيء من هذا». والظاهر أن النصر كان للفريق الأول. وعندئذ طرح

عرض، شفاهة طبعاً، فالعرض المكتوب أشبه بالوعد الملزم، ومثل هذا المخلوق غير موجود في غابة سلطة التحكم بالتصدير.

هاكم العرض: يجوز لشركة لوتس، أن تصدر إلى الأسواق الخارجية البرنامج تس مع عدة التشفير من الخوارزمية آر إس إيه وآر سي 2، بالإضافة إلى مفتاح بحجم 32 بت [خانة ثنائية]. وقد اعتقدت جماعة وكالة الأمن القومي أن في هذا العرض تنازلاً كبيراً من جانبهم. فعملهم هو تفكيك الرموز. ولذلك كان عليهم أن ينظروا في عواقب عملهم، خاصة إذا ما أطل عليهم الرئيس، وطلب هو أو مجلس الأمن القومي حل رموز رسالة مشفرة ببرنامج كانوا قد أجازوا تصديره. والحق أنا لحدس حملهم في البداية على إجازة مفتاح لا يزيد عن 24 بت. ولكن بعد المراجعة ودراسة الأمر مع كبارا لمسؤولين عن وضع سياسة وكالة الأمن القومي، كما قال أحد ممثلي الحكومة، وجدوا أنفسهم مستعدين للمضي حتى «الميل الأخير» وإجازة ما كانت الوكالة تعتبره مفتاحاً ضخماً بصورة غير مألوفة يتألف من 32 بت.

ضخم بشكل غير مألوف؟ لقد شعر فريق اللوتس حينذاك بالارتياح. وكان معنى ذلك أن المفاتيح التي يختارها المرء لتشفير البيانات وكذلك لفك الشيفرة كانت محدودة بمجال لا يزيد عن أربعة بلايين مفتاح إقليلاً. فإن كنت لا تريد محاولة تفكيكها يدوياً فإن هذا الأمر ليس بالشيء الذي يذكر في عصر الكمبيوتر لجسارة. فمثل هذه المسألة إن اعترضت أولئك الذين يقاتلون السليكون في قبو فورت ميد [وكالة الأمن القومي] وطلب إليهم العثور على مفتاح للشيفرة بين أربعة بلايين لأخذهم الملل وراحوا يتشاءمون لسهولتها، وقد أقر جماعة وكالة الأمن القومي في الاجتماع بأن الكمبيوتر العملاقة المتوفرة لديهم قادرة فعلاً على تحطيم مثل هذه المفاتيح في غضون يومين (وهذا تقدير بدا متواضعاً قليلاً). غير أن لصوص البيانات المحتملين، ليسوا بحاجة لكمبيوترات عملاقة فعلاً، لتفكيك شيفرة مركبة بمفتاح من 32 بت. ذلك أنهم

إن كانوا على قدر كافٍ من التصميم ولديهم ذخيرة مناسبة من الدولارات وفسحة من الوقت يبدؤونها بلا حساب فإن بوسعهم أن يتصدوا بما لديهم من قوة حسابية للمشكلة والثور على المفتاح. وتذهب تقديرات شركة الآر إس إيه إلى أنه من الممكن إنجاز هذه المهمة في غضون 60 يوماً. وقد أصرّ المسؤولون في الحكومة على أن مفتاحاً كافياً بهذا الحجم، وفترة طويلة كهذه، يوفّران عنصر الأمان اللازم وسألوا: «من تراه يتجشم العناء لتفكيك رسالة، أو عدة رسائل تجارية ويبدل لكل واحدة 60 يوماً؟».

ولقد بدا أن هذه النظرة تهمل المبدأ الموجه في التكنولوجيا المتقدمة والمعروف بقانون مور القائل: أن قوة الكومبيوتر الشخصية تتضاعف كل ثمانية عشر شهراً أو نحو ذلك. وهذا يعني أن مدة الستين يوماً سرعان ما تتقلص إلى فترة شهر. وهكذا سوف لن يستغرق تفكيك مفتاح من 32 بت، في عام 1995، إلا أقل من أسبوع. بيد أن هذا كله كان بعيداً عن النقطة الجوهرية. فلئن كان حقاً أن قضاء أيام أو أسابيع في تفكيك رسائل موجهة، وفق برنامج اللوتس نوتس، وهي في معظمها بريئة نسبياً يعتبر تبديداً للوقت، إلا أن بعض المعلومات التي تبثها هذه الشركات الضخمة ذات الرساميل التي تبلغ مئات الملايين أو البلايين من الدولارات هو ذو قيمة بلا ريب. فكيف تستطيع لوتس أن تطمئن هذه الشركات إلى أن المعلومات بأمان، إذا ما اقتصر المفتاح على 32 بت؟ إنها لن تستطيع الزعم باستحالة تفكيك الشيفرة، بل ولا تستطيع حتى القول أن ذلك ضرب من الصعوبة. فمن حيث الأساس إن الوقوع على رسالة سرّية هو أمر أكثر من مزعج.

ومع ذلك فليس ثمة سبب قانوني يحول دون إنتاج لوتس لنسختين من المُنتج: نسخة للتصدير بـ 32 بت ونسخة أخرى أشد منعة وأكثر أماناً للاستخدام داخل الولايات المتحدة. وهذه النسخة الأخيرة تأخذ بالطول الذي تؤثره لوتس للمفتاح وهو 64 بت، وهذا أشد صعوبة في التفكيك بعدة أضعاف

من النسخة المعدّة للتصدير. (لنتذكّر أن كل بت يضاعف حجم حيزاً لمفتاح. فالمفتاح الذي تكلف معرفته ضعف الجهد المبذول في معرفة نسخة الـ 32 بت لن يكون طوله 64 بت وإنما 33 بت فقط. وهكذا كانت النسخة المحلية، إذن، أشبه برفع صعوبة النسخة المصدّرة 32 ضعفاً، مع تغيير الإطار الزمني لتفكيك المفتاح من أيام إلى حقبة ومحصلة القول أن المرء ليس بحاجة لمخيلة عظيمة ليستخدم طريقة القوة الغاشمة ليفكك مفتاحاً من 32 بت. ولكن إذا أخذ المرء بقدرات الكومبيوتر سنة 1989 فإنّ سعه القول دون تعسف، أن هجوماً كهذا على مفتاح من 64 بت هو أقرب إلى المستحيل).

كانت مثالب إنتاج مفتاح حين بقدرات مختلفة أمراً تنوّع بحمله الجبال؛ وما لتكاليف اللوجستية - رزمتان ومجموعتان من الأقراص، وجدولان بأسماء ومواصفات المنتجين - إلاّ البداية. وكان على أوزي وفريقه أن يتفقدوا النسختين ويتأكدوا من تناسقهما في العمل. ولأن برنامج النوتس كان موجهاً لقاعدة من الزبائن تشمل في ما تشمل الشركات المتعددة الجنسية مثل شركة جنرال موتورز كان لا بد من كتابة لبرمجيات على نحو يستطيع معه المستخدمون في هذه الشركات، ومنهم من يقيم في الولايات المتحدة ومنهم من يعمل في بلدان أجنبية، من التخاطب مطمئنين إلى أن مخاطباتهم تظل مأمونة من تطفل المتطفلين. وإذن فقد كان على لوتس أن تحرص على أن يعمل المنتج، على نحو يطمئن الناس، إلى أن الرسالة الإلكترونية ستبلغ مقصدها سواء كان بعض المستقبلين في إسبانيا أم في كندا. وكان على كل من يستخدم برنامج نوتس أن يحمل بالضرورة مجموعتين من المفاتيح - زوج من المفاتيح الدولية وزوج آخر من المفاتيح للدخل - (وإن لم يكن هذا ظاهراً للمستخدم). وكان تنفيذ ذلك كابوساً لمن يقوم بالبرمجة، لما فيه من جهد وعناء. ولكن ذلك أمر فرضته الرغبة في الإتقان، فلم يكن أصحاب لوتس يقبلون «بالمجازفة» بتقديم سوية متدنية من العمل، في هذا البلد، على حد تعبير أوزي، وهكذا مضت الشركة وقامت بتنفيذ البرنامج.

كانت المشكلة الوحيدة التي لم يكن هناك من سبيل لتجاوزها هي أن القيد الذي فرضته الحكومة على المُنتج الموجه للتصدير جعلت هذا المُنتج أضعف كثيراً من ابن عمه الأمريكي. إن لك أن تنظر إلى هذا الأمر باعتباره مثلباً، عيباً، إنما كعيب ملازم للمُنتج. فهل يرفضه الزبائن في الخارج لذلك السبب.

في البداية لم يعرض الزبائن هؤلاء عن المُنتج بسبب من أن فكرة شراء مُنتج ببرنامج تشفير هو من مكوناته، كانت من الجودة ما جعل الزبائن لا يبدون اهتماماً بمستويات الأمان. ويقول أوزي في هذا: «كنا نحاول بيع مُنتج ذي استخدامك لم يكن [زبائننا] يدرون بها وهي جزء منه. وكان [هذا المُنتج] يتطلب بطاقة شبكة لم يكونوا يملكونها وأداة توليف مصورة يفتقدونها. وبعد أن تمكنا من إقناعهم بالتزود بهنّ للمكونات فحسب سألوا: «هل هذا مأمون؟» وكان جوابنا: «نعم، إنما مأمون؛ ولكن ليس بالقدر الذي عليه النسخة الأمريكية؛ إلا أنه مأمون في مطلق الأحوال». ثم يسألون: «هل يمكن لأحد أن يتدخل أثناء التخاطب؟» ويكون ردنا: «لعلكم تستطيعون ذلك، إذا جمعتم ثلاثين أو أربعين من أجهزة الكمبيوتر الشخصي. ولكن يلزمكم لذلك بهجيات خاصة وسواها». وكان تعريف الزبائن بأننا نحاول حماية معارفهم وبياناتهم عملية تعليم وتربية. ولم يمض إلا بضعة سنوات حتى أخذت الأسئلة ترد إلينا عن السبب الذي يجعل النسخة العالمية دون المحلية قوة. وإهمالنا تضمين تلك لنسخة معيار تشفير البيانات».

كانت لوتس تأمل أن تخفف الحكومة القيود التي وضعتها، وتسمح بمفاتيح أضخم، مع مرور الوقت، وذلك حين ينتبه الزبائن في الأسواق الخارجية إلى ضعف النسخة لديهم من حيث نوعية الحماية، بالمقارنة مع النسخة الأمريكية. فلقد كانت المفاتيح ذات الاثني والثلاثين بت مجرد حل وسط، أراد به أوزي دفع المُنتج إلى الخارج: «لقد رأينا أننا متى بدأنا طرح

(البرنامج) في الأسواق وبات لدينا زبائن ذوي شأن، غدونا في وضع يسمح لنا بطلب التحول إلى مفاتيح من 48 بت [في نسخة التصدير]. ذلك ما كنا نسعى إلى تحقيقه (وتلك كانت خطتنا لبلوغ هذا الهدف).

ولكن بدا في تلك الأثناء، أن الحكومة تدفع باتجاه مضاد. فقد اعتقدت وكالة الأمن القومي أن النسخة المعدة للتصدير ظلت أشد متانة مما ينبغي، بالرغم من ضعف حجم المفتاح، بسبب عناصر معينة في التصميم، وهي تتصل بإمكانية إعادة تشفير معلومات هي في الأصل مشفرة، وقد حسب أوزي أن من شأن هذه النقطة أن تجعل تفكيك الرسالة في أسوأ الأحوال، أشد صعوبة بعض الشيء. واقترحت الحكومة، دون أن تبدي أسباباً لطلبها، إجراء تعديلات في التصميم بشكل يحقق لها الرضى. وكان أبعد تقدير ذهب إليه أوزي هو أن القضية ربما كانت تتصل على الأرجح بطريقة محللي الشيفرة في وكالة الأمن القومي في حل الرموز. ولكن حسم القضية استغرق، بعد، عدة شهور أخرى من المفاوضات، وانتهت بإعادة تصميم المنتج بشكل ملحوظ وجعل البرنامج أشد بظاً من سابقه في بعض النواحي.

