فوضى التشفير

عندما بدأ فيل زيمرمان مغامرته في الكريبتو جرافيا، لم تكن لديه أدنى فكرة بأنّه سيغدو بطلاً شعبياً، وفي الوقت نفسه سيخضع للتحقيق لانتهاكه القانون الفيدرالي. فقد قام بهذه المغامرة بدافع من فضوله العلمي، وولع الهاوي، وشيء من البارانويا السياسية. ولد زيمرمان عام 1954، وترعرع في عدد من مدن ولاية فلوريدا، ووصف نفسه «لست بطبعي شخصاً يهوى الحفلات». وكان شخصاً انعزالياً غريب الأطوار. ووالده سائق شاحنة؛ كذلك كان والداه يدمنان الكحول. أما هو فكان يطمح إلى أن يصبح عالم فلك. وعلى الرغم من أنّه كان ما يزال في الصف الرابع الابتدائي، فقد استهوته الرموز حتى ملكت عليه عقله. وكان تلفزيون ميامي قد دأب على بثّ برنامج يدعى إم. تي. جريفيز وسجن المغارة، في فترة الظهيرة من كل يوم سبت، وكان يضم ناد للأطفال، ويباع لأعضاء النادي «مفتاح كالمفاتيح العادية لتفكيك رموز سرّيّة؛ وفي البرنامج كان يتم عرض عدد من الأرقام تظهر على الشاشة بشكل ومضات، وعلى أعضاء النادي ترجمتها باستخدام المفتاح لتغدو رسائل سحرية واضحة. ولم يشتر زيمرمان المفتاح قط، إلاّ أنه، قام بتدوين الأرقام على عجل واستطاع أن يحل الشّيفرة لتصبح نصاً بسيطاً واضحاً. فبالنسبة لطفل وحيد لعائلة مضطربة، كان تحويل هذه الرموز الغامضة إلى ما

هو مفهوم قد منحه إحساساً بالتفوّق، والانتماء. والإحساس ببيت منظم.

فلا عجب إذن إن يسعى الفتى لمعرفة المزيد عن الشّيفرة. وكان أن وقع على كتاب من تأليف هيربرت اس. زيم، وهو كاتب للأطفال، عنوانه «الرموز والكتابة السرّيّة»، من منشورات دار سكولاستيك ليكون في متناول الأطفال بين سنّ العاشرة والاثنتي عشرة سنة. وهذا الكتيب نقل بطريقة مباشرة متعة الكريبتوجرافيا، وكأنما الكاتب موظف رفيع في المخابرات يقوم على تدريب مجنّد ذكي، إنما غرّ. وقد كتب زيم قائلاً: «ليس القصد من هذا الكتاب إعطاؤك رموزاً لتنسخها، بل مساعدتك على ابتكار رموز خاصة بك، لا رمزاً واحداً أو رمزين، بل المئات منها، إن شئت، أما كيفية استخدام معرفتك بالرموز فأمر هو من شأنك».

لقد غدا هذا الكتاب، منذ ذلك اليوم، كتاب زيمرمان المقدس، وقام بحل كل ما فيه من التمارين، بكل أمانة وإخلاص، مثل صنع حبر سري من عصير الليمون، وابتكار شيفرات أصيلة، وبالطبع تفكيك الرسائل المشفرة في الكتاب. وبعد عامين، عندما كان في المرحلة الإعدادية، تباهى زميل له بشيفرة كان قد ابتكرها، وأن أحداً لن يستطيع حلّها، إلاّ أن زيمرمان قَبِل التحدي. وقال لزميله: «احرص على أن تجعلها رسالة طويلة». فاستجاب الفتى، معتقداً عن حمق أن رسالة طويلة ستكون أصعب حلاً. كانت الرسالة مكتوبة بأسلوب رموز الكتابة الرونية [أبجدية تيوتونية قديمة وعلامات تنطوي على معنى خفي أو سحري. هـ. م]، وتذكر بشكل ضبابي باللغات التي تشيع في رواية توليكين: «مملكة الأرض الوسطى» [عمل شهير من أدب الخيال العلمي]. قام زيمرمان بتحليل الرسالة ونهج في ذلك منهج تحليل تكرار الرموز، وهو أسلوب بدائي في تحليل الشّيفرة يقتضي ببساطة حساب عدد المرّات التي تظهر فيها الأحرف الأبجدية. وذلك ما مكّنه من حلّها، وكأنّها نص مشفّر عادي. فكان هذا الإنجاز مدعاة لدهشة صديقه كثيراً.

انحسر اهتمام زيمرمان بالشّيفرة، في سنوات المراهقة، ولم يدرك أن الكومبيوتر، يمكن أن تستخدم بوصفها أدوات تشفير حتى التحق بجامعة فلوريدا أتلانتيك. وعلى الرغم من أنّه كان متخصصاً بالفيزياء، إلاّ أن الأمر انتهى به أن أصبح يقضي معظم وقته في غرفة الكومبيوتر، ففي البدء قام بأعمال تتعلّق بتخصّصه، ولكن في النهاية راح ينهل من إكسير البرمجة ذاتها. وكان ما يجذبه إلىٰ ذلك ابتكار عالمه الخاص في الجهاز. إذ يقول: «يمكنك أن تتفاعل مع قطعة جماد، شيءبلا حياة، إلاّ أنه يبدو كذلك في ظاهره». وأجمل ما في ذلك أنه يجيده، بعكس كفاءته في الفيزياء. أما خصمه الرهيب فكان: حساب التفاضل والتكامل.

بالرغم من أنّه بدأ العمل بالترجمة منذأ سبوعه الأول في الجامعة عام 1972، إلاّ أنه لم ير كومبيوتراً حقيقياً طوال عامبا كمله، ذلك أن كليته كانت تمتلك محطات تتصل بآلات بعيدة فقط. فجا معة فلوريدا أتلانتيك ليست معهد ماسشوسيتس للتكنولوجيا أو جامعة ستانفورد. أو حتى جامعة حكومية ضخمة. ثم أصبح زيمرمان طالباً مساعِداً، يعلّم الآخرين استخدام المحطات. وترك الفيزياء ليختص بعلوم الكومبيوتر.

وفي غرفة الكومبيوتر تلك، استعاد شغفه بالشّيفرة. وقد اقتضت إحدى تجاربه، كتابة رمز سرّي خاص به، مستخدماً لغة الفورتران المستخدمة في الكومبيوتر والتي باتت منسقة الآن. واستخدم في مشروعه مجموعة من الأرقام العشوائية لاستبدال كل حرف في النص الواضح للرسالة بحرف آخر. وجعل عمل الأرقام العشوائية يرتبط بمفتاح هو عبارة عن كلمة سرّيّة. ولما كانت رموزه لا يمكن حلها باستخدام التحليل الترددي (عمل العشوائية يقوم على تغيير حرف مثل التاء t الذي يظهر في بداية الرسالة إلىٰ حرف ما أما أحرف ا لتاء اللاحقة فتستبدل بحروف أخرى). وظن زيمرمان أن وكالة المخابرات المركزية CIA ذاتها، عاجزة عن أن تحل هذه الرموز. فهو لم يكن ليتخيّل أبداً تقنيات

مثل الهجوم على نصّ واضح منتقى، أو تفكيك مولدات الأرقام العشوائية. (ولم يسمع قط بوكالة الأمن القومي). ولكن كان من المقدّر له أن يتصدّى لتلك الشّيفرة المنيعة ذاتها بعد سنوات حينما عرضت له في وظيفة مدرسية على أنّها شيفرة يمكن حلّها بسهولة باستخدام تقنيات أساسية في تحليل الشّيفرة. ويتحدّث عن ذلك بقوله: «وهكذا كانت نهاية مخططي الباهر».

في صيف عام 1977، كان زيمرمان يعمل ـ في ذلك الحين ـ في شركة لصناعة أجهزة الكومبيوتر الصغيرة في فورت لودرديل، ولم يكن قد بقي على تخرجه يومذاك سوى فصل دراسي واحد، وفي أثناء ذلك قرأ مقالاً نُشر في عمود ابتكارات رياضية في مجلة العلوم الأمريكية، وصادف أمراً أخذ بلبه. وكان ذلك بالطبع وصف مارتين جاردنر للمفتاح العام وخوارزميتو سا. ولما كان متعطشاً لمعرفة المزيد، اتصل برون رايفست في معهد ماسا تشوسيتس، على نحو غير متوقع، وسأله عن إمكانية تطبيق النظام على الكومبيوتر. فأفاده رايفست بأن فريق معهد ماسا تشوسيتس قام ذلك بأجهزة ليست LISP [لغة برمجة لمعالجة القوائم. هـ. م.] أثناء اختبارهم للغة صوتية للكومبيوتر، تستخدم في الذكاء الصناعي. فقال له زيمرمان وقد شعر بخيبة الأمل: «إن ذلك يتجاوز طاقتي». إذ لم يكن لديه القدرة على الحصول على أجهزة الـ ليسب المبهرة؛ فهي أدوات باهظة الثمن، تبلغ تكلفتها مئة ألف دولار، صممت لأغراض البحث، وليس لأداء مهمات عملية مثل الأعمال الحسابية. وعلى الرغم من أن زيمرمان لم يكن ضليعاً بعلم الحساب، إلاّ أنه أدرك أن احتمال حصوله على جهاز ليسب في جامعة فلوريدا أتلانتيك تكاد تكون معدومة. إلاّ أنه أخذ يفكّر في إمكانية تطبيق الخوارزمية رسا على تلك الكومبيوتر الصغيرة الحجم والرخيصة. فالأمر هنا مختلف. كان زيمرمان يمتلك حصة صغيرة من واحد من تلك الأجهزة الصغيرة الرخصية الثمن المستخدمة حينذاك، والتي تصدر ضجيجاً وتعمل على معالج يدعى زيلوج زد ـ 80 Zylog Z-80 وهو نوع

من النموذج آ Model A كان مستخدماً في منتصف السبعينات. لكن بينما كان يفكّر في أمر تطبيق خوارزمية رسا، أدرك أنّه لا يعرف إلاّ القليل عن كيفية القيام ببعض لعمليات الحسابية المطولة المملّة التي تم شرحها في ورقة بحث فريق ملما تشوسيتس ولذلك تخلّى عن المحاولة.

في ذ لك الوقت كان ثمة أمور أخرى، تجري في حياة زيمرمان. ففي السنة ذاتها التي اكتشف فيها الرسا، تزوج صديقته كيسي كافانو التي كانت عاملة مقسم في الكلية، وبعد فترة ليست بالطويلة، قام الزوجان بزيارة أصدقاء لهما في بولدر بولاية كولورادو، فأحبّا المنطقة كثيراً. ولما عاد زيمرمان إلىٰ عمله في فلوريدا، راح يخطّط للانتقال إلىٰ تلك المنطقة. وبعد سنة حزم وكيسي أمتعتهما واستقلا سيارتهمالفو كسفاكن الصغيرة، وانطلقا إلىٰ جبال روكي. وهناك حصل على عمل في شركة للبرمجيات لتصنيع محطة عمل معالج نصوص، وبدأ بتكوين عائلة: فقد ولد أول أبنائهما في عام 1980. ثم استمع إلىٰ دانيل إلسبورج وهو يتحدث إلىٰ حشد في دينفر [ولاية أوهايو هـ. م] عن مناهضة التجارب النووية.

كان فيل زيمرمان، قد تجاهل في مرحلة دراسته الثانوية، حرب فييتنام إلىٰ حد كبير. ولكن عندما درس في جامعة فلوريدا أتلانتيك أخذ يتبنّى موقفاً سلبياً من للحكو مة مناهض لها أشد ما تكون المناهضة. إذ أن فضائح نيكسون فتحت عينيه وكشفت له مبلغ الصفاقة التي يمكن للحكومة أن تبلغها في الكذب. ولما كانت رئاسة رونالد ريغان بلغ به الإستياء من السياسة حداً كبيراً. وكان قد قرأ كتاب روبرت شير With Enough Shovels، وانتابه قلق من احتمال إبادة البشرية بالقنبلة الذرية. فقرّر زيمرمان وزوجه أن يرحلا إلىٰ نيوزيلندا، إذ وجدا أنه من الحكمة أن يتجنّب المرء المحرقة المقبلة. وبلغ بهما الأمر حد الحصول على جوازات سفر وتجهيز أوراق الهجرة (لم يكن يعلم بعد أن صناعة الكومبيوتر في نيوزيلندا لم تكن ذات شأن). وفي عام 1982، حضر الاجتماع

الجماهيري الذي أُقيم في تلك السنة، واستمع إلىٰ إلسبورج، الذي أصبح من كبار الناشطين في منا هضة النشاطات النووية، بعد اللحظة المشهودة التي نشر فيها «وثائق لبنتاغون». وهكذا انخرط زيمرمان في هذا التيار. ومنذ تلك اللحظة، نسي أمر الهجرة وقرّر أن يصبح ناشطاً سياسياً، وأن يبقى ويقاتل.

كان زيمرمان وبعض أصدقائه، يقومون بتأسيس شيفرة، تدعى ميتا فوريك سيستمز، وقد عزموا على إنتاج لوحة مثبت عليها دارة كهربائية لأجهزة أبل التي تعمل على تشغيل برامج متوافقة مع إينتل. لكن زيمرمان استطاع أن يجد الوقت ليبحث في كل كتاب يقع عليه في موضوعات سيا سة الحلف الأطلسي، ومنظومات الأسلحة... إلخ وكان ينفق مئات الدولارات في مكتبة واحدة ويمضي الوقت بحثاً وتنقيباً في الكتب. وأخذ بعدئذ في تدر يس السياسة العسكرية في الجامعة الحرة في بو لدر. وتحدّث في الاجتماعات الجماهيرية المناهضة للتجارب النووية وعمل مستشاراً لاثنين من المرشحين لعضوية الكونغرس، واعتُقل مرتين لمشاركته في تلك التجمعات. وفي إ حدى المرات اعتُقل في المنطقة المخصّصة لإجراء التجارب الذرية في صحراء نيفادا، جنباً إلىٰ جنب مع بطليه إلسبورج وكارل ساجان. (إلاّ أنه لم يوجه إليه اتهام في كلتا المناسبتين).

مع مضي عقد الثمانينات، بدا أن حركة منا هضة التجارب النووية أخذت تفقد زخمها. كذلك فإن شركة ميتافوريك سيستيمز لم تكن تبلي بلاء حسناً: فمنذ أن أصبحت لكومبيوتر آي بي إم الشخصية هي المسيطرة، با تت فكرة وضع معالجات إينتل، لكومبيوتر آبل ـ 2 ضرباً من السخف. وكان ذلك مدعاة لاضطراب زيمرمان نوعاً ما. إلاّ أن كل شيء تغيّر بعد اتّصال هاتفي تلقاه من مبرمج يعمل في أركنساس، ولديه مشروع ما من أحد يقدره أكثر من فيل زيمرمان وقلّة قليلة من الناس.

كان هذا الشخص يدعى شارلي ميريت، واتضح أنّه كان في الواقع يقوم

بالشيء الذي حلم به زيمرمان، منذ أن طالع مقال مارتين جاردنر في عام 1977: إذ كان يطبق الخوارزمية رسا في نظام المفتاح العام للتشفير على أجهزة كومبيوترات صغيرة الحجم. ذلك أن رد فعل ميريت كان يشبه رد فعل زيمرمان عندما قرأ عن الإنجاز الذي قام به الباحثون في معهد ماساتشوستس للتكنولوجيا (إم آي تي). وقد انتقل ميريت من مسقط رأسه في هيوستن (تكساس) إلى فايتفيل في أركنسا س، وهناك أسّس وعدد من أصدقائه شركة، وبالفعل استطاعوا وضع برنامج مفتاح عام يعمل على كومبيوتر من نوع زد-80. كان البرنامج يعمل ببطء شديد، إلاّ أن الابتكار نجح. لكن لم يكن هناك من يريد شراءه. وهكذا، بعد فترة من الزمن، انسحب أصدقاؤه جميعاً من الشركة، وبدأ ميريت وزوجته بتسويق البرنامج بأنفسهما. وفي النهاية وصلت أنباء مشروعهما التجاري الصغير إلى العمليّة الاستخباراتية في فورت ميد التي أنفق عليها بلايين الدولارات. كانت وكالة الأمن القومي ترسل مبعوثيها دورياً إلى أركنساس لتحذير ميريت من العواقب الوخيمة التي قد تحدث إذا ما صدر برامج مشفّرة خارج البلاد. ولما كان معظم زبائن برمجيات ميريت شركات تعمل وراء البحار وتنشد برامج تشفير تمنع عملاء الأنظمة الفاسدة المتنصتين، فإن هذا القيد جعل الشركة تغلق عملياً. وفيما لو سمح ميريت، للحصول على بعض الحلول من داخل البلاد اضطر للاتّصال بشركات مغمورة كان قد قرأ عنها في المجلات المتخصّصة بأمل أن يرسلوا برامجه مع بضائعهم. وهكذا عثر على ميتا فوريك وفيل زيمرمان.

عندما سمع زيمرمان ما كان ميريت ينوي القيام به، شعر بسعادة غامرة حتّى حسب ميريت أن في الأمر خدعة: إذ لم يكن هناك أحد ممن قابلهم من قبل مفتوناً بالتشفير بمثل هذا القدر. وكان زيمرمان قد عبّر لميريت عن مقدار عشقه للتشفير، وعن أم تي جريفزو سجن لمغارة، وهيربرت زيم ورون رايفست. كذلك عبّر له عن كرهه للأخ الكبير، [رمز السلطة الشمولية في رواية

جورج أورويل الشهيرة 1984 هـ. م]. لكنّه أراد أولاً، أن يعلم كل شيء يعرفه ميريت حول جعل رسا تعمل على الكومبيوتر الشخصي.

والآن، بعد أن علم زيمرمان أن بالإمكان القيام بذلك، أصبح مدفوعاً لكتابة، برنامج لمفتاح العام للتشفير الخاص به، للناس عموماً. ففي حين كا نت جهوده السابقة في التشفير مجرد أعمال مأجورة، وتعبيراً عن شغفه بالرموز عموماً وحسب، إلاّ أنّه الآن أصبحنا شطاً سياسيّاً مثقفاً اعتُقل مرتين لتعبيره عن رأيه. كما يعلم أن الحكومة تمتلك في عصر الكومبيوتر أداة قوية لمراقبة المعارضة: ألا وهي الرقابة الإلكترونية. إذ لم يعد أمثال الأخ الكبير يقتصرون على التنصّت على المحادثات الهاتفية بآذانهم الكبيرة وحسب، ولكن بإمكانهم اقتلاع سائل البريد الإلكتروني من الأثير الرقمي وقراءةا لمشاريع التجارية والأسرار المخزية إرضاء لقلوبهم السوداء القاتمة. ففي حين كان البريد الإلكتروني أمراً رائعاً، إلاّ أنه في واقع الأمر مثّل خطوة إلىٰ الخلف فيما يتعلّق با لخصوصية: فحتّى بوجود البريد العادي غير الأمين نسبياً، كان الناس يقومون بإغلاق المغلفات لحماية سرية رسائلهم. والأمر الذي كان زيمرمان يأمله هو إنتاج المعادل الإلكتروني للمغلفات المغلقة. لكن إنأعطيت ا لناس برنامج تشفير لحماية البريد الإلكتروني، فسيكون لديك شيئاً أفضل من المغلفات المغلقة، وأعتقد، أنّه في حال وفق ا لناس جميعاً على استخدامه، فسيكون ذلك نوعاً من التضامن، حركة جماهيرية لمقاومة التنصّت المقيت. فإلىٰ الأمام، يا صاحبي!

ولما كان زيمرمان يعلم حدود سرعة المفتاح العام، فقد قدّر أن برنامجه، يجب أن يكون نظام تشفير هجين. بحيث يستخدم نظام المفتاح العام «لرسا» البطيء لتبادلا لمفاتيح، وبعض الخوارزميات السريعة الأخرى، لتشفير كامل الرسالة. وكان لا يعلم ببرنامج لوتس نوتس، الذي كان يطبّق مثل هذا النظام الهجين، وبالتأكيد، يجهل تماماً شركة آر إس إيه داتا سيكيوريتي. والتي ستبني

تجارة كاملة، تعمل بوجب ترخيص (مفتاح عام لتلك الأنواع من الأنظمة التي اعتقد زيمرمان أنّه كان رائداً فيها.) كذلك لم يكن لديه أي فكرة عن براءات الملكيّة الفكريّة عن ابتكار رسا. وعلى أية حال، لم يكن لدى أي من الشركتين منتجاً للشحن في عام 1984.

أدرك زيمرمان عدداً من الأمور على الوجه الصحيح؛ منها أن البرنامج المفيد يجب ألا يقتصر في عمله على نوع واحد من الكومبيوتر، وإنما ينبغي أن يكون متوافقاً مع كافة الأجهزة. ولذلك كان ينبغي أن يكتب بلغة كومبيوترية يمكن لجميع أنواع المعالِجات تعديلها، وكما يعلم المبرمجون فإن اللغة التي تلبي هذه الحاجة على أفضل وجه كانت لغة البرمجة سي C، ولحسن الحظ، أن زيمرمان كان يتقن هذه اللغة تمام الإتقان. كذلك يجب أن يكون البرنامج سهل الاستخدام، واسع الانتشار ومتاح في كل مكان وفي جميع الأوقات تقريباً، ويسهل فهمه بسرعة. وهكذا يصبح بإمكانه الإفادة من تأثير الشبكة.

كان شارلي ميريت يشكّل عائقاً إذ لم يسبق له أن تعامل مع لغة البرمجة سي، لكنّه كان قوياً في مجال كان زيمرمان ضعيفاً فيه على نحو يحمل على الأسى: وهو الرياضيات المعقدة التي تسمح للمرء بالتعامل مع الأعداد الضخمة التي تتطلبها خوارزمية رسا. وكان ذلك ضرورياً على نحو خاص لتطبيق الرسا على الكومبيوتر الشخصية، التي تستخدم «كلمات» مؤلفة من 8 بتات في حساباتها: وكانت العملية التي تنطوي على الكثير من التحدي هي تطبيق تلك الأعداد الصغيرة نسبياً، بطريقة يمكن بها معالجة الأعداد الضخمة التي تتطلّبها الرسا ـ والتي تصل إلى 512 بت، و1028 بت، أو حتّى أكثر من ذلك. وإذا لم تستطع القيام بذلك على نحو فعّال، فإن البرنامج سيعمل ببطء شديد لدرجة أن أحداً لن يُقبل على استخدامه.

على الرغم من أن الاتّصال الهاتفي، الذي أجراه ميريت بشركة ميتامورفيك لم يؤد إلى اتفاق تجاري فوراً، إلاّ أن المكالمات الهاتفية بينه

وزيمرمان، باتت أمراً مستمراً، وكان زيمرمان لا ينفك يسعى، للحصول على كل ما لميريت من معرفةبا لداول (التوابع) الحسابية المتعدِّدةا لدقيقة. وكانت عملية معقَّدة لدرجة أنَّهما قرَّرا ضرورة قدوم ميريت لزيارة زيمرمان في بولدر في شهر تشر ين الثاني/ نوفمبر 1986، وذلك لإقامة ما يشبه المعسكر يكرسانه، لدراسة المسائل الرياضيَّة بشكل مكثَّف.

ولقد كان أسبوعاً حافلاً بالأحداث، ولم يقتصر على الحساب الذي تعلمه زيمرمان. ذلك أن ميريت كان يعمل على مشروع لحسا ب البحرية، وهو إنتاج شيفرة تقليديَّة؛ قام بتعليمهاللشا ب الأصغر منه [زيمرمان]. وكان ميريت قد تعاقد بشأن هذا المشروع من الباطن، مع شركة كان يقدم لها المشورة؛ وكانت هذه الشركة هي شركة آر إس إيه داتا سيكيوريتي. وكان قبل سفره إلىٰ بولدر، قد اتصل هاتفياً بمديرها الجديد ليسأله عن إمكانية اجتماعهما في كولورادو، وهو مكان يسهل الوصول إليه، أكثر من فايتفيل بولاية أركنساس. فوافق جيم بيدزوس على ذلك.

كان بيدزوس يتطلع إلىٰ عشاء للتعارف بميريت مشحون بالانفعال، رجلان في مطعم يقدِّم شرائح لحم البقر، وهما يدخنان ويتبادلان الأكاذيب. إلاَّ أنه عوضاً عنذ لك وجد رجلاً ثالثاً انضم إلىٰ الاجتماع، وهو زيمرمان. وعوضاً عن مطعم يقدِّم شرائحا للحم انتهى بهم المقام في جود إيرث (الأرض الطيبة)، وهو متجر ضخم، تسطع فيه الأضواء ويقدِّم مختلف أنواع السلطة والبقول.

إن لحد يث الذي جرى في المطعم أصبح لاحقاً موضع خلا ف. وقال جيم بيلزو س فيما بعد أنه فوجئ عندما تحدَّث فيل زيمرمان عن خطته لابتكار برنامج يستخدم أنظمة تملكها شركة آر إس إيه. وفي الواقع كان لدى الشركة برنامجاً مشابهاً، كان بيلزو س يحمل معه نسختين عنه، ويدعى ميلسيف (البريد الآمن)، كتبه رايفست وأدليمان، الضليعان بالرياضيات والكريبتوجرافيا

ومعرفتهما بهذينالمو ضوعين تفوق بمراحل، ما استطاع زيمرمان الحصول عليه من مير يت خلال سنتين. ادّعى زيمرمان أن بيدزوس أُعجب كثيراً بخططه، لدرجة أنه منح المبرمج رخصة، للحصول على الخوارزمية رسا مجاناً. وقد أنكر بيدزوس لاحقاً، وبأعلى صوته أنه قدّم عرضاً كهذا.

لم ير زيمرمان أي مبرّر لعدوله عن خططه، فأمضى السنوات القليلة التالية، في توسيع معرفته بالكريبتوجرافيا بحيث يتمكّن من إتمام برنامج التشفير الخاص به. وكتب بعضاً من أفكاره في بحث نُشر في مجلة IEEE Computer، وهي مجلة مختصة بعلوم الكومبيوتر ذات مكانة رفيعة، وكان ذلك مدعاة لفخر زيمرمان، وهو نجاح يعتد به، لشاب تخرج من جامعة فلوريدا أتلانتيك.

وبعد ذلك، بدأ بالعمل لوضع البرنامج ذاته. ومن الخطوات الهامّة والحسّاسة التي قام بها إنتاج خوارزمية التشفير الإجمالية التي تقوم بتحويل نص الرسالة إلى رموز. وتحاشياً لاستخدام معيار تشفير البياناتو معيار آر سي ـ 2 RC-2 الذي تملكه شركة آر إس إيه واخترعه رون رايفست، أقدم زيمرمان على سلوك طريقمحفو ف بالمجازفات، وهو إنتاج الشّيفرة الخاصة به. كما نت مبنية على الشّيفرة التي علمه إياها ميريت، تلك الشّيفرة التي ابتكرها هذا لصالح سلاح البحرية. لكن زيمرمان جعل النّظام أكثر متانة عن طريق تقديم حلقات متعدّدة من الاستبدالات. وبينما كان يعمل على صقل فكرته، تذكّر فقرة قام بأدائها دان آيكرويد في برنامج تلفزيوني يدعى ساتورديناي يت لايف (البث المباشر ليلة السبت). وهذه الفقرة تمثّل بائعاً جوالاً من الباعة الذين يعملون آخر الليل تتدافع الكلمات من فمه رشاً، وكان آيكرويد ينادي على خلاط قوي جداً لدرجة أنهإ مكانك أن ترمي بسمكة فيه، وسيكون السائل الناتج عبارة عن عصير مفيد للصحة (يا لمذاقه اللذيذ). كان اسم ذلك الخلاط باس ـ او ـ ماتيك، فقال زيمرمان لنفسه، يا له من اسم مثالي لخوارزمية تشفير، إن أي

محلِّل للشيفرة يواجه رسائله المعماة، لا بدّ عاجز عن توضيحها، كما أمل، مثله في ذلك مثل من يحاول انتشال سمكة فضية اللون ضربت بقوة من المصيدة التي أنتجها خلاّط باس ـ او ـ ماتيك.

انتقل زيمرمان للاهتمام بمشكلا ت أخرى، استطاع حلّها جميعها كتنظيم الرسالة والسطح البيني ومجموعة من البروتوكولات. ولكن كل ما كان لديه بعد أشهر عديدة من العمل، مجموعة من المكونات منفصلة عن بعضها البعض، ولا تزال غير مترابطة، لا يجمعها برنامج عامل. وقد قال عن ذلك: «إن ربط هذه العناصر ببعضها البعض، يتطلّب عملاً وجهداً عظيمين». وبحلول عام 1990 ـ أي بعد ستّ سنوات من الزيارة التي قام بها ميريت إلىٰ بولدر. أدرك زيمرمان، أن عليه لكي ينجز مشروعه، أن يلتزم به التزاماً كاملاً، حتّى ولو كان ذلك يعني التقشف وضبط الميزانية، وأن يتوقف عن قيامه بتقديم المشورة، وقضاء و قت أقل مع أسرته. وباشر العمل بالبرمجة فوراً منقطعاً له ساعات طوال.

كان زيمر مان قد فكّر بإطلاق اسم معين علىا لعمل الذي يقوم به لكن ليس اسماً رناناً بلا وقار مثل باس ـ او ـ ماتيك. وكان زيمرمان من أوائل الرواد المخلصين لكومبيوترات ماكنتوش، وسبق له أنجرّ ب وضعبر نامج بسيط لاتّصالات البيانات، حين لم يكن قد ظهر أي منها بعد. وفيما كان يفكر خطر بباله Ralph's Pretty Good Grocery، العراب الخيالي في البرنامج الإذاعي A Prairie Home Companion الذي يخرجه جاريسون كيلور، ثم خرج باسم Pretty Good Terminal «محطة طرفية جيدة جداً» وقاده هذا إلىٰ تسمية برنامجه للشيفرة Pretty Good Privacy «منتهى السرّيّة» [أصبح يُعرف بالاسم المختصر P.G.P. هـ. م]. والحق أنّه لم يكن ليفكر جدياً بأن هذا الاسم يصلح لأن يكون علامة تجارية كبيرة. ولكن أي ضير في هذا، فلطالمكا نت مشاريعه التجارية مشوبة بالغموض. وكان يأمل في جني بعض المال، من بيع برنامجه منتهى السرّيّة،

بي جي بي .P.G.P لكنّه قدر أن الريعية ستكون متواضعة ذلك أن البيع سيكون وفق قواعد الحصول، على حصة من السلعة، وبموجبه يقوم الناس بتصريف البرنامج ويسدّدون الثمن، بموجب نظام الدفع عند الاستحقاق.

دأب زيمرمان على العمل طوال الأشهر الستة التالية، اثنتي عشرة ساعة يومياً في غرفة نوم في منزله، الذي كاد أن يخسره لأنه لم يكن لديه المال لتسديد أقساط الرهن. ولعله اعتقد، أنه حينما ينهي برنامجه ويطلقه في لسوق، فإنأ عداداً لا بأس بها من المستثمرين لهذا البرنامج سوف يرسلون له المال مما يمكنه من حل مشكلاته المادية. ولما شارف البرنامج على الانتهاء اتصل بجيم بيدزوس ليرى إذا كان بإمكانهم أخيراً تسوية موضوع الملكية الفكرية التي تطرّق إليها مدير شركة آر إس إيه خلال ذلك العشاء المشؤوم. وشرح له زيمرمان منتجه وطلب منه الإذن باستخدام الخوارزمية رسا. فدُهش بيدزوس لذلك الطلب: هل يعتقد هذا الرجل، أننا سنقدم له أغلى ما عندنا على طبق من فضة. وأشار على زيمرمان أنه ربما كان من الأجدى له، تصنيع منتجه لصالح إحدى الشركات الغنية التي تستطيع أن تحصل على ترخيص رسمي من شركةآر إ س إيه، بدلاً من التسول.

كا نتا لمحادثة برمتها، بعيدة كل البُعد عن رؤية زيمرمان لمُنتَجه، ونظرته القاتمة لعالم التجارة الضخمة، لدرجة أنّه أشاح عن المشكلة بأكملها، وانصرف إلىٰ عمله من جديد.

ولماأ طل عام 1991، كان زيمرمان يحرز تقدماً نحو تصنيع منتج نافع. ثم وقع ما جعله يسلك طريقاً غير الذي سلكه ـ وليجعل برنامج منتهى السرِّيّة شهيراً. كان العاملغير ا لمتوقع في هذا التحول، هو السيناتور جوزيف بايدن، رئيس اللجنة التشريعية في مجلس الشيوخ ومن المسلد ين في اقتراح التشريع المنتظر المتعلق بمكافحة الإرهاب وهو مشروع قانون مجلس الشيوخ رقم 266.

ففي مسودة المشروع المقدم في 24 كانون الثاني/ يناير، أدخل بايدن لغة جديدة:

إن الرأي السائد لدى الكونغرس، أن على القائمين بتأمين خدمات الاتّصال الإلكترونية ومصنعي تجهيزاتها، ضمان أن تمكن أنظمة الاتّصالات الحكومة من الحصول على النّص الواضح لمحتويات الصوت، والبيانات، ووسائل الاتصال الأخرى، عندما يتم إقرار ذلك قانونياً. [إضافة لتشديد].

كانت هذه إبرة مسمومة، في كومة قش من البنود والفقرات والقيود، ومع ذلك فقد أفلت هذا المقطع من التدقيق والتمحيص. لكن ظهوره لم يكن محض صدفة. ولا بد أن تكون لغة مشروع القانون، قد صيغت بمساعدة المؤسسات التي تعمل على حفظ النظام. وتم وضع هذه الجملة بناء على طلب صريح من مكتب التحقيقات الفيدرالي FBI. ويا لها من جملة! فلقد كانت بمثابة طعنة خنجر في قلب ثورة الشّيفرة. فكيف يمكن لشركات التكنولوجيا الخاصة أن تعد بتقديم محتويات النصوص الواضحة للنصوص المشفّرة إذا استخدم الناس لتشفيرها برامج مثل ميلسيف ولوتس نوتس وبي جي بي؟ فالرسائل الأصلية يراد بها أن يقرأها المتلقي المقصود. ومنطقياً، الطريقة الوحيدة التي يمكن بها إرضاء «الرأي السائد في الكونغرس» هي حظر جميع برامج التشفير، فيما عدا تلك المزودة «بالأبواب السرّيّة» التي بإمكان المصنعين والقائمين على الخدمات فتحها نزولاً عند طلب السلطات الفيدرالية.

ولكن، لم يعلم العاملون في مجال الشيفرة بهذا التشريع ـ الذي يعد قنبلة موقوتة ـ إلاّ بحلول نيسان/ أبريل من عام 1991. إذ كشف مستشار كان يعمل لدى وكالة الأمن القومي عن هذه الفقرة المسيئة في عدة لوحات لنشرات الإنترنيت، ومعها تعليق رؤيوي: «هل بين قراء هذه القائمة من يعتقد بأن القائمين على تأمين خدمات الاتصالات الإلكترونية، يستطيعون الاحتفاظ

لأنفسهم بالقدرة على قراءة جميع الأتصالات، وكذلك الإبقاء على «سرّيّة» الاتّصالات بأي معنى من المعاني؟... إن أي تأكيد بأن كل استخدام لأي من الأبواب السرّيّة، سيكون عندما يقر قانونياً بشكل مناسب وحسب، إنما هو هراء... وأي آلية كهذه ستكون عرضة لإساءة الاستخدام. وانتهت الرسالة بتحذير، عمل على جرف فيل زيمرمان مع التيار: «إني أقترح أن تبدؤوا بتخزين معدات التشفير، وهي ما تزال في متناولكم».