ولم يسع أوزي إلا أن يتساءل: ما الجدوى من كل هذا؟ وهل تصدير برنامج اللوتس نوتس بمفتاح من 32 بت، قد حسن من وضع الأمن القومي فعلاً؟

كان الصراع مع لوتس حول البرمجيات المصدرة مجرد علامة وحسب وإن على وكالة الأمن القومي أن تنتبه وتواجه التحدي الذي تمثله ثورة التشفير، بعد سنوات من الهمود. فبعد نوبة الذعر الخفيفة التي حدثت في أعقاب الانطلاقات الأولى في أواخر السبعينات زين الفكر للمسؤولين في «القلعة» أن زمام الأمور ما زال بأيديهم وتحت سيطرتهم. ومع أن التسوية التي حققها بوبي راي إنمان - وبموجبها يقدم علماء الشيفرة أعمالهم لتنظر فيها وكالة الأمن القومي - لم تكن لتخلو من الثغرات فإن نسبة عالية تستدعي الاهتمام من علماء الشيفرة البارزين الذين يعملون متقلين عن المؤسسات الرسمية كانوا يقدمون

أعمالهم طواعية أسوة بسواهم لتطلع عليها الوكالة. ولما كان ذلك قد تمّ بخيارهم الشخصي فإنه بوسعهم تبرير قرارهم بالامتثال لمبادئ الحرية الأكاديمية. فضلاً عن ذلك لم يكن لدى هؤلاء الأكاديميين رغبة بالإخلاق بالأمّن القومي. ثم أن في مخاطبة الأشباح متعة، على نحو ما. فهذا الحوار كان ينطوي على إثارة معينة، ناهيك عن الإقرار الضمني بجدية العمل الذي ينهض به المرء. وكان رجال وكالة الأمن القومي لا يقدمون أية اقتراحات في الغالبية العظمى، وإذا طلبوا أمرّ فهو تعديل بسيط، وقد جرت القاعدة على أن يكون ذلك حين يقع الباحث على موضوع ذي صلة بالأساليب التي تنهجها وكالة الأمن القومي في شيفراتها أو في تحليل الشيفرة.

وبعد، فلقد ظهر أن وكالة الأمن القومي قد تدّخلت، على الأقل مرة واحدة، لصالح أحد الباحثين. ولم يكن هذا الباحث سوى آدي شامير. فلقد كان شامير في السنوات التي تلت مغادرته لمعهد ماساتشوسيتس خصب الإنتاج على نحو استثنائي. فقد خرج وزملاء له إنطلاقاً من أفكار المفتاح العام بأفكار أخرى جديدة تتصل بالشفير، ومنها ما كان مثيراً للعجب. وكان من بين تلك الأفكار فكرة اشترك في تطويرها مع أدليمان ورايفست وتقدم طريقة للعب «بوكر ذهني»... وهي كعبة البوكر العادي، سوى أنّها تنفذ بدون أوراق اللعب بعكس ما هو مألوف في العادي». وكان من المبتكرات الأهم التي خرج بها شامير برنامج «الشراكة الخفية». فلم يكن قد مضى إلاّ سنتان على مشاركته في اختراع خوارزمية الآر إس إيه، حين شغله ما أسماه مشكلة تبحث عن حل، كيف تشترك مع عدة أطراف في مفتاح واحد، خاصة إذا كان هؤلاء يتبادلون الشك والريبة؟ والحل الكلاسيكي في حالة كهذه هو معادل إلكتروني لما يحدث في مستودع الصواريخ النووية: إذ يقتضي إطلاق الصاروخ تحريك عدة مفاتيح معاً وفي آن واحد، وهذا يتطلب وجود أكثر من شخص واحد لتنفيذ العملية. فهل تستطيع تكرار هذه العمليّة في العالم الآلي؟ ولقد تبين أن ذلك ممكن، ولما

شرح شامير بإعمال فكره، خرج بفكرة المشاركة الخفية، وهي وسيلة لتعميم مفتاح للشفيرة بين عدة أشخاص. فإذا استطاع عدو الحصول على أي جزء من حصة شخص من هؤلاء الأشخاص من المفتاح (ويُعرف بـ «الظل») فلن يكون لذلك أية فائدة في محاولة معرفة المفتاح. أما تنفيذ الفكرة فكان البداية. وكان واضحاً أن النهج الذي ينبغي أن يسلكه المرء يتطلب تعاون كافة الشركاء حتى يتم تصميم المفتاح. ولقد توقف شامير عندئذ وراح يعمل الفكر قليلاً... . وتساءل ماذا لو أن أحد هؤلاء اختفى أو مات أو اختطف؟ فقاده هذا التفكير إلى فكرة بناء القدرة على التحوّل بحيث إذا أعطيت مجموعة جزئية من المفاتيح مقرّرة سلفاً يكون بوسعك معرفة السر. وقد باتت هذه الطريقة تُعرف بـ «مخطّط البداية» ولها استخدامات شتى، لا تعد ولا تحصى. فيمكن توزيع سرّ مهني مثل تركيبة مياه غازية بين عشرة أشخاص، ثم لك أن تضع مسبقاً ما تشاء من التركيبات المعقّدة لاستعادة المفتاح. فإذا اجتمع مثلاً الأشخاص الستة الذين لا يطمئن إليهم من بين من يحملون ظلال المفاتيح فقد لا يتمكّنون من بناء المفتاح. غير أن الشخص الذي يتمتع بأعظم الثقة قد يتمكّن من بناء المفتاح مع شخصين آخرين في هذا المجمع.

وفي عام 1986 طلع شامير مع زميلين آخرين من زملائه في معهد وايزمن، بأسلوب مبتكر وواعد يُعرف بـ «نظام إثبات المعرفة الصفري». وهذا يتيح لأليس، باستخدام الدالة الحسائية وحيدة الاتجاه، [أليس هي الشخصية المفترضة. هـ. م] إثبات معرفتها رقماً معيناً (يخص عادة وثيقة تُعرف بها، مثل بطاقة الضمان الاجتماعي أو البطاقة المصرفية)، دون كشف ذلك الرقم للسائل. وقد قال شامير فيما بعد أنه يستطيع بهذا الأسلوب «دخول مخزن تملكه المافيا مليون مرة متتالية، ويظلون غير قادرين مع ذلك على تقمص شخصيتي [واستخدام هذه المعلومات في شراء البضائع وسوى ذلك من النشاطات]». ولقد أدرك شامير ورفاقه المبتكرون قيمة هذا المخطّط في عقد

لصفقات التجارية بالوسائط لإلكترونية فتقدموا بطلب منحهم براءة الاختراع عن هذا الابتكار. غير أن مكتب حقوق الملكية الفكرية أفاد هؤلاء الباحثين، في أوائل 1987، أن اختراعهم هذا الآن بأمر من الجيش الأمريكي يُعتبر سراً من أسرار الدولة، ويعتبر تداول المعلومات عنه يلحق ضرراً بالأمن القومي». ولم يكن الأمر ليقصر على منع العلماء الإسرائيليين من مناقشة الموضوع وحسب وإنما وجه إليهم الطلب بتحذير أي شخص سبق له الاطلاع على البحث لأن اطلاع شخص آخر على الفكرة قد يؤدي إلى معاقبته بالسجن عامين. ولكن هذا التوجيه بدا صعب التحقق إن لم يكن مستحيلاً، نظراً لأن أصحاب البحث، قد قدموا الموضوع إلى عدد من الجامعات فضلاً عن عرضه أمام مؤتمر كريبتو Crypto' 86 86، كما بعثوا بنسخة منه إلى جمعية الآلات الحاسبة لنشره في أيار/ مايو القادم. وبعد، كيف يمكن للحكومة الأمريكية أن توجه المؤلفين، وهم ليسوا من الأمريكيين، وتملي عليهم ما يمكن لهم الحديث فيه أو لا يمكن؟

إن وكالة الأمن القومي لم يكن لها ضلع في ذلك الأمر بالتزام السريّة، ولكنه سرعان ما بلغها من علماء أمريكيين، ومن صحيفة ذي نيويورك تايمز التي جاء من يبلغها بالموضوع المختلف عليه. وما أن مضى يومان حتى طوي الأمر بهدوء. ولكن شامير لم يعلم بإلغاء القرار إلا بعد أسابيع، وبات مقتنعاً بتدخل وكالة الأمن القومي لصالحه. والسبب؟ تذهب سوزان لاندوا الباحثة في السياسة المتعلقة بالشيفرة، بعد حين، أن سبب تدخل الوكالة هو رغبتها في استمرار مشروعها القديم الهادف إلى استمرار الباحثين في تقديم بحوثهم إليها للاطلاع. فإذا سادا لاعتقاد لدى الباحثين بأن طرح فكرة جيدة في مجال التشفير يؤدي إلى فرض حظر على تداولها فجأة جنح الباحثون إلى الامتناع عن تقديم بحوثهم إليها وانقطع تدفقها على الوكالة. وكما كتبت لاندوا: «إنه من الأيسر معرفة أثر المنافسة لو قدموا لك أبحاثهم».

ومع ذلك فإنه بات جلياً، مع اقتراب عقد الثمانينات من نهايته، أن نهج العرض الطوعي قد ستنفذ أغراضه. ثم جاءت نقطة الانعطاف، وهذا مما له مغزاه، مع بحث ليرالف ميركل. وكان ميركل قد انتقل للعمل مع شركة زيروكس Xerox Corporation، في مركز البحوث الشهير التابع لها في بالوا ألتو PARC وكانت دراسته الأساسية - بل قل هواه لشاغل - تكنولوجيا الجزيئات الصغيرة Nanotechnology، وهو علم حديث يعتمد على آلات بحجم الذرة. ولكن الرجل ظل يتابع التطورات في عالم التشفير. وفي عام 1989 وضع ميركل بحثاً عرض فيه سلسلة من الخوارزميات التي من شأنها تسريع لحسابات المشفرة واختصار سعر التشفير. وكان هذا البحث في حد ذاته تهديداً لمهمة وكالة الأمن القومي. غير أن بحث ميركل هذا كان مدعاة لقلق الوكالة بشكل خاص لتضمنه مناقشة لتكنولوجيا تصميم صندوق الاستبدال. وكان هذا الموضوع مسألة حساسة في دوائر «لقلعة»، منذ أن كانت قضية مشروع لوسيفر.

وكان أن أرسلت شركة زيروكس البحث، إلى وكالة الأمن القومي للاطلاع. (وكانت تراود الشركة آمال بالحصول على إجازة تصدير لمُتَشِّج يقوم على بحث ميركل هذا). وكالمعهود تقامت الوكالة بإحالة البحث إلى الخبراء داخل لسياج الثلاثي وخارجه. ولكن المحصلة لم تكن هذه المرة تصويماً مفيداً أو طلباً لبقاً بتعديل لغة البحث. فكان مطلب الوكالة هنا منع تداول البحث، بحجة أن مشروع ميركل ينطوي على تهديد للأمن القومي، دون أن تبدي مبرراً لهذا الاعتقاد.

ولقد وافقت زيروكس - الشركة التي تتمتع بعقود ضخمة لتعهدات حكومية - على طلب الوكالة. والمألوف في مثل هذه الحالات أن ينتهي الأمر عند هذا الحد. أما في هذه الحالة فيبدو أن أحد المكلفين بقراءة البحث من خارج الوكالة أزعجه الحظر الذي فرضته، وبلغ من الإزعاج ما حمله على تسريب البحث إلى متابع حر، وهاو للكومبيوتر وهو مليونير يدعى: جون جيلمور.

وكان لدى جيلمور سلاح لم يكن متوفراً قبل عقد من الزمن، عند بدء عملية الاطلاع المسبق على البحوث: الإنترنت. وكان من أكثر جماعات المناقشة شعبية من مستخدمي الشبكة (يوسنت Usenet) على شبكة وب العالمية واحد يدعى Sci. Crypt، وكان هذا أشبه بناد مفتوح طوال الليل وأشبه بولائم الكريبتو التي تُقام سنوياً في سانتا برابرة، وتقدم تياراً متصلاً من الأفكار الجديدة ونقداً لأفكار قديمة وأخباراً من عالم الشيفرة والرموز. فقام جيلمور بتعميم بحث ميركل على أعضاء الحلقة، وإذا به يبلغ في لحظة واحدة القراء عبر 8000 كومبيوتر من مختلف أرجاء العالم. إن عالم الآلة، جعل نظام الاطلاع المسبق على البحوث الذي تعتمده وكالة الأمن القومي أمراً غير ذي جدوى.