كان مشروع قانون مجلس الشيوخ اس 266، هو الموعد النهائي بالنسبة لفيل زيمرمان. فإذا لم يستطع إخراج برنامجه الجديد بي جي بي إلىٰ العالم الآن، فإنه قد يُواجه بحظره من الحكومة. وفي الوقت الحالي على الأقل كان التشفير داخل الولايات المتّحدة لا يزال قانونياً. لذلك قرّر زيمرمان أن ينهي النسخة الأولى من برنامجه بسرعة ويجعلها متاحة لأكبر عدد ممكن من لنا س. كذلك تخلّى عن الآمال التي عقدها بجني الأرباح من برنامجه «منتهى السرّيّة». فعوضاً عن إصداره كسلعة محصصة جعله سلعة متاحة مجاناً. ولم يكن ذلك يعني أن البرنامج لن يكلف شيئاً فحسب، بل يعني كذلك أن بإمكان المستثمرين توزيعه بأنفسهم شرقاً وغرباً بمباركة مبتكرة.

ولحسن الحظ، أنه وجد واسطة سهلت تداول برنامج مثل منتهىٰ لسرّيّة، أكثر من أي وقت مضى في لتار يخ: وكانت تلك الواسطة هي الإنترنيت. ففي عام 1991 كانت شبكة الكومبيوتر، التي كانتملكاً للدولة سابقاً في بداية ا نتشارها السريع الخاطف في كل مكان وجميع الأوقات. إذ راحت تعج بالآلاف من حلقات النقاش، وتحمل ملايين الملفات يومياً. لكن غالبية المستثمرين فيذ لك الوقت لا يمثّلون الناس بشكل عام، فمعظمهم كانوا من العارفين بالكومبيوتر والكثير منهم جريئون إلىٰ أبعد الحدود. غير أن هؤلاء كانوا من النوعيات ذاتها التي ستستجيب لـبي جي بي الذي كان على الرغم من جهود زيمرمان الحثيثة، لا يزال استخدامه دون برامج مثل ماك رايت، أو تيتر يس يسراً، وسهولة في الاستخدام.

والأمر الغريب، في ذلك الوقت، أن زيمرمان، لم يكن من المتحمسين للإنترنيت. وعرف استخدام البريد الإلكتروني بصعوبة، وهو بهذا المعنى كان لا يزال الغريب الذي ينظر إلىٰ الداخل. لكنه في الأشهر الأخيرة، أخذ يراسل شخصاً من المتحمسين للتشفير يعيش في كاليفورنيا، يدعى كيلي جوين، تعرف إليه من خلال شارلي ميريت. ويبدو أن زيمرمان في غضون شهر بعد الاتّصال الهاتفي الذي أجرياه بخصوص مشروع قانون مجلس الشيوخ إس 266، قد قدم نسخة من برنامج منتهى السرّيّة، لينتشر عبر الإنترنيت، وكتب زيمرمان لاحقاً عن ذلك «مثل بذور الهندباء البرية». وفي 24 أيار/ مايو قام جوين بإرسال رسالة عبر البريد الإلكتروني إلىٰ جيم وارين، وهو ناشط في مجال الكومبيوتر وله زاوية في صحيفة مايكرو تايمز المختصة في شؤون الكومبيوتر والمنتشرة في منطقة الخليج سان فرانسيسكو)، و شرح له الهدف من إغراق الشبكات ببرنامج منتهى السرّيّة. وكتب جوين قائلاً: كان ذلك لنسف الحجّة التي تقوم عليها فقرة ما يسمى بالباب السري في مشروع قانون مجلس الشيوخ الجديد قبل إقراره». وبتعبير آخر، إذا كانت الآلاف من نسخ برنامج «منتهى السرّيّة» تتداول، فسيعتبر مشروع القانون إس 266 غير مجد؛ فعندما تواجه الشركات الكبرى للاتّصالات أمثال إيه تي أند تي AT & T بملفات مشفّرة بواسطة برنامج منتهى السرّيّة، ستكون عاجزة عن ضمان النص الصريح لرجال المخابرات أو الأشباح.

وفي عطلة نهاية الأسبوع من شهر حزيران/ يونيو، تلقى جيم وارين عدداً من الاتّصالات من جوين، الذي أخبره أن يوم منتهى السرّيّة قد حل. ومن الواضح أن جوين كان مسحوراً بتأثير الحوادث بمجملها، ولخذ تدابير احترازية، مستوحاة من كتاب ماكسويل سمارت أكثر مما استوحيت من جيمس بوند و كتب وارين فيما بعد في مايكرو تايمز: «كان يتجول بسيارته حول منطقة الخليج ومعه كومبيوتر نقال ومولف أصوات وهاتف خليوي، ويتوقف عند

هاتف عمومي، ويقوم بنقل عدد من النسخ لبضع دقائق، ثم يقطع المكالمة ويهرع إلىٰ هاتف آخر يبعد أميالاً. إذ قال أنه يريد أن ينشر أكبر كمية ممكنة من النسخ وعلى أوسع نطاق ممكن من البلاد قبل أن تتمكّن الحكومة من الحصول على أمر قضائي بمنع نشره».

ويبدو أن جوين كانحر يصاً على نقل البرنامج إلىٰ مواقع الإنترنيت داخل الولايات المتّحدة فقط. ولكنبا لطبع، ما أن يظهر برنامج على مخدملفا ت الشبكة، حتّى يكون بإمكان أي شخص في العالم تخزينه: متسلّلونبا كستانيون أَو إرهابيون عراقيون، أَو بلغار ثائرون، أَو زناة سويسريون، أَو طلاّب مدر س ثانوية يابانيون، أَو رجال أعمال فرنسيون، أَو هولنديون يعملون في مجال صور الأطفال الإباحية، أَو نرويجيون مهووسون بالخصوصية، أَو تجار مخدرات كولومبيون. وعلى الرغم من أنه لم يصبح بعد متداولاً على نطاق واسع، فإن شعارالإ نترنيت بدأ يصبح مألوفاً: إن الحدود على طريق المعلومات الدولي لم تعد سوى صدمات ناتجة عن السرعة.

ما هومبلغ ا لسرعة التي غادر بها برنامج بي جي بي الولايات المتّحدة ووجد طريقه إلىٰ ما وراء ا لبحار، حتّى دون أن يتوقف للسلام على قوانين التصدير؟ فوراً. وقد دهش زيمرمان حين بلغه في اليوم التالي، أن الناس في دول أخرى، يشفرون رسائلهبها سطة بيانات بي جي بي. كيف يمكن لزيمرمان أن يتجنّب هذا العبور غير القانوني لبرنامجه إلىٰ دول بعيدة؟ وقد كتب لاحقاً: «كان من الممكن ألا أنشره إطلاقاً، لكن ليس ثمة قانون يحول دون حصول الأمريكيين على كريبتوجرافيا منيعة». فبعد كل شيء لقد دبر زيمرمان نشره المفاجئ لبرنامجه بي جي بيليس للا حتيال على قوانين التصدير، ولكن لتسليح رجال بلده، الناس الذين ربما يتضرّرون من مشروعقانو ن مجلس الشيوخ رقم 266. لقد كان شعاره، كما عبّر عنه في توثيقه للبرنامج: عندما يكون التشفير محظوراً، فإن الخارجين عن القانون وحدهم سيحصلون عليه».

ومن قبيل المفارقة، أنا للغة المهينة التي لمتخدمها جوزيف بايدن، وكانت الحافز لزيمرمان، ليخطو خطوته الخارقة، لم تلق الحماس الذي حظي به برنامج منتهى السرِّيَّة. و لقد فوجئ السيناتور بايدن بالغضب الجماهيري الهائل (الذي أزكته جماعات الحريات المدنية) بسببا للغة المعادية للسرِّيَّة والخصوصية التي استخدمها. وبحلول شهر حزيران/ يونيو، قام بسحب هذه ا لفقرة بهدوء. لكن الحادث خلف تركة غير متوقعة: مئات الآلاف من الرسائل المشفَّرة ببرنامج «منتهىا لسرِّيَّة» يتم تداولها في مختلف أرجاءا لمعمورة. لقد أ فلت برنامج «منتهى السرِّيَّة» من السواقة لصلبة لكومبيوتر فيل زيمرمان وتمّ ا ستنساخه بأعداد تنأى عن الحصر. ولم تعد قدرته علىا سترداده أكثر من قدرة المرء على استردادالكلما ت بعدما خرجت من شفتيه.

كان زيمرمان فخوراً ببرنامجه PGP 1.0 بي جي بي 1,0، بالرغم من أنّه كان في موقع الدفاع بسبب عيوبه. كون البرنامج لمأ ت بفتح رياضي جديد. ولربما كان الترميز سيء التنظيم حتّى أنّه شعر بضرورة الاعتذار عنه في وثائقه. لكنّه كان واحداً من أوائل الحلول العملية التي أتت بها الكومبيوتر الشخصية ويمكن استخدامها لنظام كريبتوجرافي كامل، بدءاً من التواقيع الرقمية إلىٰ التشفير. وفي ذلك يقول: «إذا ما نظرت إلىٰ ما كان متوفراً في ذلك الوقت، لم تجد إلاّ نسخاً معدّلة تجريبية عن خوارزمية رسا. نشرت إحداها في مجلة بايت Byte؛ ورأيت أن القيام بحسابات خوارزمية رسا يستغرق عصر يوم بكامله. أما برنامجي فلم يكن يتطلّب سوى ثوان لإنجاز مثل ذاك العمل. إنني ابتكرت تطبيقاً عملياً يحتوي على كل ما تحتاج إليه لوضع كريبتوجرافياا لمفتاح العام. لقد كان حدثاًها ماً. . . حدثاً فاصلاً».

لكن شخصاً واحداً عارض ذلك بشدَّة، هو جيم بيدزوس مدير شركة آر إس إيه وشركةببليك كي بارتنرز. فعندما رأى برنامج بي جي بي،ثار ت ثائرته. إذ شعر أنّه لم يكن مُنْتَجاً أصيلاًوإ نما سرقة واضحةلتقنيا ت شركته،

وبراءات اختراعاتها ـ حسبكم أن تنظروا إلىٰ ميلسيف ـ فلماذا لم يكن زيمرمان أميناً وأطلق عليه اسم منتهىٰ لسرِّيَّة؟ اتصل بيدزوس بالمبرمج، الذي يعيش في كولورادو ـ صارخاً به ـ وطالبه بسحب البرنامج من التداول. فعلى الرغم من العدائية التي كان بيدزوس يحملها في الماضي، فوجئ زيمرمان بهذه الاستجابة، وقال: «اعتقدت أنه سيكون مسروراً». وحاول الدفاع عن نفسه، بأنَّه قام بوضع بي جي بي لأبا ب سياسيَّة، وليس ليتحدَّى أي مشروع تجاري. فبعد كل شيء، إن الخمسمئة شركة التي تذكرها مجلة فورتشن وتعتبر زبائن آر إس إيه المحتملين لا يستخدمون سلعاً مجانية؛ بل يشترون برمجياتهم من شركات تدعمها وتسا ندها. إذن، ما المشكلة؟

لقد اتهمه بيدزوس بأنه ألعوبة في يد وكالة الأَمن القومي، ذلك أن كل ما يضرّ بشركته كان يسعد فورت ميد.

وبعيد ذلك، طلب بيدزوس من محاميه توجيه إنذار لزيمرمان لأنه بعمله هذا، ينتهك براءات اختراع ببليك كي بارتنرز. وهذا أقلق زيمرمانفا تصل ببيدزوس ثانية، محاولاً عقد صفقة معه. وكان أساس الاتفاق بسيطاً: عدم قيام زيمرمان بتوزيع برنامجه مع بروتوكولاتر سا، وبالمقابل لا يقاضيه بيانو س. وبالفعل تمّت صياغة اتفاق بهذا المعنى، وقام زيمرمان بتوقيعه. لكن كل فريق كان له فهمه الخاص لهذه المحادثة الهاتفية. شعر بيدزوس أن الاتفاق أرغم زيمرمان عملياً على قتل بي جي بي. وأصرّ زيمرمان على أنَّه إنما أكَّد فهمه لاتفاق افتراضي ليس إلاَّ، ومؤداه أنَّه إذا توقف عن توزيع برنامج بي جي بي، فإن الطرف الآخر يمتنع عن ملاحقته قضائياً. كذلك يدعي زيمرمان أن بيدزوس أعطاه تأكيداً شفهياً بأن شركة آر إس إيه ستقوم ببيع تراخيص لمستثمري بي جي بي النهائيين، وذلك ليصبح بإمكانهم استثمار البرنامج دون أن يكون في ذلك انتهاك لبراءات اختراع آر إس إيه. لكن بيدزوس أنكر هذه الإدعاءات.

اتضح لاحقاً أن تفسير زيمرمان لـ «توزيع بي جي بي» كان ضيقاً بعض

الشيء. وشعر أنّه بترك أمر التوزيع للآخرين يصبح حراً ليتفرّغ للبرنامج. وفي الواقع، فإن زيمرمان كان يشرف في تلك الأثناء، على الإصدار الثاني لبرنامج بي جي بي، بمساعدة بعض الاختصاصيين‌با لشيفرة الأوسع خبرة.

أدرك زيمرمان أنه بحاجة للمساعدة بعد تجربة إعادته إلىٰ صوابه في مؤتمر كريبتو 91 في سا نتا بربارة. وكانت مهمته الرئيسة الحصول على استطلاع رأيا لعلماء البارعين هناك، حول جانب الأمان في برنامج منتهى السرّيّة. (مع الإقرار بأنّ هذا كان أمراًتاً خر كثيراً، باعتبار أن آلاف الأشخاص باتوا يستخدمون البرنامج. وعلى الفور هرع إلىٰ براين سنو، وهو وا حد من كبار علماء الرياضيات والمختصّين بالشيفرة في وكالة الأمن القومي. وبالطبع كان زيمرمان يشعر بالفضول لمعرفة إن كانت الحكومة مستاءة من برنامج بي جي بي. لكن سنو قال له :لو« كنت مكانك، لخشيت من ملاحقة جيم بيدزوس لي قضائياً أكثر من خشيتي من الحكومة».

و لقد أثار هذاحيرة زيمرمان، فلماذا لم تكرا لحكومة قلقة؟ ثم سعى للحصول على تعليقات خاصّة على برنامجه. وفي بادئ الأمر صرفه آدي شامير الكريبتوجرافي الإسرائيلي، وبعد ذلك قال له أن يرسل البرنامج إلىٰ إسرائيل وسيمضي عشر دقائق في دراسته، لكن زيمرمان استحوذ على اهتمام إيلي بيهام زميل شامير في معهد وايزمن. وانتجع الاثنان إلىٰ كافتيريا جامعة كاليفورنيا في سا نتا بربارة، التي كانت مسرحاً للكثير من السجالات الأشبه باشتباك قرون الثيران وتحليل الشّيفرة الارتجالي في المؤتمر السنوي لعلماء الشّيفرة.بالو لنسبة لزيمرمان، كان غداء طويلاً بأكثر من معنى، إذ سرعان ما أحرج بيهامذ لك الكريبتوجرافي الهاوي حينما كشف له عيوباً ذات شأن في برنامج باس ـ أو ـ ماتيك، فعلى سبيلا لمثال، كانت الشّيفرة ضعيفة أمام هجوم تحليل الشّيفرة التفاضلي. وفي حين أن باس ـ أو ـ ماتيك لم يكن برنامجاً ميؤوساً منه، إلاّ أنه أبعد ما يكون عن كونه كنزاً ثميناً.

أدرك زيمرمان الآن أن الطريقة الوحيدة التي يمكنه بها تطوير برنامجه منتهى السرِّيَّة هي أن يعرف حدود إمكاناته. وأن أعظم إنجاز له في مجال ابتكار الرموز يتحقَّق بإدراكه أنَّه ليس بالكريبتوجرافي العظيم، وإنما واضع رزم ومبرمج واسع الاطلاع لبرامج عادية وتطبيقيَّةعا مة. لكنَّه يحتاج إلىٰ مختصين في الرياضيات والكريبتوجرافيا من طراز رفيع ليساعدوه فيالتفا صيل الجوهرية الصعبة.

ومن حسنا لحظ، أنا لعديد من الأشخاص الأذكياء قد أزكى الحماس لديهم صدور برنامج بي جي بي 1,0. وعوضاً من أن تضايقهمنقاط ضعفه، كانوا توَّاقين للمساهمة والعمل على إصلاحها. وسرعان ما جنّد زيمرمان متطوعين من نيوزيلندا وهولندا وكاليفورنيا ليصبحوا المهندسين الذين يعتمد عليهم. كذلك اجتمعت له جماعة من الفضوليين على غير اتفاق فقدَّموا له النصيحة وبضعة قطع صغيرة. وبدأوا جميعاً بالعمل معاً علىإ صدار النسخة 2,0 من برنامج منتهى السرِّيَّة. وكان زيمرمان المصمِّم الأساسي، وهو القائم على كل قرار وكل من الرموز، إلاَّ أنه حرص على إخفاء دوره، لئلا يعتقد بيدزوس، أنَّه نكث عهده بألاَّ ينتهك براءات الملكيَّة الفكريَّة لآر إس إيه.

كانت النتيجة برنامج بي جي بي 2.0 PGP 2.0، وكان مُنتَجاً أقوى مما سبقه إلىٰ أبعدا لحدود. وهذا نحَّى برنامج باس ـ أو ـ ماتيك جانباً (ويقول زيمرمان: «إنإ طلاقا سم كهذا عليه لم يكن فكرة حسنة، على أي حال. فالكريبتوجرافيا أمر لا يمكنك الاستخفا ف به»). وعوضاً عنه، اختار زيمرمان شيفرة سويسرية أقدم، تدعى خوارزمية تشفير البياناتا لدولية أو IDEA آيديا. وضعها اثنان من مشاهير علماء الرياضيات المختصين بالشّيفرة وذلك في عام 1990، وسرعان ما أثبتت آيديا وجودهاأ مام تمحيص الجماهير. وشعر زيمر مان أن شيفرة آيديا كانت أقوى من معيار تشفير البيانات ديز، وخا صة مع مفاتيح 128 ـ بت التي أوصى بها. وفيتوثيقه للإ صدار 2,0 كتب: «إن هذه ليست بخوارزمية مصنّعة محلياً».

وكان ثمة تطوير آخر، في ناحية كان زيمرمان تجاهلها أساساً، في برنامجه بي جي بي 1,0 : توثيق المفتاح، وهي العمليّة التي يتم فيها التثبّت من المفتاح العام. وغالباً ما كان يُنظر إلى التوثيق على أنّه عقب أخيل (نقطة الضعف) في أنظمة المفتاح العام. ويظهر اللغز التقليدي في مثل هذه الأنظمة عندما تريد أليس أن ترسل رسالة لبوب. فتعمل على تشفيرها بمفتاح بوب العام، وليس بإمكان أحد أن يفكّها، سوى بوب. لكن ماذا لو أن أليس لم تلتق ببوب من قبل، فكيف لها أن تحصل على المفتاح العام لبوب؟ إذا سألته عنه مباشرة، فليس بإمكانها أن تشفّر طلبها (من الواضح أنها لا تستطيع، فمفتاحه العام ليس لديها بعد، والذي ستستخدمه لتشفير الرسالة). لذا فإن متنصتاً محتملاً، مثل إيف، يستطيع أن يؤدي دور «رجل في الوسط» ويختطف الرسالة في الطريق. عندئذ سترسل إيف ـ مدعية أنّها بوب ـ مفتاحها العام إلى أليس زاعمة أنّه مفتاح بوب. (يعرف هذا لتنكّر المضلّل بـ «الخداع») فإذا خُدعت أليس، فستشفّر رسالتها السرّيّة إلى بوب باستخدام ذلك المفتاح. واحسرتاه، فلن يكون بوسع بوب فهم تلك الرسالة التي شفّرت بذلك المفتاح، بل هي إيف المخاتلة وحدها بإمكانها ذلك. وحسبنا هذا من ضمان سرّيّة المطالبات المباشرة.

ماذا بشأن نشر ما يشبه دليل هاتف رقمي مليء بأرقام مفاتيح عامة؟ إن مشكلة الاحتيال تظل قائمة، ما لم يكن لديك وسيلة أمينة يُعتد بها لحماية ذلك الدليل وضمان أن تكون المفاتيح تعود فعلاً لأصحابها المزعومين. أجل إن النجاح في هذه الخديعة يتطلّب جهداً جباراً. لكنّه ممكن، وما دامت قابلية الانتهاك قائمة، فإن على أي نظام مفتاح عام أن يجد طريقة للالتفاف على هذه الثغرة الأمنية.

كان الكثيرون يعتقدون أن الحل يكمن في إنشاء «سلطة مُوثِقة» على نطاق واسع لتوزيع المفاتيح العامة والتثبّت من صحتها. إن مركزاً كهذا سيكون قادراً

على معالجة الملايين من المفاتيح العامّة. وباستخدامك المفتاح العام للسلطة الموثقة، من المفترض أنه مفتاح متداول كثيراً لدرجة أنّه ما منأ حد يستطيع خداعه، بإمكانك أن تستعلم وأنت مطمئن عن المفتاح العام لأحدهم، أو أن تتأكّد من مفتاح عامأر سل إليك. وبالطبع، فإن حلاً طموحاً كهذا كان مستحيل التحقّق لزيمرمان. ذلك أنّه لم تكن لديه لا الوسيلة ولا الأموال لإقامة مركز لسلطة موثِقة لمراقبة التوزيع والتحقّق من المفاتيح العامّة. لذا كان عليه أن يفكّر ويخرج بمنهج آخر.

كان الحلا لذي خرج به مبتكراً للغاية. خاصة أنّه عكس إحسا س الغريب الذي كان يميز جهوده. فعوضاً عن إنشاء سلطة مركزية للمفاتيح تصور مجتمع برنامج بي جي بي نفسه هو السلطة. و شرح زيمرمان ذلكفي مقابلة أُجريت معه عام 1993، بقوله: «إن برنامج بي جي بي يتيح لأطراف غير المرسل والمستلم، وهم أصدقاء موثوقين من الطرفين، أن يوقعوا المفاتيح. وهذا يثبت أن الرسالة وردت من الأشخاص المعينين أنفسهم». وبقوله «توقيع» المفاتيح، كان زيمرمانيعني بذ لك تقنية، يمكن للمرء بواسطتها أن يربط مفتاحه أو مفتاحها العام بمفتاح شخص آخر، وكأنّه خاتم بالموافقة. فبعد أن تولد مفتاحاً عامّاً، تعمل على جعل بعض معارفك الشخصيين، يوقع على مفتا حك. ويجب أن تتم هذه التواقيع وجهاً لوجه، وذلك لتقليص خطر الوقوع في لخداع. لذا إذا كانت أليس تعرف بوب شخصياً، فإنّها ستدبر لقاء معهو تقدم له بنفسها ا لقرص الذي يحتوي على مفتاحها العام،ا لذي أوجدته باستخدامها برنامج بي جي بي. وباستخدام بوب لنسخته من برنامج بي جي بي، يوقّع بوب المفتاح العام لأليسبمفتا حه الخاص. (يتم ذلك ببساطة بانتقاء دالة في برمجية البرنامج والنقر على الفأرة) ويعيد لها المفتاح الموقّع ويحتفظ بنسخة ليضمها إلىٰ «حلقة ا لمفاتيح العامّة» وهي مجموعة من المفاتيح الموقعة والتي يتم تشجيع مستثمري برنامج بي جي بي على الاحتفاظ بها في السواقة الصلبة الخاصة بهم. وقد

يرغب، فيما بعد، فريق ثالث، ولتكن كارول، في التخاطب وأليس، إلاّ أنها لا تعرفها. لذا تسعى كارول للحصول على مفتاح أليس العام، إما عن طريقها مباشرة أو من لوحة إعلانات تحفل بالمفاتيح العامّة. وفي الحالة الثانية كيف لها أن تعرف أنها أليس فعلاً؟ إنها تتوقف لترى من الذي وقّع المفتاح، هل يحمل علامة موافقة شخص تعرفه؟ ولمكا نت كارول تعرف بوب،وكا نت سابقاً قد تلقت نسخة موثقة من مفتاح بوب العام، لذلك بإمكانها أن تتأكّد من صحة توقيعه. فإن تحقّقت منه، فإن ذلك يعني أن بوب، قد التقى فعلاً بالشخص الذي يحمل هذا لمفتاح الجديد، وهو يقول لكارول بكل وضوح: «نعم إنها أليس نفسها» وبإ مكان كارول أن تكون واثقة من أن أليس ذاتها. على الأقل، إلىٰ الدرجة التي تثق فيها ببوب.

إن هذا النّظام الذي يُعرف بـ «شبكة الثقة» يحتاج إلىٰ شيء من ا لمحاكمة العقليّة من طرف المستخدم. فبعد كل شيء، لا يمكن لكارول أن تتأكّد من هوية أليس ما لم تكن هي نفسها تعرف شخصاً ما، كان قد التقى بها شخصياً ووقّع مفتاحها. وماذا لو لم تكن تعرفأ حداً وقّع المفتاح شخصياً؟ هل الأمر يستحق الوثوق بإثبات من الدرجة الثانية؟ ربما لم يكن صديقها بوب قد وقّع مفتاح أليس، لكنه كان قد وقّع مفتاح شخص يدعى تيد. وتيد هذا قعٌ مفتاح أليس. أما ثقتك بذلكا لتوقيع، فأمر يعتمد على سمعة تيد: ومن هم الأشخاص الذين وقّعوا مفتاحه؟ ولما كان إقبال الناس على استخدام برنامج بي جي بي في ازدياد، فمن المحتمل أن بعضهم سوف يعرف بأنّه كثير الوساوس بما يتصل بالتحقّق من المفاتيح التي يوقّعها. إن رؤية واحد من هؤلاء المعرفين الموثوقين على حلقة مفتاح سيكون عندئذ إثباتاً على صحته. وعلى أي حال، فإن برنامج بي جي بي يتيح للمستخدمين تحديد ما يشير إليه الكريبتوجر افي بروس شناير بـ «مستويات البارانويا»: أي أن عدد مستويات الفصل، التيأ نت على استعداد للقبول بها، يعتمد على درجة وثوقك بالعديد من الموقعين.

ومع وجود شبكة الثقة هذه، و خوارزمية تشفير أقوى، ودارة ربط بينية أفضل، وعدد من التحسينات الأخرى، فإن برنامج بي جي بي 2,0، بخلاف البرنامج الكوميدي المفضل عند زيمرمان الذي يُذاع في عطلة الأسبوع، أصبح جاهزاً للعرض الأول. لا بل إن هذا الجمع من الأعوان الذين قدَّموا يدا لعون للبرنامج أعدّوا له ترجمات للبينيات بلغات كثيرة، لذلك كان بإمكان الناس في جميع أنحاء العالم ستخدا مه منذ اليوم الأول لإصداره. وفي شهر أيلول/ سبتمبر 1992، قام اثنان من مساعدي زيمرمان بإطلاق برنامج بي جي بي 2,0 على الشبكة في بيتيهما في أمستردام وأوكلاند. وبهذه الطريقة يمكن استيراد البرنامج إلىٰ داخل الولايات المتّحدة، دون انتهاك قوانينا لتصدير. وسرعان ما خلف الإصدار الجديد الإصدار الأول وفاقه. ويقول زيمرمان: «بعد شهر واحد من الإصدار تلقيت رسائل بريديَّة أكثر بكثير مما تلقيته طوال السنة السابقة. لقد كان الأمر أشبه بالنار في الهشيم».

لقد ازداد جيم بيدزوس غضباً، إذا جاز التعبير، وثارت ثائرته بالأخص، لرأي أورده زيمرمان في الوثائق التي ترافق كل شحنة من برنامج بي جي بي. إذ ادعى زيمرمان أن ببليك كي بارتنرزكا نت تنهب الجمهور الأمريكي، بأن جعلت الناس يدفعون ثمن تقنية تم تطويرها بأموال الحكومة. وبعد محاولات زيمرمان تغطية نفسه بالتنصل كقوله: «إن مبتكر هذا البرنامج التطبيقي لخوارزميةر سا يقدم هذا... للأغراض التعليميَّة فقط... وعلى عاتقك تقع مسؤولية الحصول على رخصة، لاستخدام هذه الخوارزمية من ببليك كي بارتنرز، فأنت المستخدم، وليس فيل زيمرمان...»،ا سترسل في تبر ير مطول لأفعاله، مدعياً أنَّه لم يعتقد أنَّه كان ينتهك حقوق أي براءة اختراع. وألمح إلىٰ أن ببليك كي بارتنرز، بسيطرتها على براءت اختراع كريبتوجرافيا المفتاح العام، فإن هذه الشركة ـ وقد سمَّاها «شركة مقاضاة أساساً» ـ كانت تقوم بالأعمال القذرة، نيابة عن وكالة الأمن القومي، وذلك باحتكار التشفير وإنكاره على

الناس عموماً! وأخيراً قال للمستخدمين المحتملين، أنّه ليس ثمة ما يحملهم على القلق من احتمال خرقهم حقوق براءة اختراع ببليك كي بارتنرز، إذ كتب: «هناك أعداد من مستثمري برنامج بي جي بي أكبر من أن تستطيعوا ملاحقتهم فلماذا ينتقوك للملاحقة دون سواك؟» إلاّ أنه لم يقدم لهم أي ضمانات.

وفي عام 1994 قال بيدزوس: «إنه [زيمرمان] يضلّل الناس، ويتعمّد الإساءة إلى سمعتنا لكي يحصل على دعم لبرنامجه. تلكم هي الحكومة الشريرة التي تحاول حرمانكم من حقكم في السرّيّة، وأصحاببراءات الاختراع مصمّمون على سرقة أموالكم ونهب الحكومة، وليس واضحاً من الأسوأ، لكن بإمكانكم أن تصدوهما باستخدام هذا البرنامج. لقد كان يعلم أن [ادعاءاته] زائفة».

كان بيدزوس محقاً في أمر واحد: أنّه سبق لشركة آر إس إيه أن أنتجت بر نامج ميلسيف، وهو تطبيق لبراءات اختراع المفتاح العام. وكان الفريقان كلاهما متفقان، على أن بيدزوس قدملز يمرمان، أثناء لقائهما علىا لعشاء الذي حصل عام 1986، نسخة من برنامج ميلسيف، لكن زيمرمان يدعي أنّه لم يختبر البرنامج أبداً، ولم يقرأ الوثيقة المرفقة به، لأنّه كان قد اكتشف طريقة عمل منتجه قبل ذلك. ويقول بيدزوس: «يخبرنا هذا الرجل أنّه ذُهل لابتكار خوارزمية رسا، ثم يفترض أن نصدّقه حين يقول أنّه أخذ البرنامج الذي وضعه أصحاب ذلك الإنجاز، وهم أبطاله، ولم يجد لديه الفضول الكافي ليلقي نظرة عليه؟».

لكن معظم غضب بيدزوس، لم يكن موجّهاً ضد أفعال زيمرمان وحسب، بل إلى الشعبية المتصاعدة لبرنامج بي جي بي أيضاً. لأنّه كان يقدم مجاناً، وغدا متاحاً في جميع أرجاء العالم بصرف النظر عن قوانين التصدير، ولما اكتسبه من رونق بين جمهور عشّاقالتقنيا تا لمتطورة، فضلاً عن شيوع استخدامه حتى فاق برنامج «ميلسيف»، وأخذ الآن يهدّد بأن يصبح برنامجاً نموذجياً في الإنترنيت. وبالرغم من أن زيمرمان ليس من الكريبتوجرافيين

المبرزين ممن يحملون شهادة من جامعة ستانفورد، ولا ينتسب إلى الدوحة العطرة لمعهد ماساتشوسيتس للتكنولوجيا، وليست له دراية تقريباً بالتجارة أو التسويق، إلاّ أنّه تمكّن من إنجاز ما عجز عنه علماء الرياضيّات مبتكرو المفتاح العام ذو الشهرة العالمية، وما فشل فيه جيم بيدزوس الخبير بالسوق: وهو خلف ظاهرة تشفير متصاعدة لم تستمل إلى جانبها مستثمرين من جماهير الناس فحسب، بل وصفت كذلك بأنّها التحدي الأكبر للوكالة التي تعمل وراء السياج الثلاثي وتكاليفها التي بلغت عدة مليارات من الدولارات. فلا عجب إن غدا في نهاية عام 1992، بطل النضال السري للشيفرة بعد أن كان مغموراً. ويقول: «لو ذهبت إلى أوروبا فلن أضطر لدفع ثمن الغداء، إذ لدي أعداد هائلة من المعجبين المتفانين».

كان من شأن جهود زيمرمان الشخصية لابتكار برنامج تشفير وتوزيعه على الناس ـ وهو جهد قام به بهدف الالتفاف على سيطرة الحكومة ـ أن شكّل بعداً جديداً للمعركة المستمرة بين وكالة الأَمن القومي والكريبتوجرافيين الذين يعملون خارج نطاق سيطرتها. وسبق للوكالة أن شعرت بأن التسويات التي عقدتها مع الأكاديميين لتقديم أعمالهم طواعية قبل النشر قد خففت من معظم المخاطر المحتملة لذلك المجتمع الصاعد. (والخيار هنا ضئيل بسبب التعديل الأول في الدستور) كذلك كان صنائع فورت ميد يعملون أيضاً على إبعاد تهديد التجارة لهيمنتهم بزحزحة موقفهم قليلاً في موضوع التصدير.

لكن الأمر كان يزداد صعوبة في إقناع الناس بأن السيطرة على الكريبتوجرافيا أمر منطقي. إذ أخذ يتضح أكثر فأكثر أن الكريبتوجرافيا لا تنتمي إلى تكنولوجيا الأسلحة، بل هي تقنية يمكن أن تصبح جزءاً من حياتنا اليومية. لقد كانت هذه الملايين كلها التي تستخدم لوتس نوتس مدركة لمنافعه. وصدم مستخدمو البريد الإلكتروني المتنوّع عند اكتشافهم أن الحماية الأساسيّة لم تكن متوفّرة في أجهزتهم. إن إرسال البريد عبر الإنترنيت الذي بدا آمناً لكنّه في واقع

الحال ظلّ متخلفاً خطوة واحدة عن اللحاق بالإذاعة. وعلى سبيل المثال، مع ازدياد أعداد الأشخاص الذين يستخدمون الهواتف الخليوية، راح هؤلاء يتساءلون عما يجعل مراقبة اتّصالاتهم الهاتفية سهلة على أي جهاز فاحص ثمنه مئة دولار. حتى أن المكالمات التي أجراها أمير ويلز مع عشيقته عبر الهاتف الخليوي تم اعتراضها ـ وبسببها أصبح العالم كله يضحك الآن، على كلمات تحبّب قالها لعشيقته ـ كلمات شخصية إلى أبعد الحدود (حسن، لقدكانت تتعلّق بأشياء تتصل بالطمث). لم لا ينبغي أن يكون كل شيء محمياً، في عالم من الاتّصالات المتطورة جداً؟ فحتى الفريق الوطني لكرة القدم قرّر التالي: استخدام الشيفرة لتشفير إشارات الراديو التي يرسلها المدرّبون في غرف المراقبة، إلى لاعبي الظهير الربعي في الملعب. كان ذلك شيئاً يمكن لأي شخص أن يفهمه. فهاك طريقة بسيطة تمنع فريق جرين باي باكرز من سرقة اللعبة التالية من جون إلواي... وندعوذ لك أمنا قومياً؟

تلك كانت أسئلة صعبة، موجهة لفرع من الحكومة ليس معتاداً على الإجابة على أي سؤال إطلاقاً. لكن التساؤل كان على وشك أن يصبح أكثر حدّة، مع دخول قوة جديدة على اللعبة، قوة كانلزيمر مان نصيب في بروزها، وأصبحت الآن فاعلة، إنها لفعالية الكريبتوجرافية Cryptoactivism. أي نشر الكريبتوجرافيا المنيعة عبر الإنترنيت. وحركة ثورية مبنية على إنتاج ونشر وتوزيع الرموز القوية، وقد بدت في ظاهرها نشاطاً عارضاً. لكن مع احتدام الجدل حول التشفير، اتضح أن الوقت قد حان، لظهور حركة صغيرة لتقوم بممارسة بعض الضغط.