وقامت الوكالة عندئذ، بطي طلبها بعدم نشر البحث.

وحتى البيروقراطيون في القلعة أخذوا في ذلك الوقت يعون واقعاً جديداً بدأ يتشكل، وخلاصة الأمر أن التحديات التي تواجهها لم تكن تصدر عن بحوث أكاديمية، وإنما مصدرها السوق. وأفضل مثال على ذلك شركة برمجيات المفتاح العنلي التي كانت تلفظ أنفاسها ذات يوم، ثم إذا بها تبعث من جديد على يد جيم بيدزوس.

كان جيم بيدزوس يؤدي فيما يقترب عقد التعينات استعراضاً راقصاً معقداً، منفرداً، مع وكالة الأمن القومي. وكان الخيال قد زين له الآن أن الوكالة جاهدة لزعرعته وشركته، وإن لم يكن يملك برهاناً حقيقياً على ذلك. فقد أبدى الكثير من زبائنه المحتملين، على ما ظهر يومئذ، حماساً في البداية لمُنتج، وإذا بتلك الشركات تتوقف دون سبب واضح عن رد مكالماته. كذلك وجد الاهتمام من وكالات وهيئات حكومية بمنتجاته يتبخر. ولقد خامر بيدزوس شعور، استولى عليه حتى نخاعه الشوكي بأن هذا الصمت ليس مرده شلل أصاب مهاراته في التسويق وإنما سببه ضغط خفي مصدره في ولاية ماريلند.

بل لقد بلغ به الاستغراب حداً جعله يعجب لطبيعة علاقته با امرأة أخذت تطلعه تلقائياً لسبب من الأسباب على معلومات لا يدري بها إلا مطلع من داخل وكالة الأمن القومي . وكانت تبدو له تلك المعلومات يومئذ مقبولة ، إلا أنه أخذ يتساءل فيما بعد ما إذا كانت تلك المرأة مأجورة من الوكالة لتقدم له معلومات مضللة . وقد قال لاحقاً : «أعتقد أن هذا الأسلوب معروف في دوائر المخابرات بـ «فخ لعسل» . والمفارقة في الأمر أن هناك من كان يتساءل بين الحين والآخر ما إذا كان بيدزوس ذاته عميلاً مزدوجاً ، يتظاهر بالصراع مع وكالة الأمن القومي بينما هو يسرّب المعلومات خفية ويكشف أسرار التكنولوجيا في شركته . إلا أن الرجل كان يعتقد جاداً في أعماق عقله أنه أكبر شوكة في القدم التي تستند إليها الوكالة في الضبط والأصلا ت .

وما أثار الفزع في جيم بيدزوس حوالى عام 1990 لم يكن وكالة الأمن القومي ، وإنما تهديد أقرب كثيراً إلى عمله . وليس للحكومة ضلع فيه أيضاً ، وإنما سببه براءات الملكية الفكرية لمفتاح الشيفرة العام الذي كان الأساس الذي تركز عليه التكنولوجيا الخاصة بشركته . كانت المشكلة تتصل بشيفرة لا تنافس منتجاتها شركة الآر إس إيه مباشرة ، إلا أن براءات الملكية الفكرية لديها تحمل النذير بالقضاء على الشركة .

كانت الشركة تسمى سايلينك Cylink ، وتاريخها يشهد بلا استقرار والهدوء وأهى للراحة من ركوب قطار التسلية في مدينة ملاهي الآر إس إيه . وكان الشريك في تأسيسها جيم أومورا ، حائزاً على شهادة الدكتوراه من جامعة ستانفورد ، ثم أصبح أستاذاً في جامعة كاليفورنيا ببلوس أنجليس ، حيث درس الهندسة الكهربائية . أما حقله الأساسي فهو نظرية للمعلوما ت . وكان الرجل لا يحيط بشيء من الكريبتوجرافيا ، شأنه في ذلك شأن كل من اتصل بعلم الكمبيوتر في تلك الأيام الخوالي ولم يعمل لوكالة الأمن القومي . ولكنّه كان يعلم ساذ مساعد شاب في ستانفورد ذي اهتمام بالموضوع . ويروي لنا أومورا

أنه دأب يسأله: «علام تضيع وقتك في الكريبتوجرافيا؟ إذ بدا لي أن هذا موضوع عقيم لا طائل منه». وكان من حسن حظكريبتو جرافيا المفتاح العام أن هذا البروفسور - مارتي هيلمان - لم يأخذ بنصيحة أومورا.

ولما أخذ عقد السبعينات يقترب من نهايته كانت نظرة أومورا قد تغيرت وأصبح خبيراً في هذا الحقل. وقد أخذ فيما بعد يدرّس منهاجاً في الكريبتوجرافيا ليزيد من دخله، وكان تلامذته من العاملين في الصناعة، وأكثرهم يعملون في المقاولات في مشاريع الحكومة ويسعون إلى تطوير مُنتجات للمشاريع العسكرية. أما المنهاج الذي كان يقوم بتدريسه فيشتمل على مبادئ التشفير الأساسية، ولم يقتصر على تعليمها على الولايات المتحدة وحسب، بل في بلدان أخرى أيضاً مثل سويسرا. ويقول أومورا أنه كان حريصاً على ألا تتضمن الدروس التي يلقونها على طلابه أية معلومات سرّية. ولم يكن هو ذاته قد اطلع على موضوعات سرّية. ولكن من الذي يعلم ما تعتبره الحكومة من المحظورات؟

بعد سنوات قليلة أخذ أومورا وصديق له يتعاطيان العمل بالشيفرة فخرجا بمنتج، هو مفتاح عام في رقاقة سيليكون، مستخدمان في ذلك مبادلة لمفاتيح كما عرفت عند ديفي وهيلمان. ثم مضى إلى صديق آخر، يدعى ليو موريس، وكان من أوائل المشاركين في شركة صن مايكروسيستم، وأخذ الاثنان يقلبان فكرة الإتجار بهذا المنتج على وجوهها، فوضعا مخططاً عملياً لتنفيذ المشروع، ثم شرعا بالاتصال بأصحاب الرساميل لتمويله.

كان ذلك في عام 1984، أي في ذات الوقت الذي كانت تمر فيه شركة الآر إس إيه، بأصعب فتراتها تقريباً. كذلك لم يجد أومورا وصاحبه التمويل أمراً يسيراً، لأن «الممولين ما كانوا يهتمواً من المعلومات»، على حد تعبير أومورا. ثم قيض لخطة المشروع أن تقع بين يدي جيم سيمونز حين أحالها إليه أحدهم؛ ولم يكن سيمونز هذا رياضياً ومشتغلاً بالكريبتوجرافيا (كان أحد أوائل

الذين درسوا برنامج لوسيفر) وحسب، بل له نصيب في لا شتغال بالاستثمارات أيضاً. ولقد وافق عندما عرض عليه الأمر على مساعدة لشركة الناشئة سايلينك على الوقوف على قدميها.

كان محور اهتمام سايلينك، على العكس من الآر إس إيه، التي كان هدفها أن تشيع الشيفرة بين عامة الناس، حماية مرسلات الشركات الكبرى، وخاصة تلك التي تتولى التعهلات الحكومية. فلم تكن سايلينك لتعنى بما تسمح أو لا تسمح به وكالة الأمن القومي. وقد سمي أول مُنتج لها، وصدر إلى الأسواق في عام 1986، CIDECS-HS، (وحسبك ذلك من اسم ينضح إغراء). وكان هذا عبارة عن صندوق معدني مشحون بالرقاقات ومهمته تشفير لآصلات الهاتفية داخل الشركة ذاتها، بواسطة نظام شيفرة مركب: ديثي - هيلمان لتوليد المفاتيح ومعيار تشفير البيانات للتشفير. ولما كان الكثير من عملاء سايلينك من المؤسسات المالية المرخص لها استخدام كريبتوجرافيا تقوم على معيار تشفير لبيانات (ومنها SWFT سويفت المؤسسة لدوليتلتعاملات المصرفية التي تتعامل بتريليون دولار في اليوم البطيء)، فإن سايلينك لم تتعرض لمشاكل التصدير التي تفسد حياة شركات صناعة البرمجيات، مثل شركة لوتس. وهكذا سرعان ما تحولت تلك الشركة إلى مؤسسة رابحة.

كانت سايلينك قد مضت منذ البداية، إلى جامعة ستانفورد في طلب الإذبا استخدام براءة اختراع ديثي - هيلمان. وعندما أجازت الجامعة استخدام البراءة، كانت الإجازة في بداية الأمر غير حصرية. ويصف روبرت فوجنر، مستشار سايلينك، استقبال ستانفورد للطلب بأن ستانفورد كانت ثملة بالسعادة» فقد وجدت أخيراً من يستخدم براءة الاختراع فعلاً، وكان أن عقدنا صفقة جيدة جداً جداً». وكانت الآر إس إيه في منتصف الثمانينات تكافح كفاحاً شاقاً، والحق يقال، لترسي أقدامها، في حين كانت سايلينك لشركة الوحيدة، التي تحقق أرباحاً مر لمفتاح العام. فكان أن نمت العلاقة مع ستانفورد

وانتعشت . ثم عرضت سايلينك بعدئذ أن تمنحها الجامعة مزيداً من الحقوق لاستخدام براءات المفتاح العام . وكانت تريد في جوهر الأمر السيطرة على كافة البراءات . فإذا أراد آخرون ابتكار وتسويق مخططات شيفرة تعتمد على المفتاح العام أصبح عليهم وفق هذا التدبير طلب حقوق الإجازة من سايلينك لا من ستانفورد كحقوق ترخيص من الباطن .

ولقد وافقت ستانفورد على هذا المطلب ، بيد أن الأمر انطوى على علاقة ذات مغزى : نزاع مستمر حول حقوق الجامعة في الملكية الفكرية ، كما حول حقوق معهد ماساتشوسيتس التي تملك براءة الخوارزمية RSA رسا . وكان ستانفورد تعتقد بأن ما تملكه من البراءات تختص في جوهرها لمفتاح العام نظراً لأنها جسدت الفكرة العامة لكربيتوجرافيا لمفتاح المجرأ . فيمكن لأي شخص كان ، وفق هذا المنطق ، استخدام الخوارزمية رسا إذا شاء ، لكن عليه أن يحوز على ترخيص براءات ستانفورد أيضاً . لكن محامي معهد ملما تشوسيتس ذهبوا إلى أن الخوارزمية رسا موضوع مستقل . ولقد أطلق هذا الاختلاف حالة من التوتر بين الجامعتين استمر عدة سنوات . وكان ذلك (ومعذرة للتعبير) خلافاً هادئاً ، نظراً لأنه لم يكن في الأمر مبالغ ضخمة يومذاك .

ومع ذلك فقد رأى الجميع ، أن الخلاف بين مؤسستين ضخمتين لم يكن لائقاً ، وكان أن تم التوصل إلى تسوية هذا النزاع بينهما . وقامت ستانفورد برزم كل براءات الملكية الفكرية لديها والخاصة بمفتاح العام وأحالتها إلى معهد ماساتشوسيتس ، وقام المعهد بدوره بنقل تلك الحقوق لشركة الآر إس إيه داتا سيكيوريتي إنكوربوريتد . فأزاح هذا العمل سحابة ضخمة كانت تخيم فوق هذه الشركة ، التي كان نظاها يعتمد فعلاً على فكرة لمفتاح التي طلع بها هويت ديفي ومارتي هيلمان . ولم تعد برمجياتها الآن مشمولة كلياً بحماية براءة الملكية الفكرية وحسب ، بل لم يعد ثمة مجال بعلم هذا للحديث عن حقوق ستانفورد .