هكذا بدا الأمر لاثنين من المتحمسين للشيفرة، خرجا بفكرة إنشاء مجموعة خارج نطاق اللامنتمين في المعركة من أجل الكريبتوجرافيا. ونشأ هذا المفهوم عفوياً عندما قام إيريك هيوز، وهو عالِم رياضيّات شاب يعيش في شمال منطقة الخليج ويفكّر في الانتقال إلى جنوب ساحل كاليفورنيا، بزيارة صديقه تيم ماي في سانتا كروز في بحثه عن بيت.

كان هيوز وماي ائتلافاً طريفاً بين شخصين، يجمع بينهما شغف بالعلم، وميول تحررية فيالسيا سة، وقدر من البارانويا غير المثيرةللأعصا ب. (كان يحلو لهيوز أن يسخر من هذا، مقتبساً عبارة يفترض أن فيلسوفاً مغموراً كان قد قالها: «إن الكريبتوجرافيا هي النتيجة الرياضية للافتراضات البارانوية»). وكان كلاهما شخصية مؤثرة، طرحا عنهما مظهر عالم الرياضيات، ليرتديا زي رجال الغرب الأمريكي فكانا كريبتو كاوبوي. وغالباً ما كان هيوز، يُشاهد معتمراً القبعة العريضة التي يظهر بها رعاة البقر في الأفلام.

كان ماي فيزيائياً، في الأربعين من عمره، تقاعد قبل سبع سنوات من انتل ومعه كمية من الأسهم. كان إسهامه الكبير في مصنعنصا ف النواقل العملاق برهانه على أن الوقائع الكمية (كوانتوم) ـ حركة الأجزاء المكونة للذرّة ـ يمكن أن تؤثّر في الحسابات التي تقوم بها الرقاقات المصنوعة من نلصا ف النواقل. وقد سمح كتشاف ماي هذا للمصممين في إنتل ابتكار استراتيجيات للتعامل مع هذه المشكلة. مما جعل قانون مور في التقدم المستمر ممكناً. وبعيداً عن التكنولوجيا كان ماي داعية للتحررية في وجه القيود التي تضعها الحكومة. ويقول: «لقدا هتديت لدى قراءتي لكتب آين راند عندما كنت طفلاً، وأثناء الدراسة صرت أكتب مناظرات حول الحقوق الطبيعية». ولما بلغ سن الرشدأر سل مطارحات من هذا القبيل ـ أحاديث صاخبة محرضة عالمياً، ومسلية للغاية ـ إلىٰ جماعات مستخدمي الشبكة Use net، واكتسب سمعة المنفعل لتأييداه لشديد للكريبتوجرافيا المتحرِّرة من كل قيد. وكان ماي رجلاً نحيلاً ذو لحية وغالباً ما كان يرتدي قبعة يعتمر بها أهل الريف النائي، ويمتلك منزلاً صغيراً تتكون فيه أكداس من الكتب والآلات والقطط السمان.

أما إيريك هيوز فكان من طائفة المورمون لكنه شبه مرتد، ومن فيرجينيا، ولهلحية طويلة خفيفة ذات لون بني فاتح. ويضع نظارات بإطار معدني، ويتمتع بذكاء لا مبال ساخر. ومع أنّه لم يكن قد بلغ الثلاثين من عمره إلاّ أنّه

كان ذا شخصية قوية. وكان يلطف من ثقته المفرطة بالنفس ذكاء هادئ يمكنه من فهم وجهي مسألة ما. وكان شغوفاً بالكريبتوجرافيا. ودرس الرياضيا ت في جامعة بيركلي، وعمل لفترة في شركة في الخارج. والآن مع سطوع فجر الإنترنيت كان يفكّر في كيفية استخدام الرموز لتحصين عصر المعلوما ت. وهدفه النهائي المزج بين رأ سمالية السوق الخالصة والنضال من أجل الحرية. وفي نظرته إلىٰ العالم، كا نت الحكومات تشكل خطراً دائماً على رفاه المواطنين، بما في ذلك الحكوما ت الرحيمة المزعومة مثل الولايات المتّحدة. و يرى أن خصوصيةأ سرار الفرد قلعة تتعرض على الدوام لهجوم الدولة. والمعجزة الكبرى أنه يمكن مقاومة الدولة بالخوارزميا ت. وفي لك يقول: «في الماضي كان المرء يحصل على السرّيّة بذهابه إلىٰ التخوم الطبيعية بعيداً عن الآخرين حيث لا يزعجك أحد. ومع التطبيق الصحيح للكريبتوجرافيا، بإمكانك أن تنتقل ثانية إلىٰا لتخوم وبشكل دائم».

بالرغم من أن رؤى هيوز كانت راديكالية، إلاّ أنّها بهتت بالمقارنة مع رؤية صديقه، الذي يعيش في سانتا روز. عندما فكر تيم ماي في الشّيفرة كان الأمر أشبه بإنزال قطرات من الأسيد. وفي عصر الكومبيوتر، نقوم بخُلق ـ ما يصفه بـ «مناطق افتراضية»، وأن أنابيب وأسلاك المستقبل ـ الملاط والجدران الفعلية لهذه الفضاءات الافتراضية ـ لا يمكن أن يثبتها سوى الشّيفرة وحدها ولا شيء سواها. وعند الحديث عن هذه الرؤى ينفجر ماي قائلاً: «آه، يا إلهي إنها عميقة للغاية. لا يوجدشيء سواها! ويؤكد أن الدوال (التوابع) الوحيدة الاتجاه مثل تلك التي عالجها ديفي وميركل ورايفست، كانتلبنا ت ا لفضاء المتخيّل، وإذا لم نستخدمها، فإننا سنتحوّل إلىٰكائنا ت مثيرة للشفقة ترتعش وهي تقف وسط رماد بيت افتراضي محترق. لكن بها يمكن تخيّل كل شيء أقنية ـ لا يمكن لوكالة الأمنا لقومي أن تمسّها ـ آمنة من المتسللين في لوس جاتوس، وكاليفورنيا، إلىٰ الناشطيرفي سانت بطرسبورج في روسيا. وصفقا ت بعيدة

عن متناولا لضرائب. ونهاية الدولة القومية. كانت تلك هي الثورة القادمة، وفقاً لتيم ماي.

تلك كانتا لمواضيع التي تمّت مناقشتها في أيار/ مايو عام 1992، أثناء زيارة إيريك هيوز لتيم ماي في بحثه عن المنزل. وكان ثمة الكثير مما يثير الحديث لدرجة أن الحديث استمر بينهما مدة ثلاثة أيام. ويصف هيوز ذلك بقوله: «كنا نستيقظفي الصباح، ويتصل بنا الحديث، غير عابئينبأ مر البحث عن البيت المنشود. ثم نذهب لتناول الغداء، ونعود لنتابع الحديث من جديد. واستمر الأمر على هذا المنوال». وبنهاية الزيارة اتفقا على تنظيم اتحاد حر، يتألّف ممن لهم آراء مشابهة ـ لم يحرز هيوز أي تقدم بشأن العثور على منزل، فعاد، ولا عجب، إلىٰ شقتها لمشتركة في بيركلي ـ كماا تفقا على عدم الجلوس وتبادل الأحاديث غير المجدية، بل علىا لعمل، حسب نهج زيمرمان، على إ نتاج الأدوات التي ستسلح الجماهير لمواجهة لصوصا لكومبيوتر، ومكاتب القروض، وبشكل خاص الحكومة.

في الأسابيع القليلة التالية، حصلوا على دعم من بعض الشخصيات ذات النفوذ في مجتمع الشيفرة المعاديللحكو مة. وكان أحد الحلفاء الأقوياء جون جيلمور البالغ منا لعمر سبع وثلاثون عاماً، من متسللي لكومبيوتر لطيف المعشر مسترسل الشعر، في سبيله إلىٰ الصلع، وذو لحية خفيفة. وكان جيلمور قد أصا ب ثروة صغيرة بفضل كونه واحداً من المبرمجين لذ ين يتميزون بالأصالة عندما كان يعمل لدى شيفرة صن مايكروسيستمز ـ كان الموظف رقم خمسة في سلسلة المراتب ـ لكنه ترك العمل عام 1986. وفي عام 1990، قام بتأسيس شيفرة إليكتريكال فرونتير فاونديشن (EFF إي إف إف)، وقد شاركه في هذا كل من ميتش كابور وجون بيري بارلو، والهدف تعزيز الحريات المدنية في العصر الرقمي، وكان قد أسّس للتو شركة جديدة تُدعى ساينوزسبور تموتهد ف إلىٰ مساعدة مستخدمي البرمجيا ت المجانية. وكانت هوايته المفضلة: السرّيّة

الشخصية. وفي مؤتمر عُقد عام 1991 أطلق عليه اسم «الكومبيوتر والحرية والسرِّيَّة» ألقى خطبة استبق فيها أفكار ماي وهيوز ـ حركة تشفير جماهيرية لدرء شر الحكومة.

ماذا لو استطعنا بناء مجتمع لا تجمع فيه أية معلومات؟ مجتمع يمكنك فيه أن تدفع إيجار شريط الفيديو دون أن تترك بطاقة اعتماد أو رقم حسابك المصرفي؟ ويمكنك أن تثبت أنَّك مؤهل لقيادة السيارة دون أن تعطي اسمك؟ وإرسال أو تلقي الرسائل دون الإفصاح عن مكان إقامتك، مثل صندوق بريد إلكتروني؟ ذلك هو المجتمع الذي أريد بناءه. أريد أن أثبت ـ باستخدام الفيزياء والرياضيات لا بالقوانين ـ أموراً مثل السرِّيَّة الفعلية للاتِّصالات الشخصية... السرِّيَّة الفعلية للسجلات الشخصية.. الحرية الفعلية للتجارة.. السرِّيَّة الفعلية للأوضاع المالية.. [و] السيطرة الحقيقية على الهوية.

كان جيلمور مهتماً بشكل خاص، بأن يكفل وصول المعلومات التي تتحدَّث عن الشَّيفرة إلىٰ عالم الجماهير. (كان هو الشخص الذي استخدم الإنترنيت لنشر البحث الذي وضعه ميركل عن التشفير السريع بعد أن طلبت وكالة الأَمن القومي من شركة زيروكس عدم نشره). وفي العهد القريب، كان يحاول تحرير أربعة كتب مدرسية قديمة في تحليل الشَّيفرة، كان قد وضعها وليم فريدمان الرجل الأسطوري البارع في وكالة الأَمن القومي. وتقديم طلبات باسم حرية تدفق المعلومات وذلك لرفع الحظر عن هذه الكتب التي يعود تاريخها إلىٰ ثلاثين سنة مضت. بل لقد أوكل محامياً في بيركلي، لمساعدته على إتمام العمليَّة المعقدة، ورفع الدعاوى حين لا تبدي الهيئات الحكومية تجاوباً، ضمن الفترة الزمنية القانونية المحدَّدة.

بعيد المطالبة برفع الحظر عن أعمال فريدمان، بدأ جيلمور بحثاً ببليوجرافياً مطولاً حولها على الإنترنيت، مستخدماً برامج «نو بوتز Know-bot» وهي برامج بحث ذكية مؤتمتة. وقد دل البرنامج على توفر نسخ من كتابين

لفريدمان في تفكيك الرموز متاحة لاطلاع القراء، أحدهما في مكتبة كلية فيرجينيا العسكرية، والآخر على مايكروفيلم في جامعة بوسطن. ومن الواضح أن الحكومة قد رفعت عنهما الحظر في وقت من الأوقات، لكن في عهد الرئيس ريغان سُحبا مرة لتداول وأصبحا مرة أخرى من الكتب المحظورة. وعلى الفور حصل جيلمور على نسخ أرسلها إليه أصدقاؤه، وأعلم القاضي الذي ينظر في طلبه بشأن حرية المعلومات أن الكتب كانت متاحة للقرّاء في مكتبات عامة. وكان رد الحكومة إنذار جيلمور، بأن أي نشر لنصوص فريدمان سوف يُعتبر انتهاكاً لقانون التجسّس، الذي ينص على عقوبة بالسجن، لمدة قد تصل إلى عشر سنوات في حال مخالفة أي بند من بنوده. وبعبارة أخرى، يمكن أن يرسل جيلمور إلى سجن ليفنورث مدة عقد كامل، وذلك لمجرد أنه أخذ كتاباً من فوق رفوف مكتبة عامة وأطلع أصدقاءه عليه. لكن جيلمور لم يكتف بأن يعلم القاضي بأن الحقوق التي نصّ عليها الدستور (التعديل الأول) قد انتهكت، بل أعلم مراسلي الصحف المحليين بالقصة أيضاً.

بعد ذلك بيومين تراجعت الحكومة، ورفعت الحظر المفروض على النصين رسمياً. لكن جيلمور استمر في السؤال عن الكتب الأخرى، وطلب أن يعلن القاضي أن قانون التجسّس يمثّل قمعاً لحرية التعبير منافٍ للدستور. وعندما سأله أحد المراسلين إن لم يكن في موقفه إضعافاً للأمن القومي، لم يبد أسفاً وقال: «إننا لا نسعى إلى تهديد الأمن القومي، بل لنبذ فكرة بيروقراطية عن الأمن القومي، ترجع إلى زمن الحرب الباردة وعفا عليها الزمن. إنهم [الحكومة] ينتهكون حرية وسرية المواطنين. وذلك لحما يتنا من غول لن يقوموا بوصفه لنا».

بدأ هيوز وماي بالعمل مع جيلمور (لم يوافق هويتفيلد ديفي إلاّ لاحقاً، على الاشتراك بصفة استشارية) في التخطيط للقاء حقيقي للحركة المقترحة.

كان هيوز في ذلك الوقت يطلق على المجموعة اسم هواة الكريبتوجرافيا للا مسؤولية الاجتماعية [واختصاراً] CASI كاسي. أمضى هيوز وماي الصيف كله، في التحضير وإرسال الدعوات للحدث العالمي في 19 أيلول/ سبتمبر 1992 في منزل هيوزفي بيركلي. وقرّروا أن يكون شعارهم التكتم، ذلك أن طبيعة المغامرة، كانت تتضمن هجوماً ضمنياً، على أكثر وكالاتالجا سوسيّة التابعةللحكو مة قوة.

تجاوز اللقاء توقعات الجميع، وعلى العكس من أكاديميي بيركنستوكد والأشباح الفضوليين الذين التقوا في مؤتمرات الكريبتو. فإن الحضور الذين بلغ عددهم حوالي العشرينكا نواأ شخاصاً ينظرون إلىٰ الكريبتوجرافيا على أنّها خارج نطاق عملهم تماماً (إذا كان لديهم عمل، ذلك أن بعضهم كان بلا عمل). وكان همّهم الأساسي هو كيف سيستخدما لناس أدوات التشفير،و كيف يجلب ستخدامها. كا نتسيا ساتهم شديدة المناصرة لمذهب الحرية. وكان الكثير منهم يعلنون الانتماء إلىٰ جماعات متطرفة، وكانت فلسفتهم تمزج بين نظرة متطرفة إلىٰ الحريات الشخصية واعتقاد خيالي. إن الحدود البعيدة للبحث للعلمي سوف تكون في وقت قريب لصالحنا. (وقد تضمنت الموضوعات التي أدارت رؤوس المتطرفين تكنولوجيا الجزيئات الدقيقة، والتحكّم الآلي وفيزياء الحرارة المنخفضة؛ وكان بعض هؤلاء المتطرفين قد تطوّعوا ليتم تجميد رؤوسهم بعد وفاتهم، وذلك ليصار إلىٰتذ ويب الجليد عنها، ويعودوا إلىٰ الحياة في قرن من القرون لا بدّ قادم).

لكن من الخطأ أن نسيء الحكم على الجماعة لهفواتهم أو للنتائج المتواضعة التي انتهى إليها هذا اللقاء الأول. في الواقع، انتهى الأمر فيما بعد بأن أصبحوا على قدر عظيم من النفوذ لدرجة أن أثر خيالاتهم تطرفاً باتت موضع دفاع المدافعين. مجدفين وغريبي الأطوارو متناغمين تماماً مع أنغام الرقصات الرقمية لإيقاع الإنترنيت، لقدكا نوا كريبتوجرافيين، وأصحاب

مو قف. وإذا لم يكن لدى الحكومة من الأمور التي تشغلها في مجالات ا لصناعة او لمدافعين عن السرّيّة، والإصلاحيين والمطالبين بحرية التشفير، كان ظهور ثوار الشّيفرة ليصبحواأ بطال الثقافة الشعبية هيا لنقطة التيفا ضت بها الكأس، وهي إشارةغير متوقعة إلىٰ أن حروب الشيفرة، قد انتقلت إلىٰ موقع جديد. ها قد أتى ثوارا لشّيفرة، ملوحين بسلاح فكري قوي: فوضى التشفير.

قدَّم تيم ماي، نشرة من سبعة وخمسين صفحة، أعدها خصيصاً لهذا اللقاء الأول، بالإضافة إلىٰ جدول أعمال موسّع يتضمن نقاشاً لـ «المضامين الاجتماعية للكريبتوجرافيا»، و«شبكات التصويت»، و«أسواقا لمعلومات المجهولة». كما نت هناك تقارير عن الأموال الرقمية في فرضيات واقعية، وتقييم جون جيلمور لوكالة الأَمن القومي. وكان هناك بعض الوقت تم ادخاره، بالطبع، «لقرّاء البيانات الرسمية». وكان تيم قد أعد بياناً خصيصاً لهذا اللقاء، أطلق عليه «بيانقو ضو ي التشفير». انتهى بملاحظة محفزة.

مثلما غيرت تكنولوجيا الطباعة، وقلّصت نفوذ نقابات الحرف في ا لعصور الوسطى، وبنية لسلطة الاجتماعية، كذلك فإن الطرائق الكريبتوجرافية الأساسية ستحدث تغييراً جذرياًفي طبيعة ا لشركات الكبرى وتدخل الدولة في العمليات الاقتصادية. إن فوضى التشفير مجتمعة مع أسواق المعلومات الصاعدة، سوف يُخلق سوقاًسا ئلة لكل المواد التي يمكن وضعها في كلمات وصور. فكما أن اختراعاً ثانوياً في ظاهره مثل الأسلاك لشا ئكة قد جعل من الممكن تسوير وفصل المزارع الكبيرة، وبذلكأ حدث تغييراً في مفاهيم الأرض وحقوق الملكية في الغرب الجديد، كذلك فإن الاكتشاف الهامشي ظاهرياً الذي حدث في فرعسر ي من فروع الرياضيات أصبح بمثابة« مقراض السلك»، الذي فك الأسلاك الشائكة حول الملكيّة الفكريّة.

انهض، أيها العالم؛ فليس لديك ما تفقده سوى أسوارك من الأسلاك الشائكة.

دعي الناس للاشتراك في «لعبة فوضى التشفير»، لمدة ساعتين، وهو تمرين تقمص أدواراً يتخيّلون فيه، استخدامهم بروتوكولات تشفير غريبة جداً لتعمية أنظار المراقبين لنشاطاتهم، مثل تحرير الأسرار أو عقد صفقات مخدرات. ولما كان برنامج بي جي بي 2.0 قد صدر قبل أيام قليلة من انعقاد المؤتمر ـ ومعظم الحاضرين كانوا معجبين أشد الإعجاب بنسخته الأولى ـ فمضى معظم اللقاء في مناقشة آخر جهد قدمه فيل زيمرمان، ووزعت نسخ من البرنامج لجميع المتواجدين في الغرفة. (كان زيمرمان نفسه لا يزال في بولدر). وتحول الحدث إلىٰ عمليَّة تبادل مفاتيح، حيث تبادل الجميع مفاتيح بي جي بي العامة ووقَّعوا حلقة مفاتيح بعضهم البعض. فبعد كل شيء، كان برنامج بي جي بي تجسيداً لإيمان المجموعة بأن الكريبتوجرافيا أهم من أن تترك للحكومة، أو حتَّى للشركات ذات النوايا الحسنة. وحدهم الأفراد المخلصون، المستعدون لتحمّل النتائج المترتبة على العقوبات التي تفرضها الحكومة، هم الذين يستطيعون أن يضمنوا، تداول الأدوات عبر الدورة الدموية للإنترنيت. وفيما بعد، قال جون جيلمور: «إن قمع هذه التكنولوجيا يتطلّب وجود دولة أمنية قوية جداً».

ومن الأحداث الهامّة غير المتوقعة في المؤتمر ملاحظة أوردتها رفيقة هيوز، وهي كاتبة ترتدي الجلد، وتنشر كتاباتها في المجلة الهبية الرقمية «موندو 2000»، تحت اسم سانت جود. فبعد أن استمعت إلىٰ رؤى مجتمع متقلّب ذي رياضيات متكاملة، وجدت الرابطة التي تجمعهم بمن صعدوا مؤخراً وأطلق عليهم اسم «زعران الكومبيوتر»، متسلّلون إلىٰ الكومبيوتر تحولوا إلىٰ علماء بربطهم تحطيم المقذسات جهاراً الذي عرف به متمردون من أصحاب موسيقى الروك بالثورة الرقمية. صرخت المرأة يومئذ: «اسمعوا، إنكم زعران الشّيفرة!» ولقد هاموا جميعاً بهذا اللقب.

كانت المجموعة الملقبة حديثاً توّاقة لتجتمع ثانية خلال شهر من الزمن.

وفي تلك الأثناء، أعد إريك هيوز مكاناً للقاء، زعران الشّيفرة أكثر نشاطاً وخصباً: الإنترنيت. مستخدماً مخدم الشبكة لدى جون جيلمور، (كان اسم مجاله ضمن الشبكة Toad.com) كمحور العالم التخيلي، وأنشأ هيوز ما يُعرف بقائمة التخديم، وهو نقاش مستمر يجمع بين الملايين حيث يتلقى أي شخص سجل اسمه في قائمة البريد الإلكتروني الكامل مساهمات أي عضو آخر يهتم بتقديم أخبار أو نقد نظام تشفير، أو إطلاق العنان لحديث صاخب. وفي غضون أسابيع قليلة، سجل أكثر من 100 شخص أسماءهم على القائمة، وهو عدد مثير بالنظر إلى الحجم الهائل للرسائل المحررة والتي قد تصل إلى أكثر من 150 رسالة في اليوم.

بعدذ لك للقاء الأول، كتب أريك هيوز مسودة أطلق عليها اسم «إعلان نوايا قصير» وذلك لشرح ما ترمي إليه المجموعة. لقد تصور البيان الرسمي لزعران الشيفرة هذا، بنية سرية تم طبخها في البيت ولا يمكن للحكومة أن تفككها:

يكتب زعران الشّيفرة رمزاً. إنّهم يعلمون أن على أحدهم أن يكتب دفاعاً عن السرّيّة، ولما كانت المسألة هي سريتهم، فيكتبونها. ينشر زعران الشّيفرة ر مزهم ليتمكن رفاقهم من زعران الشّيفرة من التعامل معه وتشغيله. يدرك زعران الشّيفرة أن السرّيّة لا يمكن بناؤها في يوم واحد وهم صبورون مع التطور المتزايد.

إن زعران الشّيفرةلا يبالون إذا كنت لا تحب البرمجيات التي يكتبونها. إن زعران الشّيفرة يعلمون أن البرمجيات لا يمكن تدميرها. زعران الشّيفرة يعلمون أن نظاماً منتشراً على نطاق واسع، لا يمكن إيقافه.

إن زعران الشّيفرة، يجعلون الشبكات آمنة للسرّيّة.

بعدذ لك بيومين، أعلن هيوز تفاصيل للقاء الثاني، والذي سيقام في 10 تشرين الأول/ أكتوبر في المقر الجديد لشركة سانيوز في ماونتين فيو. وقد

كتب في هذا قائلاً: «إن الحضور ثقة مختلفة الأعماق. ادعوا من تشاؤون... لكن لا تنشروا الإعلان. فيحين وقت ذلك».

وهذا ما كان فعلاً. فبحلول العام التالي اتسعت القائمة لتشمل أكثر من 700 مشترك. وقد تلاشت مقاومة المجموعة في الأساس لمنع الصحفيين من حضور لقاءاتهم، وهو موقف مثير للسخرية مأن شخا ص متحمسين جداً لنشر المعلوما ت في عصر الإنترنيت. وسرعان ما أصبحت أخبار المعارف المكتسبة لزعران الشّيفرة مادة رئيسة في مطبوعات تتراوح من مجلة وايرد إلىٰ نيويورك تايمز. (وجوههم تختبئ وأراقنعة عليها خربشا ت منبصما ت المفتاح العام لبرنامج بي جي بي، كانت تزينا لعدد الثاني من مجلة وايرد). لقد أصبح لوجه الشّيفرة مسحة علمية مستحدثة.

كانت فوضى التشفير مفهوماً ساحراً، لم تقتصر عدواه على وسائل الإعلام فحسب، بلانتشر ت لتشمل أوساط الشركات الضخمة الحسنة التنظيم والحكومة كذلك. حتّى دون باركر، وهو خبير أمني معروف وكانت له خبرة قديمة، لتخصصه في تقييم متلصصي الكومبيوتر، أَخذ الآن يفكر ملياً في الأخطار الناجمة عن «حالة فوضىالمعلو ما ت القادمة إذا ما سمح للشيفرة أن تنتشر دون ضابط وهي علىحا لتها الراهنة». (أوصى باركر بشيفرة قوية، شرط أن تكون المفاتيح الأصلية في أيدي الحكومة ـ وقد اتضح أن الحكومة كانت تنظر في هذا الأمر).

لكن مع أن ثوار الشّيفرة، أصبحوا الأثيرين لدى الإعلام، وخطراً يتهدد الحكومة، وأبطال الحريات المدنية، إلاّ أن قلة كانت تدرك أن الأساس الرياضي والفلسفي لجهودهم قد تأتى من رجل واحد، يجادل فيه البعض بأنه قمة زعران الشّيفرة. لم يحضر لقاء على الإطلاق، ولم يسجل اسمه في القائمة، وفي الواقع كانت له خصومة شديدة مع بعض أفراد المجموعة. وبالرغم من ذلك، فإن أفكاره وبراءات الاختراع التي كان يحتفظ بحقه فيها عند

تطبيقها، كانت تناقش برهبة وخوف، في عالم الشركات الكبيرة والاستخبارات. كان المبتكر نفسه، واحداً من أكثر الألغاز المحيرة في هذا الحقل، وحله أصعب من حل معيار تشفير البيانات الثلاثي. كان هذا الرجل ديفيد تشوم.

كان تشوم رجل ذو لحية وشعر طويل، يربطه بشكل ذيل حصان، وهو كريبتوجرافي من بيركستوكد ورجل أعمال. وقد تخرّج من جامعة بيركلي، وبمبادرة منه، استمرت مؤتمرات الكريبتو في البقاء، كما نظم الجمعية الدولية لأبحاث علم الشّيفرة. لكن إرثه في عالم الشّيفرة امتد بعيداً، وتجاوز هذه الحدود: فلعدد من السنين كان دون كيشوت ثورة السرِّيَّة، ويسعى بمثالية إلىٰ تحرير الشّيفرة من قبضة الأخ الكبير. ومنذ أن كان على مقاعد الدراسة في جامعة بيركلي في واخر السبعينات، أخذ في البناء على أساس المفتاح العام، من أجل ابتكار بروتوكولات لعالم يمكن للناس فيه القيام بما يشاؤون من العمليات الإلكترونية وهم محافظون على هويتهم مغفلة من الاسم. وإذا كان استخدام المفتاح العام شبيهاً بالسحر، وإذا كانت التطويرات مثل تبادل الأسرار وبراهين المعرفة الصفرية تعتبر أمثلة قوية على هذا السحر، فإن ديفيد تشوم كان بمثابة الساحر «هوديني» بالنسبة للشيفرة، فقد اخترع أدوات في الرياضيات يمكنها أن تأتي بالمستحيل: منافع العالم الإلكتروني كلها من دون مثالب الطريق الإلكترونية التي يمكن أن ترشد المحتالين، والشركات الكبرى، وعناصر الشرطة إلىٰ عتبة بيتك. إن ذلك السحر يملك إمكانية، كما يعتقد البعض، أن يجعل مفهوم الدولة برمته يختفي.

أبدى ديفيد تشوم، منذ نعومة أظفاره، اهتماماً بالعتاد المتصل بالسرِّيَّة. ويقول: «أعتقد أن من المهم إدراك، أن هناك قوة تدفعني بشدة. ولقد جاء اهتمامي بأمن الكومبيوتر أساساً، والتشفير لاحقاً، من افتتاني بتقنيات الأمان عموماً ـ أشياء مثل الأقفال وأجراس الإنذار والخزائن الفولاذية». (وفي فترة ما،

عندما كان طالباً في الدراسات العليا، ابتكر تصميماً جديداً لقفل، وكاد أن يبيعه لمصنع كبير). وكان، بالطبع، مفتوناًبا لكومبيوتر. نشأ تشوم وترعرع في إحدى ضواحي لوس أنجليس، في عائلة يهودية من الطبقة الوسطى (لم يتحدد تاريخ ميلاده بسبب ما هو معروف عنه، من ميل لعدم إفشاء مثلهذه ا لتفاصيل ا لمحددة للهوية). واشتغل منذ أن كان على مقاعد الدراسة الثانويةفا لجامعية، بدأ بحضور ا لمحاضرات في جامعة كاليفورنيا بلوس أنجليس قبل أن ينال الشهادة الثانوية، ثم التحق بجامعة سونوما الحكومية ليكون قريباً من صديقته، وانتهى بنيل الشهادة الجامعية من جامعة كاليفورنيا بسان دييجو ـ بأعمال الكومبيوتر المتنوعة المألوفة على سبيل التسلية: مثلا كتشاف كلمةا لسر، والبحث في سلة المهملات وما شابه ذلك. وفي دروس الرياضيات كان يصاحب أمثاله من الرفاق الساخطين: إذ كانوا يجلسون في المقاعد الخلفية، ويدأبون على الرد علىالأ ستاذ حينما يأتي بخطأ، فيأتون ببرهانمناقض لقوله. (لم يكونوا مشاغبين بالمعنى الدقيق للكلمة، لكنهم كانوا يتحلون بالجرأة في مجال الكومبيوتر). كذلك تحقق له أن ينال معرفةا ُساسية جيدة بالرياضيات. ثم في و قت متأخِّر منحيا ته الجامعية، وقّع على موضوع الكريبتوجرافيا، وإذا نظر المرء إِلىٰ تلك المقدمات يرى أن هذا التطور في حياته كان من طبيعة الأمور.

لطالما كان يفكّر في أمر الوسائل التي توفر الحماية للمعلومات الموجودة في الكومبيوتر، لكنّه أظهر أفكاره الجادة الأولى في هذا الموضوع في حلقة بحث قدّمها في مادة اللغة الإنكليزية. فالمدرسة الشابّة ذات الاتجاهات الراديكالية فيللسيا سة التي تدرس هذه الماكا نت قد حثّتا لطلاّب على ا لكتابة عن أمور تثير اهتمامهم فكتب تشوم عن التشفير.

اختار تشوم جامعة بيركلي للتحضير للدرا سات العليا، وذلك بسبب ارتباطها بالنموذج الجديد لكريبتوجرافيا المفتاح العام. كان يعلم أن لانس هوفمان، الذي كان يدرس هناك، هوأ ستاذ رالف ميركل. لكنّه لم يكن يدري أن

هوفمان قد رفض النظر في آراء ميركل. ومع ذلك، فقد عقد صلات جيدة في الجامعة ـ حتّى أنه التقى هويت ديفي الذي كان يعيش في بيركلي آنذاك ـ وحصل على الدعم الذي يحتاج إليه ليبدأ عمله الخاص. وإن أوراق تشوم الأولى، التي طبعت عام 1979، تفصح عن المنحى الذي ستتخذه أعماله: ابتكار سائل كريبتوجرافية لضمان السرِّيَّة. وكانت أفكاره مبنية على مفهوم المفتاح العام، وبشكل خاص على ميزات التحقّق من التوقيع الرقمي. ويقول: «لقد أصبحت مهتماً بهذه التقنيات على وجه الخصوص لأنني أردت عمل بروتوكولات تصويت مغفلة الاسم. ثم أدركت أن مكان المرء استخدامها بشكل أكثر عمومية كنوع من بروتوكولات الاتِّصالات التي لا يمكن تعقبها». وإن سلوك هذا الدرب يؤدي، إلى نقود رقمية مجهولة المصدر ولا يمكن تعقبها.

يرى تشوم أن السياسة والتكنولوجيا تعززان بعضهما البعض. أما بالنسبة للسرِّيَّة، فكان يعتقد أن المجتمع يقف على مفترق طرق. وأن المضي في الاتجاه الذي نسير فيه حالياً، سوف يحملنا إلى حيث تحققت سوأ نبوءات أورويل. وقد صور المشكلة بدقة في بحث بعنوان «الأرقام، يمكن أن تكون شكلاً للنقد أفضل من الورق»:

إننا نقترب بسرعة من لحظة تخاذ قرار حاسم، وربما لا يمكن الرجوع عنه، وهو يتصل بالاختيار لا بين نوعين من الأَنظمة التكنولوجية، بل بين نوعين من المجتمع. فالتطورات الجارية حالياً في تطبيق التكنولوجيا جعلت ما تبقى من ضمانات للسرِّيَّة والحق في الوصول إلى البيانات الشخصية وتصحيحها مسألة جوفاء بلا معنى. وإذا استمرت هذه التطورات فإن إمكانياتها العظيمة في الرقابة ستجعل حياة الأفراد مكشوفة للرصد، وضعيفة أمام السلطة على نحو لا سابق له.

في أوائل الثمانينات، أجرى ديفيد تشوم بحثاً لإيجاد حل لمشكلة، بدا أن من المستحيل حلها، لأن الكثير من الناس لا يعتبرونها مشكلة بالمقام

الأول: كيف يمكن لميدان الحياة الإلكترونية أن يتوسّع دون تهديد سريتنا؟ أو بعبارة أكثر جرأة، هل بإمكاننا القيام بذلك عن طريق زيادة السرّيّة فعلياً؟ وفي غضون ذلك اكتشف كيف يمكن للكريبتوجرافيا أن تنتج نسخة إلكترونية من ورقة الدولار.