وفي حين أن هذا الترتيب كان مناسبا لشركة الآر إس إيه إلا أنه وضع سايلينكفي موقف ضعيف. فإذا أراد شخص الحصول على الإجازة استخدام شيفرة المفتاح العام فلا بد له عندئذ من أن يتوجه إما إلى سايلينك وإما إلى آر إس إيه داتا سيكيوريتي، ولكن لا يستطيع الحصول على حقوق استخدام نظام المفتاح العام إلا من شركة الآر إس إيه التي ابتكر مؤسسوها هذا النظام. لكن هذا لم يصبح مشكلة فوراً، لأن كل شيفرة كانت تسعى إلى عملاء غير أولئك الذين تنشدهم الشركة الأخرى. وفي حين أن كلتا الشركتين كانتا تناصران المفتاح العام وعلى بُعد عشرة أميال من بعضهما فإن سايلينك كانت تتسم، وفق تعبير فوجنر، بـ «العزلة لليد والباطنية لليد». . . . تركّز اهتمامها على تقنياتنا، وصنع مُنتج جيد، وبيع ذلك المُنتج لمجموعة محدودة، ولكن نوعية جيدة من العملاء». ومن الجهة المقابلة كانت سوق الآر إس إيه، العالم الأوسع من الحساب الشخصي وعيونها شاخصة إلى سوق جماهيرية واسعة.

وكان من المحتم، أن تجد الشركتان نفسيهما في صراع محتدم. فبسبب من الطريقة التي جرت بها تجزئة براءات الملكية الفكرية كان لكل شركة مصلحة في الدعوة إلى طريقة معينة في معالجة برمجيات المفتاح العام، والحط من قيمة النهج الآخر. ولأن براءات الملكية الفكرية الخاصة بمعهد سلا تشوسيتس لم تكن متاحة لسايلينك فإنها نشطت في الدعوة إلى استخدام طريقة تبادل المفتاح التي ابتكرها ديفي وهيلمان. وكان الناس في هذا الحقل يعتقدون، أن الحل يكمن، بالمعنى العملي للكلمة، في الابتكارات المشتقة عن أبحاث جامعة ستانفورد وحدها، إذ توفر طريقة لاتفاق طرفين على مفاتيح سرية؛ ولكنها على العكس من شركة الآر إس إيه لم تحدّد الوسائل لتنفيذ نظام مفتاح شيفرة عام كامل وكفاء غير أن سايلينك ذهبت في اعتقادها إلى أن بوسع المستخدمين، أن يأتوا بكل ما جاءت به الآر إس إيه، وبذات القدر من الإتيقان من الأمان للمعلومات والتثبت من الهوية وسوى ذلك، باستخدام مخترعات ديفي وهيلمان

استخداماً ذكياً وحصيفاً. وكان جيم أمورا قد كتب بحثاً في هذا، في 1987، وفي هذا يقول: «بوسعكم استخدام مبتكرات ستانفورد لتأتوا بما تأتي به الآر إس إيه. وأعتقد أن هذا أزعج جيم بيدزوس لأنه وجد أن تقنيته لم تعد التقنية الفريدة».

يقول فوجنر: «كان على شركة آر إس إيه، كي تنجح، أن ترفع من مستوى برمجياتها التطبيقية التي كانت في الواقع، تركز على برمجيات معهد ماساتشوسيتس. وبالمقابل كان هناك سايلينك التي أصابت نجاحاً تجارياً واضحاً بفضل التقنية التي تصدرها جامعة ستانفورد. وإذن فالصراع قادم، أو الاتفاق التجاري واقع لا بد متحقق».

ولقد وجد فوجنر نفسه ينضم إلى سايلينك بصفة مستشار، في 1989، ليتولى معالجة هذا الموضوع. وفي اليوم التالي لتعيينه التقى جيم بيدزوس. ولم تكن لديه إلا فكرة بسيطة عما ينبغي أن يتوقع. وتساءل في خلده إن كان جيم بيدزوس الذي اكتسب سمعة كفتان في ممارسة الضغط، في الصناعة الناشئة، سوف يظهر متصلياً؟ ولكن الرجل بدا أبعد ما يكون عن التصلب. فقد تكلف بيدزوس أشد العناء، كما يذكر فوجنر، ليبدو لين العريكة، مسيراً، وكان يظهر في سلوكه الدهول لما حققته سايلينك من النجاح في تجارتها. وقال لفوجنر: إن الآر إس إيه ما تزال تجاهد، ليظل رأسها فوق سطح الماء: إذن ليس لسايلينك ما يحملها على القلق من تلك الشركة. ولكن الشركتين، كانتا من الجهة الأخرى تواجه كلتاها معركة صعبة لإرساء التشفير على نطاق أوسع. وقال بيدزوس أن شركتيهما كانتا تعملان على نشر تقنية ليس هناك من يعطيها حقها، ولا من لديه رغبة بشرائها. ومما يزيد الطين بلة أن الشركتين الأضخم اللتين تأخذان بالمفتاح العام، كل واحدة منهما تدعو إلى تطبيق يختلف عما تدعو إليه الأخرى، فتثيران الحيرة في عقول الناس جميعاً!

وهنا دعا بيدزوس صاحبه قائلاً: دعنا لا نتقاتل مع بعضنا البعض! ولم لا

نجمع كل البراءات ونعمل سوية، ونتفق على مفتاح عام معياري، ويكون لنا الترخيص والإجازة؟ ولسوف نحقق البلايين من الدولارات!

بدا ذلك كله منطقياً لفوجنر. فلم لا نضم قوانا إلى بعضها، حقاً؟ وحدثته نفسه أنه لك سوف يحمل المحامين لدى ستانفورد على الارتياح، إذ لطالما أسف هؤلاء لمنحهم معهد ستانفورد حقوق الإجازة الجزئية عن ممتلكاتها الفكرية. إن ستانفورد إنما عزلت نفسها حين جعلت شركة الآر إس إيه مقصد كل من يطلبها لمفتاح العام. وفي هذا يقول فوجنر إن: «النكته الشائعة في ستانفورد هي أن الاتفاقية مع معهد مسلا تشوسيتس للتكنولوجيا باتت مثلاً كلاسيكياً على ما ينبغي أن تتجنبه عند إجازة براءة الملكية الفكرية». ولذلك فقد بدت فكرة بيدزوس بجمع براءات الملكية الفكرية في سلّة واحدة - مع الوعد برفع أجور تراخيص المفتاح العام - شديدة الإغراء لجماعة جامعة ستانفورد. فعملوا على حث سايلينك على الأخذ بها.

ولقد توصلت لشركتان والجامعتان إلى التفاهم في ما بينهم، يوم 17 تشرين أول/ أكتوبر 1989، وهو ذات اليوم، الذي وقع فيه زلزال ضخم بقوة 7 درجات بمقياس ريختر هزّ منطقة الخليج. (وقع العقد رسمياً في نيسان/ أبريل التالي). وبموجب هذا الاتفاق تصبح كافة براءات الملكية الفكرية ملكاً لشركة جديدة تتألف من آر إس إيه وسالينك، وتخضع هذه المؤسسة الجديدة، وتسمى ببليك كي بارتنرز PKP، لإدارة مشتركة بالتساوي من الشركتين الأم. وقد تمكّن جيم بيدزوس من النجاح في مفاوضاته تلك. ونيل قسمة مناسبة من العائدات بنسبة 55 - 45 لصالح شركته، على أساس أن قيمة حقوق الملكية الفكرية لخاصة بمعهد مسلا تشوسيتس تفوق قيمة براءات الملكية الفكرية الأخرى في الصفقة كما نت الآر إس إيه قد حصلت على بعض براءات الملكية من ستانفورد، بينما سايلينك محرومة من حق استخدام تقنيات الآر إس إيه). هذا في حين أن الجامعتين، لم تنالا إلا جزءاً يسيراً من العائدات المتوقعة: إذ

تبلغ حصة جامعة ستانفورد تسعة سنتات ولمعهد ماساتشوستس أقل من أربعة عشر سنتاً من كل دولار تناله الشركة الجديدة من استخدام حقوق الملكية الفكرية من المرخصين الفرعيين .

ويذكر أومورا أن بيدزوس حاول بعيد تأسيس الشراكة، أن يحمل سايلينك على التخفيف من القول، بأنه من الممكن تنفيذ وظائف لمفتاح العام بدون الخوارزمية رسا: «قال لي ما معناه: أما وقد أصبحنا شركاء الآن فرجائي أنتو قُف عن الترويج لطريقة ديقي - هيلمان وتدعم الخوارزمية رسا». فأجابه أومورا أشرسته سوف تستمر بالأخذ بالطريقة البديلة، ولكنه لا يرى سبباً ليكون ذلك مشكلة، «فلا يهم أي تقنية نستخدم. فنحن شركاء»، كما قال لبيدوس .

ويفسر فوجنر بقوله: «لم يكن هناك في عام 1990 من يهتم بالتقنية. ولكن ما أن مضى عامان حتى أصبحت التقنية موضع اهتمام الجميع» .

في بداية الأمر كان المدير فوجنر وبيدزوس يعملان معاً على ما يرام. فكان فوجنر من الناحية الفنية المدير المسؤول عن الإجازات وبيدزوس الرئيس. ولكن النظام الداخلي كان يفرض اتخاذ القرارات بالإجماع. وكان هذا المشروع بالنسبة لفوجنر، وهو محام اختصاصي بقوانين الشركات بعيد عن الإدعاء والتفاخر، وقد ائتمف الآن مع رجل يزهو بعقد الصفقات الرابحة مثل بيدزوس، أشبه بالمغامرة الجنونية، عمادها مغامران مجنونان، يحاولان فرض معيار عالمي لمفتاح عام للشيفرة - وجني الملايين كل لشركته .

لقد بلغ فوجنر من الشغف بالفكرة ما جعله يعرض عن توقيع أي اتفاقية، إذا بدا له بأن مصالح كل من الآر إس إيه وسيلينك ما تزال على افتراق. وكان أول عمل للشركة أن توجه كتاباً إلى المؤسسة القومية للمعايير والتكنولوجيا NIST وهي الوكالة الحكومية التي تُعتبر المرجع الأخير الذي يقرر المعايير التي ينبغي أن تقوم عليها الاتفاقيات والأسواق. وكان نجاح الشراكة بين الشركتين

يعتمد إلى حد بعيد على ما إذكا نت مؤسمة المعايير والتكنولوجيا، سوف تقبل براءات الملكية الفكرية، التي باتت تحت سيطرة فوجنر وبيدزوس معاً معياراً معتمداً، والواقع أن ثمة عدة معايير كريبتوجرافية مختلفة يجب أن تخضع لموافقة المؤسسة: معيار للتوقيع الرقمي، وثان للتشفير وثالث لتبادل المفتاح والخ... فإذا تقررت هذه لمسائل أصبحت ثورة الشيفرة جاهزة للإنطلاق. وعندئذ سوف يعلم مطورو البرمجيات جميعهم أية خوارزميات هي اللازمة للسرية والتثبت، وسيعمدون بعدئذ إلى إدماجها في برامجهم. كذلك سوف تتفاعل البرامج مع بعضها البعض، فإذا انطلق هذا الترتيب ستطاع مستخدم برنامج اللوتس إرسال بريده المشفر إلى مستخدم وورد بيرفيكت Word Perfect ويستطيع مستخدم المايكروسوفت وورد Microsoft Word وضع توقيع رقمي على دفتر حسابه للحدسي. وهذه خطوة حاسمة لا بد من اجتيازها، ومؤسسة المعايير والتكنولوجيا تدرك هذا.