من أجل تقدير ذلك على نحو كامل، على المرء أن يفكر في المعوقات أمام مهمة كهذه. فالأمر المقلق على نحو مباشر لأي شخص يحاول إنتاج شكل رقمي للعملة هو تزوير العملة. كما أن أي شخص قام بنسخ برنامج من قرص مرن إلى سواقة صلبة يعلم أنه أمر بمنتهى البساطة إنتاج نسخة مطابقة تماماً لأي شيء في الحقل الرقمي. فما الذي يمنع إيف من أخذ دولارها الرقمي الوحيد وإنتاج مليون أو بليون نسخة عنه؟ إذا كان بإمكانها القيام بذلك فإن كومبيوترها النقال، وكل كومبيوتر، آخر يصبح آلة لصك العملة، وإن تضخماً مفرطاً يجعل مثل هذا النوع من العملة لا قيمة له.

كانت طريقة تشوم في التغلّب على المشكلة هي استخدام تواقيع رقمية لتأكيد صحة الأوراق النقدية. يتم تحديد قيم متسلسل وحيد لـ «ورقة نقدية» معينة ـ ويصبح الرقم نفسه هو الورقة النقدية ـ وعندما يتم تقديم هذا الرقم الفريد إلى تاجر أو مصرف، فبالإمكان فحصه بدقة لمعرفة إذا كانت الورقة الفعلية أصلية ولم تصرف من قبل. سيكون القيام بذلك سهلاً إذا تم تعقّب كل وحدة إلكترونية للنقد عبر النّظام في كل نقطة، لكن هذه العمليّة يمكن لها أن تتعقب الطريق التي يصرف الناس فيها أموالهم، حتّى آخر قرش منها. وهو بالضبط ذلك النوع من كابوس المراقبة، الذي يخيف تشوم. فكيف يمكنك القيام بذلك وفي نفس الوقت تحمي إغفال ذكر اسم المرء بشكل مطلق.

بدأ تشوم حله، عن طريق الإتيان بشيء يدعى «التوقيع الأعمى». وهي عملية يمكن للمصرف من خلالها، أو أي وكالة مخولة، إثبات أصالة رقم بحيث يمكن له أن يقوم بعمل وحدة نقدية. مع ذلك فباستخدام عمليات تشوم

الرياضية، فإن المصرف ذاته لا يعلم من لديه الورقةا لنقدية، ولذلك لا يستطيع تعقبها. وبهذه الطريقة، عندما يعطيك المصرف سيلاً من الأرقام التي صُمِّمت لأن تقبل على أنّها نقد، فإن لديك طريقة لتغيير الأَرقام (لتضمن أن الأموال لا يمكن تعقبها) وفي الوقت ذاته تحافظ على موافقة المصر ف.

كانأ حد أكثرشوفا ت تشوم أهمية قد حصل، عندما استطاع أن يبرهن رياضياً، على أن هذا النوع من إغفال الاسم، يمكن توفيره على نحو غير مشروط. و جاء ت لحظة الإلهام عندما كان يقود سيارته الفولكسفاكن الفانمن بيركلي إِلىٰ بيته في سانتا بربارة، حيث كان يدرِّس علوم الكومبيوتر في أوائلالثما نينا ت. ويصف ذلك بقوله: «كنت أقلب هذه الفكرة مرّات ومرّا ت في رأسي، ودرست الحلول كلها بعناية. ثم أمعنت التفكير في الأمر، وأخيراً في الوقت الذيتو صلت فيه إِلىٰ الحل، عرفت تماماً طريقة القيام به على أحسن وجه».

وقد قدم نظريته مع مثال حي: سيناريو عن ثلاثة كريبتوجرافيين، انتهوا مرتناول طعام ا لعشاء في مطعم وينتظرون الفاتورة. يظهر النادل ويقول لهم، أن الفاتورة دُفعت مسبقاً. والسؤال هو، من الذي دفع الحساب؟ هل قرَّر أحد لحا ضرين أن يدعو زملاءه دون إعلامهم بذلك ـ أم أن وكالة الأَمن القومي أَو شخص آخر قام بدفع ثمنوجبة ا لعشاء والمعضلة هنا ما إذا كان بالإِمكان الحصول على هذه المعلوما ت دون كشف هوية الكريبتوجرافي، الذي يحتمل أنَّه دفع ثمن العشاء.

إن حل مشكلة «عشاء الكريبتوجرافيين» كان بسيطاً علىنحو يدعو للدهشة، فهو يتضمن رمي قطعة نقد مخفية عن أنظارأ شخا ص معينين عدة رميا ت. فعلى سبيل المثال، يمكن لكل من أليس وبوب، أن يقوما برمي قطعة النقد عدة مرا ت خلف قائمة ا لطعام بحيث لا يستطيع تيدروْ يتها، ثم يقوم كل منهما بكتابة النتيجة على انفراد وتقديمها له. والشرط الأساسي أنَّه في حال كان أحدهما، هو المضيف لكريم الذي دفع ثمن لعشاء، فإن ذلك الشخص

سيكتب النتيجة لمعاكسة لرمي قطعة النقد. وهكذا إذا تلقى تيد تقرير ين متضاربين لرمي قطعة النقد ـ واحدة طغراء، وأخرى نقش ـ فإنه سيعلم أن أحد الذين تناولوا لعشاء قد دفع الحساب. ولكن بدون تواطؤ آخر ليس لديه طريقة لمعرفة أيهما الذي دفع، أليس أم بوب. وعن طريق سلسلة من رميا ت النقد وتمرير الرسائل، فإن أي عدد من متناولي العشاء ـ في ما يدعى شبكة عشاء الكريبتوجرافيين DC-Net ـ بإمكانهم أداء هذه اللعبة. ويمكن للفكرة أن تكون مقياساً لنظام النقد. و يقول تشوم: «إن هذه الفكرة هامة جداً، لأنّها تعني أن استحالة التعقب يمكن أن تصبح حالة مطلقة. ولا يهم ما لدى وكالة الأمن القومي من كومبيوترات قوية لفك الرموز ـ فلن يستطيعوا ا كتشافها، وبإمكانك إثبات ذلك». وهو يعني أنّها رياضياً بمثابة واق من الرصا ص.

إن أعمال تشوم اللاحقة، وكذلك براءات الاختراع التي تقدم بها بنجاح، قد تأسّست على تلك الأ فكار، وتعالج مشكلا ت مثل الحيلولة دون الإنفاق المزدو ج مع الحفاظ على إغفال اسم المنفق. وبخدعة رياضية ذكية بشكل خا ص، توصل إلى خطة يمكن من خلالها المحافظة دوماً على إغفال الاسم، باستثناء حالة واحدة: إذا أقدم الشخص على عملية إنفاق مزدوج، لوحدة نقدية كان قد سبق له أن أنفقها في مكان آخر، عندئذ يسمح الجزء الثاني من ا لمعلومة بالتعقب، والاستدلال على ا لمصدر. وبتعبير آخر، فإن ا لغشاشين وحدهم يمكن تحديد هويتهم با لفعل. وبعملهم هذا يكونوا قد قدّموا دليلاً، لقوى حفظ النّظام على محاولتهم الاحتيال.

كان ذلك عملاً مثيراً، لكن تشوم لم ينل من التشجيع على المثابرة إلاّ القليل. وفي هذا يقول: «كان من الصعب جداً بالنسبة لي أن أعمل في موضوعات كهذه في هذا الحقل لسنوات كثيرة، لأن الناس لم يكونوا يتقبّلون الأمر على الإطلاق». ففي أوائل ثمانينا ت وعلى مدى سنين كثيرة، حاول تشوم عقد صلا ت شخصية مع الشخصيات الهامّة والمشاعل الهادية التي تحدّد سياسة السرّيّة وبسط لهم أفكاره.

يقول تشوم: «كان رد الفعل الرسمي سلبياً، ولم أتمكّن من فهم السبب. وهذا جعل من الصعب علي الاستمرار في متابعة العمل، ذ لك أن المستشارين الأكاديميين الذين كنتأر جع إليهم في البحث، كانوا يقولون، «إن هذا موضوع سياسي،وذ لك اجتماعي، لقد تجاوزت الحد». حتّى مستشاره في جامعة بيركلي حاول أن يثنيه عن متابعة البحث، قائلاً لتلميذه العنيد: «دعك من هذا الموضوع، إنك لا تستطيعأ بدأ أن تتنبأ بتأثير فكرة جديدة على المجتمع». وعوضاً عن الإصغاء للتحذير، قام تشوم بإهداء أطروحتهذ لك المستشار، قائلاً: إن رفضه لتفكير مستشاره هو ما حثّه على إنهاء العمل.

وأخيراً، قرّر تشوم، أنّ فضلطريقة لنشر أفكاره هي إنشاء شركته الخاصة. وفيذ لك الوقت كان يعيش فيأ مستردام؛ ففي زيارة سابقة لهذه المدينة مع صديقتهالهو لندية، التقى مصادفة ببعض الأكاديميين، وعُرض له أن يشغل منصباً، وهذا قاده لأن يصبح موظفاً، في مركز الرياضيات وعلوم الكومبيوتر في أمستردام CWI. وهكذا أسّسفي عام 1990 شركة ديجيكاش، برأسماله القليل وعقد جاهز في يده من الحكومة الهولندية لدراسة الجدوى الاقتصادية لتقنية تتيح دفع رسوم الطرقات العامة إلكترونياً. طور تشوم نموذجاً أولياً حيث يثبت على زجاجا لسيارة بطاقات ذكيةتحمل ما يعادل مبلغاً معيناً من المال وتقوم أجهزة فحص سريعة جداً باقتطاع الرسوم فيما السيارات تمر مسرعة بجانبها. كذ لك يمكن للمرء استخدام البطاقا ت لدفع تكاليف استخدام وسائط النقل العام، وأخيراً لأشياء أخرى. وبالطبع فإن الدفع يتم وتبقى هوية الدافعين مغفلة. فبالنسبة لتشوم كان هذا أكثر الأجزاء أهمية في النظام: وخوفه هو أن خطة تتيح للمسؤولين تعقبا لمواطنين على الطرقات ستكون واحدة من الأهوال التي عرض لها أورويل. (الأنظمة التي طبقت أخيراً في الولايات المتّحدة، مثل نظام E-Z Pass الشهير تقوم فعلاً بتعقب المسافرين).

بعد إنهاء ذلك العقد (لم يطبق النظام أبداً)، استمر تشوم في تشغيل

شركته في تطبيقات البطاقة الذكية؛ وركزت بعض المشاريع على أنظمة نقد يمكن استخدامها في عمارة أو مجمع من الأبنية. وكان لديه مثال عملي في المقر الرئيسي لديجيكاش في أطراف أمستردام؛ يمكن للزوار أخذ عينة عن المستقبل، عن طريق استخدام بطاقات نقد مغفلة الاسم، لشراء الصودا وإجراء المكالمات الهاتفية.

لكن في أوائل التسعينات، وحتّى مع إدراك العالم لأهمية أفكار تشوم التي أنتجها في العزلة. إذ أن شركات مثل مايكروسوفت وسيتي بنك كانت تسعى وراء مشاريع النقد الرقمي، فإن نطاق عمليات الشركة [ديجيكاش] كان ما يزال ضيقاً نسبياً. وظلت ديجيكاش مستقلة، ولم تدخل في تحالف وثيق مع شريك كبير، في مجال المصارف أو الخدمات المالية. شعر تشوم أن هؤلاء الشركاء، أو على الأقل من سيحصلون على رخصة استخدام تقنية ديجيكاش سيظهرون مع مرور الزمن. وأنّهم لا بد أن يظهروا. وقد أصبح الرأي المتفق مع الحكمة الآن، أن الأرقام المحمية بالشّيفرة سوف تحل محل الأوراق النقدية. وعندما يحصل ذلك. فإن الصيغ الرياضية التي ابتكرها ستصبح عاملاً حاسماً في الحفاظ على السرّيّة، في عصر الأموال الإلكترونية. كانت هذه هي الفكرة التي اعتقد تشوم أنّها جديرة بالمتابعة والتمسّك بها.

رأى البعض في هذا الموقف عناداً ومكابرة، أو على الأقل، ضعف في الخبرة التجارية. ويقول موظف سابق في ديجيكاش: «أراد الناس شراء براءات اختراع ديفيد لكنّه كان يبالغ في ما يطلبه». وهناك قصة أخرى شائعة هي أن تشوم قرّر في آخر لحظة رفض صفقة مع شركة فيزا والتي كانت ستجعل ديجيكاش معياراً للأموال الإلكترونية. وقد أخبر مدير تنفيذي في ديجيكاش أحد المراسلين عن حالات فشل مشاريع عقود مع شركات أخرى، بما فيها مايكروسوفت. لكن تشوم قاوم بشدة نظرية أن شذوذ طباعه وتصرفاته أعاقت عقد صفقات هامة. وعندما أجرى أحد المراسلين، مقابلة معه حول هذا

الموضوع، اندفع تشوم يرد بعنف: «إنه افتراء خبيث القول أن من الصعب عقد اتفاقات معي». ومع ذلك، فقد بدأت بعض الشركات ـ التي شعر ت بالإحباط لعدم قدرتها على الحصول على براءات اختراع تشوم ـ بابتكار مشاريعها الخاصة فيما يتعلّق بإبقاء الاسم مغفلاً، والتي قد تكون انتهكت، أو لعلها لم تنتهك براءات اختراعه.

شعر بعض زعران الشّيفرة أن تشوم، اتّخذ توجهاً غير لائق أيديولوجياً بتقدّ مه لطلب براءات اختراع لأعماله. (كذلك كان هؤلاء المثاليين غير معجبين ببراءات اختراع آر إس إيه، أيضاً). وكانوا يشتكون أنّه بحجبه التكنولوجيا عن أي شخص يريد تطبيقها ـ وتهديده بمقاضاة أي شخص اختبر آفاق براءات الاختراع هذه ـ كان في الواقع يحول دون تحقيقأ حلا مه. وأثار هذا النقد غضب تشوم، وردّ بالقول: «إني أعتقد بأن أمراً كهذا ربما كان ممكن التحقيق، وشعرت بحق أن القيام به هو مسؤوليتي. وما من أحد كان يعمل على هذا مدة ست سنوات بينما كنت منشغلاً أعمل فيه والجميع يظن بي الجنون. إن براءات الاختراع مفيدة جداً لشركتنا الصغيرة؛ ولم يكن بالإمكان الحصول على ترخيص للعمل دون براءات الاختراع، ومن وجهة نظري فإن الهدف منها هو إخراج العمل إلىٰ حيّز الواقع».

كان زعران الشّيفرة يؤمنون، بأن بروتوكولات إغفال الأسماء سو ف تلاقي رواجاً. وأن ذلك نتيجة محتومة. وحاولا لعديدون القيام بمشاريعهم الخاصّة، مستخدمين أسماء مثل ماجيك موني. وفي نفس الوقت، كان سيتي بنك وفيزا يدرسان النقد الرقمي بمعزل عن الآخرين. وتهيّأ سيس شركة جديدة بدعم مادي جيد خارج واشنطن العاصمة دعيت سايبركاش؛ وكانت شركة آر إس إيه داتا سيكيوريتي أحد المستثمرين فيها. وأراد زعرانا لشّيفرة معرفة ما إذا كان هذا الشكل الجديد من المال سو ف يسمح بتعقّب المستخدم إلكترونياً. وكانوا يأملون بألاّ يكون الأمر كذلك. كانت لائحتهم مليئة بالسيناريوها ت ومنها أن

لإ نترنيت توفر «ملاذاً للبيانات» خارج الولايات المتّحدة. في أماكن خارج نطاق سلطةالدول ا لصناعية الكبرى حيث بإمكان الناس إيداع أموالهم في البنوك، أو حتّى المقامرة باستخدامإ لنقد الرقمي. وعندماسا عد بعض زعران الشّيفرة في تنظيم أول مؤتمر حول الكريبتوجرافيا المالية كان اختيارهم لمكان انعقاده في إنجويلا أمراً حتمياً. ذلك أنّها جزيرة صغيرة في الكاريبي قوانينها التجارية، أقل ما يقال فيها، أنّها حرّة.

كا نت إحدى أفكار تشوم التي تبنّاها زعران الشّيفرة بإخلاص، ظهور خدمات تدعى «مدورو الرسائل». وهي نوع من منظفي المعلومات... مواقع أمامية على طريق المعلومات السريعة، يحافظ عليها بشكل مستقلنا شطون من زعران الشّيفرة، ينتزعون أي إشارة مميزة عرإلر سالة، ويرسلونها إما إلىٰ وجهتها الأخيرة، أو إلىٰ مدور آخر للرسائل، لتخضع لجولة أخرى من تنظيف البيانات. تدخلر سالتك في مدور الرسائل (والذي يُعرف كذلكبا سم المخدم المجهول) ومعها عنوان المرسل، وتستمر في طريقها دون العنوان.

إن مجرد إرسال رسالتك مغفلة الاسم إلىٰ مدور واحد للرسائل، على الرغم مرإ عتباره حماية غير كافية، فإنّها في الواقع تعطي الشخص الذي يسيِّر المخدم سلطة بالغة. وإذا اتضح أنه غير جدير بالثقة، أو تم التسلل إليه، أو سلّم مذكرة إحضار، فيكون من السهل جداً على الدخلاءا لحصول على عنوان المرسل. كانت تلك نفس المشكلة التي اشتكى منها هويت ديفي أصلاً والمتعلّقة بمديري الشبكة وكلمات السر. واعتقد زعران الشّيفرة أن لديهم الحل للتغلّب على هذه المشكلة: إذا تعاونوا على إنشاء اتحاد حر من مدوري الرسائل حول العالم. وللحصول على حماية فعلية، عليكتو جيو سائلك عبر سلسلة، من مدوري الوسائل.كل خد مة تدويرللر سائل ستنزع عنوان المرسل؛ وسيكون لدى المخدم الأول وحده العنوان الأصلي. عندئذ على الشرطي أوا لجا سوس الذي يحاول تعقب رسالة ما الحصول على سجلات

عشرة أو اثني عشر أو عشرين مدوررللر سائل (إذا كانت السجلات ما تزال موجودة، والتي على الأغلب غير موجودة) وذلك ليقتفي الأثر ليصل إلى المصدر. لذا إذا لم تستطع السلطات الحصول على السجلات من أحد مدوري الرسائل الجريئين في تونجا، فإنّهم لن يعثروا على السجلات الأصلية أبداً. (إن بعض المستخدمين، الذين لديهم جنون اضطهاد [بارانويا] ـ أو على الأرجح زعران شيفرة يعرضون برمجياتهم ـ قد مروا عبر نحو مئة مدور للرسائل في سلسلتهم؛ ولما لم يكن هناك هذا العدد الكبير من المخدمين المجهولين في العالم، فإن الأمر يقتضي القيام بعدة جولات).

لكي تتأكّد بالفعل من إغفال اسمك وحماية سريته، عليك استخدام برنامج بي جي بي لتشفير الرسالة كلها با لمفتاح العام لمدور الرسالة الأخير في السلسلة وبهذه الطريقة لن يتمكّن من قراءتها أي مدوررللر سائل سوى الأخير في السلسلة، وتكون الرسا لة في ذلك الوقت قد اختفتأ صولها تماماً. أتريد إجراءات وقائية أكثر إحكاماً؟ شفّر تلك الرسا لة الأخيرة في مغلف آخر من تشفيربي جي بي ويتم اهبلا ستخدام المفتاح العام لمدور الرسائل قبل الأخير في السلسلة. وسيؤمن ذلك طبقة مضاعفة من التشفير. وهكذا دواليك، مغلفات ضمن مغلفات أخرى، حتّى تكفل السرّيّة التامة. ففي أي نقطة على طول الطريق، إذا حاول شخص ما قراءة لر سالة، فلن يحصل إلاّ على كلام غير مفهوم. وقد وصف إيريك هيوز ذلك بسرور: «مثل الحصول على شريط من همس الميكروفون».

بتشجيع من زعران الشّيفرة، أسّس هيوز أول مدوررللر سائل على مخدم بيركلي، وبحلول عام 1993 كان هناك نحواً من عشرين مدوررللر سائل يعملون بنشاط. ومن بين جميع الجهود الحثيثة التي بذلها أفراد القائمة، كان أقواها ابتكار طريق أسهل للإفادة منسلا سل مدوري الرسائل. ويبدو أنّه لم يزعج زعران الشّيفرة عدم قيام هذا النّظام الناشئ بأي شيء لتحسين المجتمع. فمعظم

الرسائل المرسلة عبر مدوري الرسائل، كانت كتابات موجهة إلىٰ مجموعات النقاش من مستخدمي الشبكة عبر الإنترنيت؛ والأمر المحزن أن هذه الرسائل كانت على العموم مضايقات متلاحقة، لأشخاص أو مجرد ثورات غضب حمقاء. وعوضاً عن إغناء حوارات عالم الكومبيوتر، فإن هذه القنابل النتنة الخالية من التوقيع قد حطّت من هذه الحوارات. قد يكون هناك اتصال بين عدد من الزملاء المثقفين يتحاورون حول مسائل تقنية أو أمور شخصية، ويقوم أحد الحمقى بمقاطعتهم ويلقي إهانات بملء فمه، فيشعر المشاركون الجادون في النقاش بالإحباط، لأنه ما من طريقة لتطبيق عقوبات، على مخرّب الاتّصالات الذي أفسد صفاء الجو. من جهة أخرى، في بعض الجماعات، وبالأخص تلك التي تشجع المساهمات من أصحاب الوجدان الاجتماعي اليقظ، أو ضحايا الجرائم الجنسية. من ناحية أخرى فإن مرسلي الرسائل المعارضين اكتشفوا إجراء للسرّيّة وذلك بترميز رسائلهم بما ينسبها إلىٰ هويات أطراف أخرى لا يمكن اقتفاء أثرها إنما تُعرف بـ «أسماء» ولم يكن بالأمر الغريب في مجموعات كهذه أن ترى الكثير من البريد من مراسلين واضح فيهم التخفي وراء عبارات في مواقع مثل bogus@no.return.address.

إن أصعب جزء في تشغيل مدور الرسائل، كما اتضح، لم يكن تقنياً. فقد يسّرت نصوص زعران الشّيفرة على لمؤهلين تقنياً ولو كانوا غير مختصين بالكريبتوجرافيا عملية إنشاء مخدم مجهول. فالجزء الصعب هو الوقوف في وجه الضغوط الاجتماعية والقانونية والتي ستظهر عندما يطالب المستهدفون من بريد الكراهية ومحبي المزاح بإيقاف المسالك المغفلة الاسم. ومن الحالات النموذجية حالة أزعر الشّيفرة في جامعة واشنطن الذي استخدم نظام كومبيوتر الجامعة مدورا للرسائل. مضت الأمور على أحسن ما يرام عدة شهور، وكتب المشغل: «لم يكن الأمر سيئاً إذا أخذت بالاعتبار أنه يستند إلىٰ معاناة طالب مع إدارة شبيهة بالحكم النازي. وجاءت الضربة القاضية عندما تقدم إلي أحد المستهدفين، [من هجمات البريد الإلكتروني] يشتكي من أن أحدهم يرسل له

رسائل بغيضة عبر مدور الرسائل الذي أقوم بتشغيله». ووصل طلب إيقاف هذا النوع من البريد إلىٰ «مدير بريد» لنُظام، الرجلا لمسؤول عن نظام البريد الإلكتروني في الجامعة. وبالطبع، لم يكن المدير يعلم شيئاً عن كون خدمة كهذه يتم تشغيلها على كومبيوتر الجامعة، «لقد فوجئ كثيراً حينما درس الأمر!» وتلك كانت نهاية مدور الرسائل.

أما حالة يولف هيلسينجوس فكانت أكثر نجاحاً، وكان هذا فنلندياً خبيراً بالكومبيوتر، بدأ في عام 1993 بتشغيل مدورللر سائل في منزله خارج هلسنكي. إذ أراد التغطية على أشخاص ضمن مجموعة مستخدمي الشبكة (يوسنت جروب)، يتراسلون حول قضايا معالجة الإدمان على الكحول. وقد أنشأ «بينيت» (وهو تحويرلا سم شركته بينيتيك) على جهاز يونيكس يعمل برقاقة متواضعة الإمكانات من نوع إنتل 386. وأطلقه للعمل معتمداً بشكل كلي على مصداقية كلمة المستثمرين. وسرعان ما أصبح آلاف الأشخاص يرسلون عبر الجهاز، الذي يرسلها إلىٰ وجهتها دون الرأسيةالتي تحدّد هوية المرسل. ولما أصبحت حركة المراسلة شديدة الكثافة اضطر جلف إلىٰ أن يركب في منزله أنبوب إنترنيت[للمعالجة التواصلية] ذا سرعة عالية، كانت تكلفته ألف دولار شهرياً. وفي بعض لأ حيان، يكتب له بعض المستخدمين يسألونهما ا لذي دفعه إلىٰ هذا العمل. وكان الجواب معقداً: ذلك أن جلف ينتمي إلىٰ أقلية تتحدّث السويديقي فنلندة وهو يؤيد دعم الأقليات للتعبير عن آرائها. ومن جهة ثانية فإنه يعتبره هواية. ويقول: «ينفق البعض مبالغ مماثلة على الغولف أو أي شيء آخر». وعندما اشتكى البعض من أنّه كان يسمح لأشخاص بغيضينومنحر فين للتعبير عن أنفسهم، رد على ذلك بالتالي:

لا يعني إلاّ أن أجيب باعتقادي الراسخ، بأنّه ليس لي أن أملي على لآ خرين تصرفاتهم. ولكن تذكروا أن الرسائل المغفلة هي امتياز، فلتستخدموها

على هذا الأساس. وأعتقد أن الأشخاص الناضجين يمكنهم التصرّف بمسؤولية. رجائي ألا تخذلوني.

مهما تكن النتيجة فإن جهد زعران الشّيفرة، الذي تمثّل في مدور الرسائل قد ولّد حواراً حيوياً حول قضية إغفال الاسم في المجتمع الرقمي. وكان أحد النصوص الهامة لزعران لشّيفرة لعبة إندر Ender's Game، وهو رواية من الخيال العلمي لأوسون سكوت كارد. وقد تمحور جزء من الحبكة على نقاش عام مؤثر بين اثنين من القلة سفة المغمورين استغلا تقنية مثل مدور الرسائل، لإ سالها تحت اسمين مستعارين هما ديموستين ولوك. ولما كانت الأفكار هذّامة، كان من الضروري جداً إبقاء هويتهما الحقيقية سراً، وبالرغم من ذلك فإن الحجج التي اعتمداها هذان كانت من القوة بحيث غيّرت مجرى المجتمع في الرواية. وثمة سبب آخر لإخفاء هوية الأشخاص الحقيقيين الذين وراء هذه الأفكار كون الكاتبين كانا طفلين، صبي وأخته يبلغ عمرهما اثنتي عشرة سنة وعشر سنوات على التوالي. وقال الصبي لأخته شارحاً: «ليس ذنبي إن كان عمري الآن ثلنتي عشرة سنة. إن العالم ديمقراطي دوماً في أوقات التغير، وسيفوز الشخص ذو الصوت الأكثر عذوبة».

ولكن لم يكن أدب الخيال العلمي وحده، الذي قدّر إغفال الأسماء حق قدرها. فهذه الممارسة كانت أمراً حاسماً في تشكيل الولايات المتّحدة ذاتها، وكانت على ما يذهب البعض تقليداً أمريكياً مثل فطيرة التفاح. وكما يحب مؤرخو زعران الشّيفرة أن يشيروا إلىٰ أن أنموذج النقاش ربما لمتلهم ا لنقاش الذي دار في رواية أوراق الفيدرالي The Federal list Papers، ومقتطفات من كتابات جيمس ماديسون، وجون جاي، وألكساندر هاميلتون ولكن نشرت باسم مستعار هوبو بليوس. وعندما كتب توماس بين كتابه Common Sense، كان قد وقّعه أصلاً تحت اسم رجل إنكليزي An English man. وقد أشارت المحكمة العليا «أن الكتيبات والكراسات وحتّى الكتب التي أغفل فيها اسم كتّابها قد

لعبت دوراً هاماً في تطور الإنسانية». وهو دور أيّدته المحكمة في قراراتها. وفي عام 1995، أعادت تأكيد ستورية المفهوم مرة أخرى، مستخدمة عبارات جون ستيوار ت ميل في تمجيد إغفال الاسم «درعاً يقي من طغيان الأكثرية». فمن يلوم زعران الشّيفرة لإنتاجهم أدوات كريبتوجرافية، لحفظ قدرة الكاتب على متابعة هذا التقليد الحيوي؟

الكثير من لنا س، كما تبيَّن فيما بعد، نقّاد ـ من بينهم مدير مكتب لتحقيقا ت الفيدرالي (إف. بي آي) لويس فريه ـ سيذهبون إلىٰ القول، أنه عندما ا نتشر ت الغفلية Anonymity [إغفال الاسم] عبر الإنترنيت، لم تجد مجرد بيئة ملائمة في وسيط جديد؛ بل تضخم أمرها بما يفوق كل تقدير، و تحوَّلت إلىٰ شيء أكثر خطورة. وأدّى اختراع ديڤيد تشوم للتواقيع الرقمية العمياء، و لنقد المجهول المصدر والذي لا يمكن تعقّبه، إلىٰ إمكانية جعل الفضاء التخيلي منطقة حرة الهوية حيثما مكان أحدهم أن يعمل سراً على نحوأ سهل بكثير وأكثر فاعلية منه في العالم الحقيقي، وعلى سبيل المثال، عندما تقوم بصرف عملة صعبة في متجر، لا يسألك أحد عن بطاقتك الشخصية، لكن وجهك سوف يسم الصفقة في ذهن أمين الصندوق، وخاصة إذا كنت زبوناً جيداً تتردد باستمرار. (إذا كنت تحمل حقيبة فوق رأسك، فعلى الأرجح أنّك ستجد صعوبة في تسديد الدفعات أ ساساً). وباستخدام بروتوكولات تشوم بإمكانك القيام بمشترياتك، وإرسال بريدك، وحتّى تلقّي الأموال مع ضمان تام بأنّه ما من أحد سيعلم من أنت. ولكن الأمر يصدق أيضاً على المختطفين، والعاملين في دعارة الأطفال، والإرهابيين، الذين ستصبح حياتهم أكثر يسراً وأماناً بأدوات كهذه.

إن هذه الهموم لم تكن مصدر قلق لزعران الشّيفرة. بل على العكس تماماً، إذ أنهم كانوا شديدي الحرص على بيان الأسباب التي تجعل تقنيا ت الغفلية موضوع خلاف وجدل. وكان المثال الجيد على ذلك، إعلان تيم ماي

عن تأسيس مشروع تجاري، أطلق عليه اسم بلاك نيت (الشبكة السوداء). وبالطبع، لم يكن للمجموعة وجود. بل كانت تجربة فكرية قرَّر طرحها للنقاش في اجتماع لزعران الشيفرة، لكنَّه بعدئذ قرَّر إطلاقها مغفلة على الشبكة. ويقول ماي: «لقد أرسلتها عبر مدوري الرسائل لإضافة لمسة من التوابل إليها». ولم يكن تيم ماي بالتأكيد يمانع في الإعلان عن معتقداته على الملأ (كان يوقع بريده الإلكتروني عادة بقائمة من أشكال العذابات التي تقشعر لها الأبدان «فوضى التشفير، النقد الرقمي، الشبكات مجهولة المصدر، اسم مستعار رقمي، الأسواق السوداء، انهيار الحكومات»).

كانت بلاك نيت، عرضاً مسرحياً هجومياً لتلك الاهتمامات. بدأت الرسالة «لقد استلفت اسمك اهتمامنا. ولدينا ما يحملنا على الاعتقاد، بأنَّك ربما كنت مهتماً بالمنتجات والخدمات التي تقدّمها منظمتنا الجديدة بلاك نيت. إن بلاك نيت تعمل في البيع، والشراء، والمتاجرة، وعدا ذلك فهي تتعامل بالمعلومات بكافة أشكالها». ويمضي العرض ليشرح بأنه بفضل كريبتوجرافيا المفتاح العام، قامت سوق سوداء رائعة للبيانات حيث يمكن للمرء أن يحصل على أو يبيع أي شيء من أسرار التجارة والصفقات إلى مخططات صواريخ كروز دون أي خطر من اكتشاف هويته. وأطراف الصفقات هذه لن يكونوا معروفين لبعضهم البعض، ولا حتَّى لبلاك نيت. وغني عن القول، أنَّه ما من أحد يملك أن يعلم من يقف وراء بلاك نيت:

إن موقعنا في الفضاء المادي غير ذي أهمية. فالمهم هو موقعنا في الفضاء التخيلي. عنواننا الأولي هو مفتاح بي جي بي لموقع «بلاك نيت» ويمكننا أن نتواصل (يفضل عن طريق سلسلة من مدوري الرسائل لمغفلي الاسم) عن طريق تشفير رسالة باستخدام مفتاحنا العام (المذكور أدناه) ووضع هذه الرسالة في واحد من مواقعنا العديدة في الفضاء التخيلي الذي نرصده.

بالإضافة إلى ذلك ادعت بلاك نيت بالتعامل بالمال، وعرضت القيام

بإيداع مجهول المصدر في البنك الذي تختاره. ويمكنك التعامل مع بلاك نيت باستخدام نقد حقيقي، أو «اعتمادات مشفَّرة»، وهي عملة بلاك نيت الخاصة والمتداولة داخلياً (يمكن استخدامها في أي نوع من صفقات المعلومات السرِّيَّة التي لا يمكن تعقّبها ولكأمر ا ختيارها). ولم يكن لبلاك نيت أي أيديولوجيا خاصة بها، ماعدا قولها: «إننا نعتبر الدول ـ الأمم، و قوانيا لتصدير، وبراءاتلا ختراع، واعتبارات الأمن القومي، و ما شابه، على أنها بقاياحقبة ما قبل الفضاء التخيلي».

ابتهج ماي، لقبول الكثيرين بإعلان بلاك نيت بمعناه الظاهر، وخاصة أن أنباء عنه قد تسرّبت إلىٰ أبعد من مجتمع الشيفرة، وإلىٰ عالمأكثر ميلاً للفزع عموماً. على الرغم من أن بلاك نيتكا نت وهمية، فإن ماي كان يعتقد أننا سوف نرى في المستقبل مشاريع مشابهة. ولم يقلقهذ لك على الإطلاق، فالناس عملاء أحرار، ومسؤولين عن أنفسهم. وقد قال: «إذلات أ شخاص نتيجة لذلك... إيه! إنني لم أعمل على إيذائهم».

على العموم، لقد وضعت التجربة، علامة استفهام صارخة على فلسفة زعران الشّيفرة. ربما كانت فوضى التشفير حتّى الآن مجال عمل كتاب الخيال العلمي، لكن الأدوات التي ستجعلها أمراً حقيقياً كانت في الطريق. وعندما وُضع هذا العتاد الرقمي موضع الاستخدام، يمكن لألف شركة مثل بلاك نيت أن تنشأ. بالتأكيد كان ذلك أمراً تنبه إليه، من هم وراء السياج الثلاثي، وكذلك في مقر قيادة مكتب التحقيقات الفيدراليأ يضاً. هل كانت المسألة تتذ ر بقيام حركة يجب وضع حد لها؟ إن المؤسّسة كانت قد بدأت تفكّر في ذلك.

وقد أقر دان باركر الخبير في شؤون الأمن، أننا بفضل قدرات التشفير بات «لديناا لقدرة على التمتع بسرِّيَّة تامة بملة لمئة. لكن إذا استخدمنا هذه ا لسرِّيَّة فلست أعتقد أن المجتمع يستطيع الاستمرار في البقاء».