ولقد قررت الحكومة أن ترسي تكنولوجيا التوقيع الرقمي، باعتباره المعيار الأول. ولكن حذار. فلقد كان لكل من سايلينك، وآر إس إيه فهمه الخاص للتوقيعات، وكل منهما قائم على مذهبه في المفتاح العام المنفصل: أهو مذهب ستانفورد أم مذهب معهد ملنا تشوسيتس؟ وأي من المفهومين سوف تقدمه شركة بيليك كي بارتنز للحكومة وترشحه رسمياً ليكون معياراً؟ وكان الجواب في جعبة جيم بيدزوس: ليكن هذا باسم آر إس إيه. أما قوم سايلينك فكانوا في شك؛ فبعد كل شيء كان هؤلاء قد اشتغلوا بتواقيع ديقي - هيلمان مدة تبلغت سنوات. وكان لدى بيدزوس حل لهذه المعضلة، فقال لشركائه: إذن لنقدم خوارزمية «سا» للتوقيع، وحينئذ مشكلة معيار التحكم لمفتاح (الطريقة التي تسمح باستيعاب بلايين وبلايين المفاتيح الرقمية التي يسمح نظام ضخم بمعالجتها)، فسوف نأخذ بطريقة ديقي - هيلمان. وقد وافقت جماعة سايلينك على هذا الاقتراح. وأرسلت رسالة من شركة بيليك كي بارتنز، إلى

مؤسسة المعايير والتكنولوجيا، بتوقيع فوجنر يوم 20 نيسان/ أبريل، أي بعد أسبوعين فقط من تأسيس الشركة. وقد حُتّت الرسالة الوكالة على اعتماد خطة «رسا» كمعيار. وذهبت الرسالة بالقول، أن بليك كي بارتنرز تكفل الترخيص بتواقيع «رسا» بشروط معقولة ميسرة دونما تمييز».

لكن حين بلغ الأمر للتوقيع الرقمي فإن الحكومة بدت تحمل آراء أخرى.

وسط هذا الجدل المحتدم كان جيم بيدزوس ما يزال مهتماً ببقاء شركته عائمة. وهو يعمل الآن على الفوز، بأضخم صفقة ترخيص، عقدها حتى ذلك الحين - اتفاق واسع، مع أقوى شركة للبرمجيات في العالم: مايكروسوفت، الحوت الأبيض في محيط التكنولوجيا المتقدمة. فمنذ بضع سنوات، أصبح عباقرة الشركة يعون باطراد، أن زبائنهم يحتاجون إلى توفر عنصر الشيفرة، في ما تنتجه مايكروبو فت. ومن مقر إدارة الشركة في رهوند، بولاية واشنطن، كان كبير الخبراء ناثن مرفولد، قد دأب منذ حين على تعميم مذكرات حول الأهمية التي سوف يحتلها عنصر التشفير في أجهزة الكمبيوتر. وكان مرفولد كثيراً ما يتوسل بذكر جدته ويضرب بها للمثل؛ وكانت جدته هذه تعيش في منطقة زراعية اعتاد أهلها ترك أبواب بيوتهم مفتوحة دون قفل. ولم يكن في ذلك بأس في بيئة منعزلة قلما يطرقتها غريب، إلا أن هذا لا يصلح لبيئة مدينية بأي حال. وكذلّك الأمر مع الكمبيوتر، فالكمبيوترات كانت في حالة انتقال من وحدات منعزلة لا اتصال بينها وتقع على طاولات المكاتب إلى عقد متصلة ببعضها بشبكة في قاعدة بنية تحتية عريضة واسعة. فلتوفير الحماية والأمان لكل شيء بدءاً من الضرائب حتى السجلات الطبية من تطفل المتطفلين، لا بد لك من التزود بأقفال؛ وقد أدرك مرفولد أن كريبتوجرافيا المفتاح العام هي الأقفال الموعودة.

كان مرفولد ما يزال طالباً على مقاعداً لدراسة في الجامعة يوم نشرت

مقالة مارتين جادنر، عن الخوارزمية «رسا» في مجلة العلوم الأمريكية Scientific American، وأعجب بها حتى أنه وصفها بـ «الرائعة»، كذلك التهم من غدا عالماً فيزيائياً في ما بعد (وقد درس على يد ستيفن هوكينج في جامعة كامبردج) بحث الخوارزمية رسا وورقة بحث ديثي - هيلمان التي استلهمها البحث. وبعد عقد من الزمن، وعقب شراء شركة مايكروسوفت، شركة البرمجيات التي أسسها، أصبح مرفولد أحد الأعوان الأقرب والموثوقين من بيل جيتس. وقد أثار هذا المنصب حماسه إذ وجده فرصة للمساعدة في تعميم المفتاح العام. وكما كان الحال مع راي أوزي وشركة لوتس انتهى الرجل إلى التعامل مع الشخص الوحيد في هذا المجال: جيم بيدزوس.

كانت إجازة مايكروسوفت أمراً حاسماً لبيدزوس، لأنها سوف تجعل من تقنيته معياراً آمناً لمئات الملايين من العملاء، الذين يستخدمون برامج مايكروسوفت دوس DOS ووندوز Windows وتطبيقاتهم مثل معالج الكلمات وورد Word وجدول البيانات اكسل Excel. ومع ذلك فقد دخل بيدزوس المفاوضات بروحه الهجومية المألوفة، متفاخراً بأنه، باعتباره يحمل الملكية الفكرية للاختراع، فهو المرجع لوحد لكل من يُعنى بالشفرة والتشفير. ولكن هذا الادعاء والتفاخر لم يستفزا مرفولد. فإذا كانت الخوارزمية «رسا» على هذا القدر من العظمة فلم لا نجد الناس يقبلون على استخدامها؟ ولكنه سلم بأنه سيكون من المحتم أن تشيع أنظمة المفتاح العام، ثم مازح بيدزوس بقوله: إن الناس ربما اقبلوا على استخدام هذه الأنظمة في نهاية القرن، حين يكون أمد براءة الملكية الفكرية قد مضى وانقضى.

غير أن هذه الملاحظة، لم تنل من متانة أعصاب بيدزوس، فاستمرت المفاوضات - بين رجلين كلاهما ذو شخصية ضخمة، ويرمي في المعركة أقصى ما لديه. وكانت القضايا المطروحة معقدة، بسبب رغبة مايكروسوفت في التمتع بحق تعديل رمز عدة تشفير الخوارزمية «رسا» ليلائم منتجاتها. ثم كان

هناك كما علم راي أوزي من قبل، عقبة أضخم تواجههم جميعاً: قوانين التصدير.

بدأت مايكروسوفت، إدراكاً منها، بأن تضمين منتجاتها عنصر التشفير يشكّل معضلة، حواراً مع وكالة الأمن القومي. وبالرغم من أن العلاقة الجديدة اتّسمت بالودّة، إلّا أنّها لم تكن بالميسّرة. ففي الزيارات القليلة الأولى التي قام بها ممثلو فورت ميد إلى مقر الشركة في ردموند لم يشأ هؤلاء حتى أن يكشفوا عن اسم الكنية عند مكتب الاستقبال؛ فكان على مرفولد، أن ينزل إلى موظف الاستقبال ليمنحهم بطاقات الدخول دون أن تحمل أسماءهم كاملة، بل الاسم الأول وحسب. ويصف مرفولد سلوك الجماعة، بلهجة تجمع بين الاستطراف والضيق بأنّهم «ذوو غريزة استمرارية». والأدهى من ذلك أنّهم ما كانوا يصرحون بما هو مسموح، وما هو ممنوع. ولكنّهم كانوا غاية في البيان في أمر واحد: آر إس إيه داتا سيكيوريتي. فيبدو أنّهم كانوا يحملون ضغينة تجاه هذه الشركة.

وغني عن القول، أن جماعة وكالة الأمن القومي لم يكونوا ليرتاحوا، لتولي هذه الشركة الحديثة العهد عمليّة توفير درع مضاد لاعتراض المعارضين، والراصدين لمثبات الملايين من زبائن مايكروسوفت. ولقد حاولوا تأليب مرفولد، كما يروي هو تطور الحوار، على جيم بيدزوس وشركته. وكان نهجهم في تأليبه على بيدزوس طريفاً. فبدأوا بالتلميح، دون التصريح، بأن الشيفرة التي طلع بها رايفست وشامير وأدليمان قد تم تفكيكها خلف السياج الثلاثي. وخشي مرفولد من ألا يتمكّن من توفير قدر معقول من الأمن لزبائنه - فإذا كانت الحكومة تستطيع تفكيك الشيفرة، لم لا يستطيع نصّاب أيضاً من تفكيكها؟ - وهكذا أخذ يقرب بيدزوس، على مشواة زعم وكالة الأمن القومي.

ولقد ذهل بيدزوس للمفاجأة، إذ كان يشعر بأن الصفقة في طريقها إلى الاختتام. فهب لدحض هذه الادعاءات، وتابع: «لقد اتصلنا بكل منظر في علم

الأرقام، وكل رياضي، وكل باحث نعرفه في هذا الحقل، ثم عادوا إلينا جميعاً، في غضون أربع عشر بين ساعة. لقد أفحمننا [مايكروسوفت] بما فعلنا، وقالوا لنا: «من الواضح أن هذا الزعم غير صحيح».

ولكن مرفولد يذكر الحادثة على نحو مختلف، فيقول أولاً ضرورة لدحض الزعم، إذ كان يعتقد على الدوام بسلامة مبدأ لخوارزمية «رسا». إلا أنه يذكر أنه كان يملخ بيدزوس، حين قال ذات مرة أن ليس ثمة طريقة تصمد أمام تحليل الشيفرة إلا إذا كان ورقة الحل لمرة واحدة One-Time Pad. وكان رد بيدزوس منطقياً إذ قال: إن بوسع المرء الوثوق بشيفرة مطبوعة ومتاحة للناس وللنقد من أي شخص في المجتمع - أكثر من أية خوارزمية سرّية لدى وكالة الأمن القومي. ذلك أن مستقبل الخوارزمية «رسا» يعتمد كلياً على قوة رموزها، لهذا فلديها كل خلل للتأكد من قوة هذه الرموز. وفي هذا يقول بيدزوس: «إذا تمكّن أحد من تفكيك الخوارزمية فلن يكون لديك إلا أطلال من شركة، كان لها موقع في لصناعة ذات يوم مضى». ولكن بيدزوس تمكّن من إقناع مرفولد بوجهة نظره. وكان نفور وكالة الأمن القومي من الخوارزمية «رسا» بالنسبة لمرفولد بمثابة شهادة لصالحها، فتساءل في خلده: لماذا تريد الوكالة منع نشرها إلى هذا الحد، إلا إذا كان يصعب تفكيكها؟

لكن وكالة الأمن القومي، لم تكن قد فرغت من أمرها بعد. فقد قامت بمحاولة أخرى بعد ذلك، لتثبيط عزيمة مايكروسوفت عن إجازة الخوارزمية «رسا» فأخذت بالتدقيق حول حق الشركة بالملكية الفكرية للخوارزمية. وراح جماعة الوكالة يشككون باعتمادقنيت الأراس إيه كمعايير معتمدة من الحكومة مستقبلاً، وبالتالي فقد ينتهي الأمر بمايكروسوفت إلى أن تنحصر ملكيتها من هذه التقنية بمجموعة يتيمة من الخوارزيمات. فهرع بيدزوس عائداً إلى ردموند، ليقدم محاضرة وعرضاً للبرهان بشكل قاطع، على متانة واتساع ما لديه من حقوق الملكية الفكرية.

ولقد جاءت محاولة وكالة الأمن القومي الأخيرة لتخريباً لصفقة، حسب الرواية التي رواها بيدزوس، حينما اتصل أحد مسؤولي الوكالة بمرفولد، وقال له، ما فحواه، «دعكم من الخوارزمية «رسا». (يقول مرفولد أنه لا يذكر هذه الكلمات حرفياً، ولكنه يؤكد أن وكالة الأمن القومي أعربت لمايكروبيو فت عن اعتقادها أن من الخطأ استخدام رسا: إنه خطأ كبير ترتكبه شركة البرمجيات العملاقة بارتباطها بشركة لا يُعتد بها).

وهنا ثارت ثائرة بيدزوس. فاتصل كما يذكر الآن بأعلى من عرفهم رتبة وراء السياج الثلاثي، وشرح له ما بلغه. وقبل أن يتمكن هذا المسؤول من النطق بكلمة واحدة طلب منه تقييم الأمر والاتصلاًهايكروبيو فت والاعتراف لها بأن الوكالة ارتكبت خطأ فادحاً [حين قامت بالتشويش على الخوارزمية]. وقال له: «إذا لم يصوب هذا الأمر فلسوف يكون لعضو الكونجرس عن منطقتي شأن معك. وإذا لم يجد هائلضاً فلسوف يكون حسابك مع المدعي العام في المنطقة، لأنني سوف أتقدم بالادعاء عليكم. وإن لم يجد هذا كذلك، فإني سوف اتصل بصحيفة نيويورك تايمز. ومهما يكن فإنكم لن تصلحوا الأمر، وجدتموني لا أدعُ سبيلاً حتى تتحملوا مسؤولياتكم». ولقد توقع بيدزوس أن ينكر محدثه ما نسب إلى عناصر وكالة، إن كلياً أو جزئياً، أو يصر على جهله بأمر التخريب. ولكنه، بدلاً من ذلك، قال على ما يزعم بيدزوس: «لسوف اتصل بهم». ولقد اتصل محدثه حسب رواية بيدزوس، بمايكروبيو فت معترفاً عما سلف من موظفي الوكالة [بحق الخوارزمية والشركة].

أصبح الطريق سالكاً الآن لعقدا لصفقة. ولكن نقطة واحدة صغيرة وقفت تعرقل الاتفاق هي إصرار بيدزوس على أن يوقع بيل جيتس العقد شخصياً، ولقد كان بيدزوس يريد عرض الصفحة الأخيرة من العقد على حائط [مكتبه]، وكيف يبدو الأمر بدون جون هانكوك مدير عام مايكروبيو فت الشهير؟ ويقول

مرفولد متفاخراً أنه استطاع بتلميحه إلى احتمال تعذر توقيع العقد من بيل جيتس شخصياً أن ينتزع من بيدزوس بعض السكاكر. (ولكن بيدزوس أيضاً نال قطعة سكر بدوره، حضور جيتس حفلاً في الآر إس إيه).

وبعد بضعة أيام، وفي عطلة نهاية الأسبوع، في ذكرى قتلى الحرب [يصادف يوم الاثنين الأخير من شهر أيار/ مايو] 1991، اتصل بيدزوس بفوجنر، وهو يتباهى بالصفقة التي بلغت اكتمالها الآن. ويذكر فوجنر أنه عجب لذلك، وقال لبيدزوس: «هذا عجيب، يا جيم. لديك مايكروسوفت، لتشتري رخصة عدة شركتك الخاصة، ثم هأنت ذا تضمّنها نظام التشغيل لديهم؟ هذا لا يصدّق! كيف استطعت ذلك؟».

فقال جيم بيدزوس: «هكذا فن الإقناع والبيع، يابوب، وأنا بائع ممتاز!».

و سواء كان الأمر يتصل بفن الإقناع والبيع أم لا، فقد بات مستقبل المفتاح العام، في أوائل 1991، موضوع شك، بسبب افتقاد موافقة الحكومة. كان بيدزوس يتحرّق طبعاً لتكون الخوارزمية رسا المعيار للشيفرة. والحق أن المؤسسة القومية للمعايير وتكنولوجيا شديدة الحماس في بداية العملية لإرساء رسا معياراً. فقد كتب عالم كبير في المؤسسة يصف «رسا» بـ «نظام مفتاح عام شامل رفيع جداً». بل لقد حاولت المؤسسة حتى في كانون الأول / ديسمبر 1990 أن تقنع خصم بيدزوس، وكالة الأمن القومي - التي كان صوتها في العملية حاسماً - بضرورة اعتماد هذا النظام، إذ قال مندوبوها في اجتماعات وكالة المخبرات أن من مزايا النظام رخص كلفته تجارياً، كما أنه ليس هناك ما يضارعه من الناحية الفنية.

ولكن المفاوضات تعرقلت بعد هذا، كما لم تُجدِ المناشدة كما يبدو من بيدزوس أو فوجنر في اعتماد رسا معياراً. ثم بدا السبب في ذلك جلياً يوم 30

آب/ أغسطس 1991. ففي هذا اليوم توصلت وكالة الأمن القومي إلى طريقتهما الخاصة في التشفير.

ولقد طرحت المؤسسة القومية للمعايير التكنولوجيا مجموعة جديدة من الخوارزميات، عبر المدونة الفيدرالية The Federal Register، لتكون المرشح الأول بين لمعايير. وكان هذا المنتج الحكومي المعروف باسم «خوارزمية التوقيع الرقمي» DSA، قد وضعه موظف في وكالة الأمن القومي يدعى ديفيد كرافيتز، وهو مشابه في الكثير من النواحي لمخطط توقيع «رسا». وكلاهما يستخدم زوجاً من المفاتيح العامة - الخاصة. وفي كلاهما على أليس، حين تشاء كتابة رسالة موقعة رقمياً، أن تنفذ خوارزمية تُعرف باسم دالة التجميع وتؤدي إلى «مختصر الرسالة». (وهذا اختصار لرسالة والإبقاء على جوهرها لتيسير المعالجة). ثم يكون تشفير الرسالة، أو «توقيعها» عبر عملية بلوكية تعتمد على المفتاح الخاص الفريد الذي تحمله أليس، وترسل كلتا الرسالتين الأصلية والمختصرة إلى بوب على الطرف الآخر. وحين يستلم بوب - أو أي شخص آخر - الرسالة يكون لديه الآن طريقة للتحقق من أن صاحبتها هي أليس فعلاً ولم تتعرض لعبث من عبث أو أي شيء من هذا القبيل، أثناء البث: وهي أن يستخدم عندئذ مفتاح أليس العام لعرض الرسالة والملخص. ثم يتوسل بدالة التجميع ليعيد تكوين رسالة أليس من الملخص. فلا تتطابق الرسالة المكونة والأصل، إلا إذا كانت قد صدرت الرسالة عن أليس وإلا ظللت رسالة على حالها دون تبديل.

كانت طريقة الحكومة تختلف عن مخطط التوقيع بطريقة «رسا» من ناحية واحدة، وهي أنه لا يمكن استخدام لمفتاح العام - الخاص المزدوج إلا للتحقق من هوية المرسل، وليس للتشفير؛ أي بعبارة أخرى أن هذا نظام مفتاح عام لا يقوى على حفظ سر، وهكذا فإنه لا يمثل خطراً على الأمن القومي، أو حفظ النظام، أي أنه بدقيق العبارة عين ما أرادت الحكومة. وقد قال مسؤول في

المؤسسة القومية للمعايير والتكنولوجيا، في شهادة أمام الكونغرس: «إن استراتيجيتنا الأساسية تهدف إلى تطوير تكنولوجيا تشفير لا تلحق ضرراً بأمننا القومي ولا تنال من قدراتنا على حفظ النظام في هذا البلد... ولقد كان هدفنا ابتكار تكنولوجيا تنفيذ توافيق - ولا شيء آخر - بشكل متقن».

ولكن المؤسسة القومية للمعايير والتكنولوجيا لم تأخذ بهذا الهدف، وهي التي كانت تحببنا أصلاً اعتماد الحل الذي أتت به الآر إس إيه، إلا إثر ضغط مارسه عليها فورت ميد [وكالة الأمن القومي]. ففي الشهور الأخيرة من 1990، كانت وكالة الأمن القومي تتشدد في الدعوة إلى اعتماد نظامها، ثم طرح الموضوع مديرها الجديد الفريق وليم ستودمان، في شباط/ فبراير 1991، وألح على المؤسسة القومية للمعايير والتكنولوجيا بأن «تختصر النقاش وتقوم بإجراء ما يلزم لتوفير الحماية الضرورية».

وفي الاجتماع التالي لمجموعة العمل المشتركة التي تضم أعضاء من الوكالة والمؤسسة رفع ممثلو المؤسسة الأعلام البيضاء، إعلاناً بأن إداراتهم، «تقبل اقتراح وكالة الأمن القومي». ولكن حين أعلنت المؤسسة القومية للمعايير والتكنولوجيا اعتماد خوارزمية وكالة الأمن القومي في نيسان/ أبريل لم يأت أحد بأي إشارة إلى علاقة وكالة المخابرات السريّة بالأمر.

غير أن بيدزوس لم يخدع بظواهر الأمور، وثار تثارته لاختيار الحكومة خوارزمية التوقيع الرقمي معياراً. ثم ذهب إلى القول بأن وكالة الأمن القومي قد تمكنت من تخريب وزارة التجارة - وهي تخضع لها المؤسسة القومية للمعايير والتكنولوجيا - تخريباً كاملاً. ومضى في ادعائه، بأن وزارة التجارة أصبحت تعمل ضد الصناعة الأمريكية، عوضاً من دعمها، وغدت في خدمة الأشباح كلياً. (ولقد دعم هذا الشك في ما بعد تحقيق قام به الكونغرس وحمل لجنة مراقبة لعمليات الحكومة على الإعلان بأن «NSA وكالة الأمن القومي» لا تصلح للقيام بهذا المشروع الهام). وحذر بيدزوس من أن الخطوة التالية

ستكون افتضاح معيار للتشفير لا يأخذ بالخوارزميات المعروفة - خوارزمياته! - وإنما خوارزميات جديدة تستطيع الحكومة تفكيكها.

لقد كان في جعبة بيدزوس الكثير من القنابل ليستخدمها في هجومه. فمن ناحية فنية محضة، كان واضحاً أن خوارزمية «التوقيع الرقمي» DSA دون خوارزمية «رسا» متانة، فكانت «معياراً غريب الأطوار»، على حد تعبير أحد المراقبين، وأبطأ من خوارزمية سا في التحقق من التواقيع (وإن كانت أسرع منها في توقيع الرسائل)، وأشد صعوبة في التطبيق وأكثر تعقيداً من الأخرى. ولم تكن تتضمن عنصر التشفير، ولا كانت تتمتع بسجل و صف مسار، على العكس من «الرسا». ومع ذلك فقد كان المبتكر الحكومي يتمتع بميزة على «الرسا»، وكان على بيدزوس أن يسعى جاهداً ليأتي بمعادل لها. فقد أعلنت الحكومة، في البيان الصادر يوم 30 آب/ أغسطس، اعتمادها توزيع معيار التوقيع الذي خرجت به على نطاق عالمي مجاناً دون أجر.

ورأى بيدزوس أنه قادر على مجابهة المعيار المقترح متوسلاً في ذلك بحقوق الملكية الفكرية. ولكن الأمر لن يكون يسيراً. فقد كانت الشركة بليك كي بارتنز PKP تسيطر على حقوق الملكية الفكرية للمبتكرات الخاصة بجامعة ستانفورد التي تتضمن أول التواقيع الرقمية. ولكن الحكومة ادعت بأن مخططاتها قد تجاوزت تلك البراءات وذلك بالاعتماد على تطبيق مغاير من التواقيع الرقمية. وكان هذا المخطط قد صُمم على يد كريبتوجرافي من ستانفورد يدعى طاهر الجمل، وهو من طلاب هيلمان القدامى، وقام بوضع وصقل فكرة الخوارزمية المجمعمة وتلخيص الرسالة من أجل التوقيع الرقمي. غير أن الجمل أخطأ بأن قام بنشر مشروعه قبل التقدم بطلب براءة الملكية الفكرية (صدر بحثه عام 1985)، فكان أن تخلى بذلك عن حقوق براءة الاختراع. فإذا كان زعم الحكومة صحيحاً فإن خوارزمية لمفتاح الرقمي تصبح متاحة مجاناً ولا يترتب على استخدامها أي حق بادعاء الملكية الفكرية.

ولكن بيدزوس ذهب مذهباً مخالفاً، إلا أنه أدرك أن عرض القضية للتحكيم هدر للوقت ومكلف مادياً. ومع ذلك فقد وجد طريقاً آخر لانهام الحكومة بسرقة الملكية الفكرية. وكان هذا يتطلب براءة أخرى.

كانت هذه البراءة تقوم على عمل لعالم شيفرة ألماني، يدعى كلاوس شنور، حصل على براءة الملكية الفكرية عن مخططه للتوقيع الرقمي في شباط/فبراير 1991. وقد أصرت شنور بعد سماعه بخوارزمية لتوقيع الرقمي على أن هذه الخوارزمية تنال من حقوق ملكيته الفكرية وطالب الحكومة الأمريكية بمليون دولار تعويضاً عن الضرر الذي لحق به. وكان هذا الادعاء في رأي العديد من المراقبين مبالغاً فيه من طرف شنور لأن كلا النظامين سواء كان هذا الذي أتى به شنور أم ذلك الذي ابتكره كرافيتز، هما نسختان عن نظام طاهر الجمل. ومع ذلك فقد أثار الأمر قلق الحكومة. ذلك أنها تجشمت عناء كبيراً، بتأكيدا عند طلب براءة الملكية الفكرية على أن الأفكار التي يقوم عليها خوارزمية التوقيع الرقمي لم تُستق من شنور. غير أن شنور كان لديه بعد براءة «فزاعة» واحدة على الأقل: ادعاء قد يمكن أن يصمد في دعوى طويلة محكمة، إلا أنها توفر للمدعي سبباً وجيهاً لمهاجمة مفهوم مماثل. وإذا لم تتم تسوية الأمر مع شنور، فإن الحكومة ستواجه مشكلة.

ولقد رأى بيدزوس في هذا الوضع، فرصة عظيمة يمكنه اغتنامها. كانت الحكومة ترعد أمام المشكلة الناشئة، شرع وهو يحاول إضافة البراءة الألمانية إلى مجموعة البراءات لدى بليك كي بارتنز، أي بعبارة أخرى تأسيس احتكار لبراءات الملكية الفكرية! وصادف أن علم بيدزوس أن شنور كان يشارك يومئذ في مؤتمر علمي في مارسيليا وهكذا طار وفوجئ للقاءه. ووفقاً الاثنان في الاجتماع به على غداء، في أحد أفخم المطاعم في المدينة. ولقد طال الغداء وامتد عدة ساعات. وكان شنور في الأربعينات، وعالماً محافظاً، ويزهو بأحدث فتوحاته العلمية، إذ كان قد نال جائزة لايبزيغ لتوه ومكافأة مالية

مجزية. وتمتق ذهن بيدزوس بسرعة عن طريقة للتعامل معه: «لقد تحدثت إليه كما يتحدث مدرب مع لاعب التنس، وقلت له أنه يستطيع تنفيذ الخوارزمية بنفسه، أو يدع لي التفاوض وتولي الاهتمام بعقوده والتراخيص، ويستطيع عندئذ التفرغ لاهتماماته العلمية». وقد أثارت هذه المفاوضات إعجاب فوجنر: «لقد أغرقه بخصص عن صداقته مع بيل جيتس وتصوره لمفتاح عام للشيفرة يعم العالم والكون».

وانتهت الولاية في خاتمة المطاف، بينما الندلاء يقفون، يتعجلون تنظيف آخر الموائد. ثم انتقل الثلاثة إلى حانة في منطقة الميناء. وهناك قام فوجنر بتدوين اتفاقية على ورقة تنتقل بموجبها كافة الحقوق الناجمة عن الملكية الفكرية التي تخص سنور إلى بيليك كي بارترز PKP. في تلك الحانة، وفي ظل سفينة شراعية من القرن الخامس عشر وقّع سنور الورقة، سواء تحت تأثير وعود بيدزوس بالثراء أم بسبب التعب الذي نال منه.

ولما عاد بيدزوس إلى الولايات المتحدة كان له لقاء آخر من سلسلة لقاءات لا تنتهي، مع المؤسسة القومية للمعايير والتكنولوجيا. وكان اتصاله محدداً بدينيس برانديستاند ولين ماكلتي، وهما عالمان من علماء الكمبيوتر في الوكالة، غالباً ما وجدا نفيهما بين مطرقة مطالب الجمهور وسندان أوامر رؤسائهما. وقد بذل هذان العالمان أقصى جهودهما لحث المؤسسة القومية للمعايير والتكنولوجيا على شراء حقوق الملكية الفكرية لمبتكر سنور، أملاً منهما بحل مشكلة البراءة الفكرية التي تواجه الحكومة. كذلك سعى العالمان إلى تسوية أي نزاع حول الملكية الفكرية التي تعود لجامعة ستانفورد بدفع تعويض مالي إلى شركة الآر إس إيه. وعليه فقد ذهب بهما الظن إلى أن الاجتماع سوف ينحصر بالتداول في مثل هذه المسائل. ولما بدأ الاجتماع وجدا بيدزوس يبادرهما بالقول: «إنني أمثل كلاوس سنور وأنتم معتدون على حقوقي بالملكية الفكرية».

ولقد غمريدزوس شعور عارم بالنشوة في هذا اللقاء، حتى أنه استذكره في ما بعد، وقال: «إنني لم أر في حياتي شخصين بلغ بهما التعب هذا المبلغ».

وراح بيدزوس، في غضون ذلك، ينظم حملة معارضة لخوارزمية التوقيع الرقمي على جبهات أخرى. فقد تلقت المؤسسة القومية للمعايير والتكنولوجيا، رداً على الإعلان في المدونة الفيدرالية يوم 30 آب/ أغسطس، تعليقات على الخطة، ومعظمها كانت انتقادات. وكانت الشركات التي تستخدم الخوارزمية «رسا»، ومنها مايكروسوفت ولوتس، قد أزعجها أن تجد استثماراتها في هذه الخطة تذهب هباء، وأن تضطر لتطوير برمجيات جديدة للمعيار الجديد. وكان ثمة انتقادات أخرى موجهة لبطء معدل سرعة عملياتها الحسابية. كذلك اهتم النقّاد بضعف مخطط خوارزمية التوقيع الرقمي. لأن المعيار المقترح لا يستخدم سوى المفاتيح من 12 بت لحساب التواقيع (تستخدم رسا 1024 بت) كان ثمة شك بقدر الكومبيوتر الضخمة في السياج الثلاثي على أن تطرح توقيعات مزورة. وكيف يمكن لكائن من كان أن يؤكد أن توقيعاً ما صحيحاً في حين أن لدى وكلّ الاستخبارات الإمكانات للقيام بأعمال التزوير؟ وكان الأمر كله عند رون رايفست رمزاً لسياسة الحكومة عموماً. لذلك طرح سؤاله في مؤتمر عقد في واشنطن لعاصمة في عام 1992: «أيسياسة للشيفرة ينبغي على هذا البلد أن يأخذ بها؟ هل يأخذ برموز قابلة للتفكيك أم شيفرة عصية على الحل؟».

ومع أن الجدل لم يتطور إلى نقاش واسع بين الجمهور عامة، إلا أنه أثار مع ذلك حماس بعض جماعات الدفاع عن الحريات المدنية التي كانت تراقب عن كثب العلاقة بين وكالة الأمن القومي، والمؤسسة القومية للمعايير والتكنولوجيا. والحق أن ميزان القوى بين الهيئتين، كان مدعاة للسخرية، فهذه سفينة القيادة لعملياتنا الاستخباراتية بميزانية عدة بلايين من الدولارات والأخرى

مخزن متواضع من مخازن الحكومة. ولئن كان الليبراليون، والمتحررون، يأملون من هذه المنظمة الأخيرة، أن تقوم بحماية مصالح المواطنين العاديين، فإن ثقتهم بأن تتمكن المؤسسة من تحقيق هذا الأمل كانت ضعيفة.

وكان للمخاوف التي تراود هؤلاء ما يبررها. فإن ألقى المرء نظرة على تاريخ هاتين المنظميتين، وجد أمامه صورة لاختلال موازين القوى. فبعد جلسات لجنة السيناتور تشيرش في السبعينات شعرت وكالة الأمن القومي أن تنظيمها كله لم تبرأ ساحتها بل عوقب. ولكن الحكومة أخذت تبدي في عام 1984، في ذروة سلطة رونالد ريغان في الثامنة، ما ينم عن عودتها إلى عالم السياسة لداخلية. فبناء على طلب واضح من فورت ميد، أصدر الرئيس ريغان توجيهاً يتصل بالأمن القومي برصد قواعد البيانات لمعلوماتية داخل الحكومة وخارجها والتي تقع في حيز المعلومات «الحساسة» ولكن غير السريّة، سواء كان مصدرها الحكومة أم غيرها. وقد أدى هذا إلى إثارة استياء شديد. وفي النهاية قام النائب عن تكساس جاك بروكس، خصم وكالة الأمن القومي في الكونغرس، بتوجيه أسمى النقد إلى الوكالة؛ فقال في إحدى جلسات الاستماع: «إن قلوبنا البيضاء والغرفة الخلفية في لبتاغون ليسوا بالأماكن التي ينبغي أن تُرسمها سياحة للبلاد». وكان أن تراجعت الحكومة وانسحبت من الساحة.

ولقد حملت هذه لتجربة بعض أعضاء الكونغرس، مدفوعين بضغوط من جماعات حماية الحريات المدنية، على وضع قانون يرسم الحدود للحكومة في عصر الكمبيوتر. فأصدر الكونغرس في ما كان تصرفاً غير مألوف يعبر عن استقلاله عن مطالب وكالة استخباراتية، قانون أمن الكمبيوتر لعام 1987 الذي أحال مسؤولية حماية أمن البنية التحتية للكمبيوتر، وخاصة بما يتصل بتزكية المعايير التي ينبغي على هذه لصناعة أن تلتزم بها، من وكالة الأمن القومي إلى المكتب القومي للمعايير حصراً (وكان على وشك أن يتخذ الاسم الذي يدل على ارتفاع المكانة، وهو المؤسسة القومية للمعايير والتكنولوجيا).

والسؤال هو، إذن، لماذا كان تنديد الكونغرس بأشباح وكالة الأمن القومي؟ حقاً أن جماعات الدفاع عن الحريات امدنية قد مارست ضغوطاً شديدة على دوائر الكونغرس. ولكن الأهم، على حد قول مارك روتنبرج، وكان يومئذ مستشاراً للسياتور باتريك ليهي، «إن الفعالية التجارية الأمريكية لم تكن لترتاح، إلى تولي وكالة الأمن القومي وضع المعايير. فالمخاوف التي تراود وكالة الأمن القومي بشأن أمن الكومبيوتر ليست المخاوف ذاتها التي تواجه التجارة - فالفعاليات التجارية لم تكن لتقلق بشأن الكرملين، وإنما ما كان يقلقها هم المنافسون».

ولما لمس المشرعون تأييد رجال لصناعة تحركوا بسرعة وباتت وكالة الأمن القومي، عاجزة عن اللحاق بمجريات الوضع. بل ما كان حتى لظهور الفريق وليم أودم مدير الوكالة يومذاك أن يمنع صدور القانون. أما شكواه من أن إحالة مسؤوليات أمنية إلى جهة مدنية «ازدواج» للوظائف لا ضرورة له فقد فاته فيها إدراك المقصود، وهنأ أصحاب الصناعة يؤثرون أن تتولى وزارة التجارة، لا الجواسيس، وضع المعايير للبنية التحتية للكمبيوتر التي تستخدمها القاعدة العريضة من الشعب. وكما ذكر أحد مسؤولي الوكالة لاحقاً في مذكرة له: «لقد استغرقنا وقتاً لاستيعاب المقصود... كان [النائب جاك بروكس] قد تمكن من حشد التأييد بالإجماع، للقرار بالشهادة والتصويت».

لم تستبعد «القلعة»، من عملية ضبط أمر الأمن، للحواسيب المصنعة في البلاد كلياً. ذلك أن الوكالة كانت تتمتع بخبرة لا تقدر بثمن، في مجال الأمان، فهي عاصمة الكريبتو في العالم بلا منازع، ولذلك فإن الكونغرس رسم لفورت ميد دوراً بأن أناط بها مهمة القيام بدور استشاري إلى جانب المؤسسة القومية للمعايير والتكنولوجيا. وكان السؤال كيف يمكن للمؤسسة والوكالة أن تعمل معاً؟ في المفاوضات التي جرت لتحديد أسلوب العمل تلخذ مندوبو الوكالة مقاعدهم مقابل مدير المؤسسة لمكلف، وكان بيروقراطياً يدعى رايموند

كرامر. ولم يكن كرامر هذا عطوفاً على وكالة الأمن القومي وحسب، بل كان في الواقع ابن اثنين من قدامى الموظفين فيها! حقاً إن مذكرة التفاهم، التي توصلت إليها المؤسسات قد حافظت على التصور بأن تقود المؤسسة عملية وضع المعايير، إلا أنها صاغت للوكالة دوراً رسمياً في كافة القضايا التي تتصل بالخوارزميات وتقنيات الشيفرة، كما ورد في المذكرة، وعلى المؤسسة القومية للمعايير والتكنولوجيا أن تطلب معونة وكالة الأمن القومي في هذه الأمور. ولتنفيذ هذا البند تعين على الهيئتين أن تتعاونوا معاً عبر «مجموعة عمل فنية». ولئن كان يفترض بأن تتولى المؤسسة مسؤولية العملية إلا أنها لم تكن تتمتع بالأغلبية في المجموعة التي كانت تضم ثلاثة أعضاء من كل هيئة.

ومع أن كلاً من الهيئتين كانت تؤكّد أن القيادة هي حقاً للمؤسسة القومية، إلا أن أهل الريبة كانوا يشككون في هذا القول. وفجأة أصبحت للمؤسسة القومية للمعايير والتكنولوجيا حتى مع اسمها الطنان الجديد المتذمر الحصيف في الحكومة، وسط معركة سياسية وأمنية قومية ضخمة. وقد اعترف واحد على الأقل من كبار المسؤولين في وكالة الأمن القومي، في ما بعد بأن المؤسسة القومية للمعايير والتكنولوجيا لم تسع إلى امتلاك السلطات التي منحها إياها قانون الأمن ولا رغبت فيها بعد إقرار القانون، وعلى حد قول هذا المسؤول لقد وضعتنا في موضع المسؤولية عما لم نكن نرغب في تحمّل مسؤوليته».

ولقد بدت المناوشات حول معيار التوقيع الرقمي، أكبر برهان على تبعية المؤسسة القومية لفورت ميد [وكالة الأمن القومي]. وقد جاءت التحقيقات في السنوات اللاحقة هداً على ذلك؛ وهناك تقرير من مكتب الحسابات العامة نطالع فيه خلاصة [تجربته] التي جاء فيها أن المؤسسة على العكس من القصد الذي شاء الكونغرس «تتبع أثر وكالة الأمن القومي في تطوير معايير تشفيرية معينة». وتوضح الوثائق التي كُشف النقاب عنها وتعرض للمناقشات

التي كانت تدور في الاجتماعات الشهرية لمجموعة العمل الفنيّة هذا بجلاء . وتظهر أن جماعة المؤسسة القومية كانت تنتظر حكم وكالة الأمن القومي في كل خطوة تتعلّق بموضوع التوقيع .

بل لقد عانت مجموعة الرقابة لتابعة للمؤسسة القومية للمعايير والتكنولوجيا ذاتها، وهي مجلس سلامة وأمن نظام الكمبيوتر، من مشكلات حادة كانت تعترض العلاقة بين الهيئتين . ففي آذار/ مارس 1992 رأى هذا المجلس أن مراجعة علنية على المستوى القومي للأثار الإيجابية والسلبية لانتشار استخدام المفتاح العام والخاص في التشفير تت ضرورية». غير أن وكالة الأمن القومي التي لم تكن ترغب في مناقشة أو عرض الموضوع تمكّنت من القضاء على هذه الفكرة . وقد عبّر مدير وكالة الأمن القومي المعين حديثاً، الأدميرال مايك مك كونيل في مذكرة سرّية، عن هذا الوضع بصراحة لا لبس فيها، إذ قال: «إن لدى وكالة الأمن القومي تحفظات فيما يتصل بإجراء نقاش علني حول الكريبتوجرافيا» .

ومع ذلك فقد بدأت الحكومة تستشعر بعض الضغط . وعاد النائب جاك بروكس إلى عقد جلسات الاستماع من جديد . فقدم فيها منتقدو وكالة الأمن القومي شهادات محرّجة . فقد أدلى ناتان مرفولد من مايكروسوفت بشهادة ذكر فيها إن نشر الحكومة معيارها للتوقيع المقترح، بما حفل من عيوب فنيّة . . . جعل من المستحيل على صناعة الكمبيوتر، أن تعتمد المعيار الذي وضعته الحكومة في أغراض التجارة». أما أديسون فيشر، وهو من أوائل المستثمرين في شركة آر إس إيه داتا سيكيوريتي، وقد سبق له أن استخدم خوارزميات الشركة في منتجات الكمبيوتر الضخم في شركته الأم أورد في شهادته تعبيراً قوياً قدر له أن يتردّد في المقامات التالية؛ إذ قال: «إن الكريبتوجرافيا وخاصة ما يتصل منها بالمفتاح العام باتت الآن في صميم التيار . إنها ببساطة جني آخر

من سلالة جن التكنولوجيا، وهو شديد النفع ولا يمكن إعادته إلى المصباح، وإن كانت له بعض الآثار الجانبية المنفّرة».

لقد كان لكل هذا النقد، وقع الموسيقى على أذني جيم بيدزوس. ومع أنه غدا فارساً مدافعاً عن حرية التشفير، فقد كان هدفه الرئيس على الدوام تدعيم شركته. وكان مذهبه أن عملية المعايير، ربما سارت في النهاية حسب هواه، إذا ستمرا لضغط على الحكومة وتابع التهديد، باستخدام براءة اختراع شنور في المعركة، ضد مرشح الحكومة، فتفوز تقنيات الخوارزمية رسا بالموافقة، على اعتبارها معيار التوقيع الرقمي رسمياً.

ثم، تراجعت للحكومة. أو هذا ما بدا على الأقل.

وحسب رواية جيم بيدزوس، كانت الحكومة قد توصلت في النهاية إلى نتيجة مفادها أن المعيار الذي أخذت به سوف يسقط ليس لاعتبارات تتصل بالشيفرة وإنما لأسباب تتعلق ببراءة الملكية الفكرية. وفي اجتماع عُقد في حزيران/ يونيو 1993 في وزارة التجارة، سمع بيدزوس محام يمثل المؤسسة القومية للمعايير يقول ما كان يتوق دوماً لسماعه: «إننا نودا لتعاون وإياكم». وتابع المحامي كلامه وبيدزوس ومحاموه يصغون مذهولين: «لم لا تقدمون لنا عرضاً لاستغلال الترخيص إذا شئتم تعويضاً؟».

فقال بيدزوس أنه سوف يبلغهم رده خطياً. وبدأت المفاوضات، مع تقديم الحكومة عرضاً مالياً سخياً للتعويض لبليك كي بارتنز: احتكار الحكومة لبراءة التوقيع الرقمي، أي حق استخدام حكومة الولايات المتحدة لخوارزمية التوقيع الرقمي معياراً مقابل منح الشركة ببليك كي بارتنز نسبة من العائدات. وقدرت هذه النسبة بدولار واحد عن كل مستخدم. ولما كان هذا الاتفاق يعد بملايين الدولارات من العائدات، إذ يتحتم على كل مواطن أن يستخدم هذا المعيار في مراسلاته مع الحكومة في كل أمر بدءاً من إبرام العقود إلى الإفادات الخاصة بالضرائب، فإن ثمة حافزاً كبيراً يحمل بيدزوس على قبول

العرض . وهذا ما كان . وكان يتصرف بهذا المعنى على أساس الحد الأدنى الذي تقبل به الشركة ، وضد مصالح الجمهور الواسع من الناس . فشركته سوف تصبح في النهاية ، شريكاً في استخدام منتج لوكالة الأمن القومي كمعيار ، خوارزمية عرض بها بيدزوس ذاته علانية .

أخذ البعض يتساءل يومذاك ، إن لم تكن استراتيجية الآراس إيه في حماية الشيفرة ببراءات الملكية الفكرية ذاتها طريقاً إلى عرقلة تقدم الحرية الشخصية في استخدام الكمبيوتر . ولربما كان بيدزوس ذاته متحالفاً مع أشباح الظلام ، جواسيس وكالة الأمن القومي . ففي النهاية ، «كان أهداف في نظام براءات الملكية الفكرية التشجيع على استثمار التكنولوجيا . . . ولقد مضى على ابتكار كريبتوجرافيا المفتاح العام عشرون عاماً ، ومع ذلك لم يقدر له أن ينتشر . ولو قام المرء بزيارة مخزن كبير ، سوبر ماركييت ، ووقف عند الصندوق لما وجد توقعات رقمية . فلماذا؟» ، كما لاحظ أحدهم .

لكن الصفقة لم يقدر لها أن تنتهي . ذلك أن الحكومة في استعجالها الانتهاء من معركة براءة الملكية الفكرية لم تقدر الثورة التي ستجتم ، عن نكو صها عن التزام سبق أن قطعه بتوزيع الخوارزمية مجاناً . ولما طلبت التعليق على الصفقة كانا لنقد الذي صدر شديداً ، حتى أن النقاد وصفوها بهبة من بليونى دولار تقدم لجليك كي بارتنرز . كذلك ألمحت للحكومة الكندية ، والمفوضية الأوروبية بأنهما ستمتعان عن دفع العوائد ، ولتذهب براءات الملكية الفكرية التي تدعي الحكومة الأمريكية ملكيتها إلى الجحيم . فكان هذا تمرداً لم تكن حكومة الولايات المتحدة بحاجة إلى مواجهته . وهكذا كان أن تراجعت المؤسسة لقومية للمعايير والتكنولوجيا عن العرض الذي قدمته لبيدزوس وأعدت تأكيدها أن المعيار الذي سوف تعتمد عليه سيكون دونما عائدات . وهكذا عادت الأمور إلى نقطة البدء في موضوع معيار التوقيع الرقمي .

ولقد قابل بينوس هذا التحول بروح فلسفية ، وليم سف لخسارة كل

تلك الأرباح، الضخمة المتوقعة بفضل هذه الصفقة. لكن الخطة فشلت. وما كان كان، وأصبح بوسعه أن يعود مرة أخرى إلى صف الملائكة، خصماً لحكومة تسعى، إلى القضاء على حرية الفرد الشخصية، ولو أدى ذلك إلى إفقار شركات البرمجيات الأمريكية.

وكان مقدراً للجدل بشأن معيار التوقيع، أن يستمر عاماً آخر. ولم تحسم المؤسسة القومية للمعايير أمرها، وتستقر على خيارها النهائي إلا في كانون أول/ أكتوبر 1994. فشاءت أن تصرف النظر عن موضوع براءة الملكية الفكرية وتتجاهل رد الفعل السلبي الهائل من الجمهور الواسع وتركيزه خوارزمية التوقيع الرقمي مرشحاً ليكون المعيار الرسمي للتوقيعات الرقمية. فذكرت في نشرة حقائق المؤسسة أنها «راجعت كافة براءات الملكية الفكرية وخلصت إلى أنه لن يكون هناك تجاوز على أي من الحقوق المترتبة على الملكية». (ولطمانة أولئك الذين ما تزال تراودهم الشكوك، اتخذت المؤسسة خطوة استثنائية بتحمل المسؤولية عن أي شخص يستخدم المعيار إذا ما تعرض لاحقاً للمقاضاة لانتهاكه قوانين الملكية الفكرية). ومع أن المؤسسة القومية للمعايير قد أجرت بعض التعديلات الفنية المفيدة التي تختلف عن عرضها الأصلي، وأبرزها تمديد طول المفتاح من 512 بت إلى 1024 بت. فإن النتيجة كانت نظام تثبت، ابتكرته سراً وكالة الاستخبارات الحكومية، نظام لم يجد فيه أحد شيئاً من الجاذبية ليأخذ به بديلاً لنظام معتمد ومطبق من مايكروسوفت وأبل وآي بي إم ونوفيل. فهل من عجب إذا ظل معيار التوقيع الرقمي يتيماً لا يوجد من يتبناه حتى بعد انقضاء الأعوام؟ وألا يوجد حتى في غمرة ازدهار صناعة الإلكترونيات وسيلة عامة للتثبيت في البريد الإلكتروني؟

والمضحك في الأمر، كما قال العالم لين مك نلتي في المؤسسة القومية للمعايير والتكنولوجيا: «قد كنا نعتقد أن التوقيع الرقمي أمر يسير». لكن معركة التوقيعات، على ما يبدو، رغم ما كانت عليه من الشدة، لم تكن سوى تمرين «إحماء» للحدث الرئيس في حرب الكريبتوجرافيا: حرب التشفير.