Realização IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife

# O Caráter Moral do Trabalho Criptográfico

Phillip Rogaway

Tradução
André Ramiro

# O Caráter Moral do Trabalho Criptográfico


## Phillip Rogaway

**Departamento de Ciência da Computação**
**Universidade da Califórnia, Davis, Estados Unidos**
rogaway@cs.davis.edu



Dezembro de 2015
(com breve revisão em março de março de 2016)

Tradução para o português:
**André Ramiro**
**Instituto de Pesquisa em Direito e Tecnologia do Recife**
**2021**

Diagramação, Projeto gráfico e Capa:
**Paju design**

Agradecimentos aos **Profs. Diego Aranha e Ruy de Queiroz** pelas contribuições de revisão da tradução para o português.

**Dados Internacionais de Catalogação na Publicação (CIP)**

**(Câmara Brasileira do Livro, SP, Brasil)**

Bibliotecária Eliete Marques da Silva CRB-8/9380

# O Caráter Moral do Trabalho Criptográfico[1]

**RESUMO:** A criptografia redistribui o poder: ela estabelece quem pode fazer o quê, a partir de quê. Isso torna a criptografia uma ferramenta inerentemente política e confere ao campo uma dimensão intrinsecamente moral. As revelações de Snowden motivam uma reavaliação do posicionamento político e moral da criptografia. Eles nos levam a questionar se nossa incapacidade de abordar efetivamente a vigilância em massa configura um fracasso do nosso campo. Eu acredito que sim. Eu lanço meu apelo por um esforço comunitário que desenvolva meios mais eficazes para resistir à vigilância em massa. Eu apelo por uma reinvenção de nossa cultura disciplinar para atender não apenas aos quebra-cabeças e à matemática, mas, também, às implicações sociais de nosso trabalho.

**Palavras-chave:** criptografia - ética - vigilância em massa - privacidade - Snowden - responsabilidade social.

[1] Este ensaio foi escrito para acompanhar uma palestra a convite da Asiacrypt 2015, em 2 de dezembro de 2015, em Auckland, Nova Zelândia. O ensaio e a palestra são endereçados à comunidade de criptografia - minha comunidade - e as palavras “nós” e “nosso(a)” devem ser lidas dessa forma. Peço desculpas de antemão se ofendi alguém com algum de meus comentários; nada do tipo foi minha intenção.

**Preâmbulo.** A maioria dos criptógrafos parece pensar que nossa área é um jogo divertido, profundo e politicamente neutro - um conjunto de quebra-cabeças envolvendo a comunicação de partes e adversários imaginários. Essa visão de quem somos dá vida a um campo cujo trabalho é intelectualmente notável e rapidamente realizado, mas também consideravelmente isolado e apartado de problemas do mundo real. É assim que a criptografia deveria ser? É assim que nós deveríamos passar a maior parte do nosso capital intelectual?

Para mim, tais questões emergiram com as revelações de Snowden de 2013. Se o objetivo mais básico da criptografia é prover comunicações seguras, como não poderia ser um fracasso colossal da nossa área a falta de um mínimo de privacidade nas comunicações de indivíduos que interagem eletronicamente? Não obstante, eu me dei conta cedo de que a maioria dos criptógrafos não pensa desta forma. A maior parte deles parece compartilhar da percepção de que quebras de sigilo sequer dizem respeito a nós, criptógrafos.

Eu acredito que elas dizem. Por isso, eu queria falar sobre as obrigações morais dos criptógrafos e da minha comunidade de forma geral. Esse não é um tópico que criptógrafos costumam debater. Mas nesta era pós-Snowden, eu acredito que é necessário.

# Parte 1: A responsabilidade social de cientistas e engenheiros

**Um manifesto famoso.** Gostaria de começar com uma história - uma história real[2]. Para compor o cenário, estamos em Londres, verão de 1995. Uma sala repleta de jornalistas foi reunida para uma coletiva de imprensa em Caxton Hall, um prédio de tijolos vermelhos em Westminster. A mídia havia sido convocada como parte de um plano traçado por Bertrand Russell, com certa ajuda do editor do jornal The Observer. Os jornalistas não sabem exatamente porque estão ali, tendo apenas escutado que um time de cientistas mundialmente renomados estava prestes a lançar algo de relevância global.  A imprensa sabe que Bertrand Russell está envolvido. Com a morte recente de Einstein, Russell se tornou o intelectual vivo mais famoso do mundo.

Russell tem estado em sua casa, escondido, a semana inteira. O telefone e a campainha tocam o dia inteiro. Jornalistas tentavam descobrir do que se tratava o grande anúncio. A esposa de Russell e sua empregada doméstica dão desculpas e expulsam os jornalistas.

Com o início da coletiva de imprensa, os jornalistas descobrem a partir de Russell e do físico que o acompanha, Joseph Rotblat, que eles não haviam

[2] Esse relato é amplamente tomado de Sandra Butcher: The origins of the Russell-Einstein manifesto. Pugwash Conference on Science and World Affairs, maio de 2005.

sido reunidos para ouvir sobre qualquer descoberta científica, mas para receber uma elaborada declaração política. É uma declaração relativamente breve, mas assinada por onze[3] das maiores lideranças na ciência - nove deles ganhadores do Prêmio Nobel. Albert Einstein está entre os signatários, tendo assinado apenas dias antes de ficar doente e falecer.

O documento ficaria conhecido como o Manifesto Russell-Einstein[4]. Espero que este conteúdo seja conhecido por você. Fala de uma ameaça existencial à humanidade oferecida por armas nucleares. Sua passagem final soa como um lamento desesperado à medida que Russell escreve:

> Apelamos, enquanto seres humanos, aos seres humanos: lembrem-se de sua humanidade e esqueçam do resto. Se assim for feito, os caminhos se abrem para um novo Paraíso; se não for possível, diante de você se abrem os riscos da aniquilação total[5].

Os jornalistas fazem perguntas e logo se dão conta da importância do Manifesto. No dia seguinte, o Manifesto está na primeira página dos mais importantes jornais do mundo. Pelo menos durante vários dias seguidos, este é o tema mais comentado no mundo.

O Manifesto Russell-Einstein galvanizou os movimentos pela paz e pelo desarmamento. Ele abriu as portas para as conferências de Pugwash, pelas quais Joseph Rotblat e as próprias séries de conferências iriam mais cedo ou mais tarde ganhar o Nobel da Paz (1995). Rotblat dá crédito ao manifesto por ter

---

[3] Até o momento da coletiva de imprensa, Russell tinha confirmação de apenas oito.

[4] O nome pareceria ser uma instância do "Matthew effect", uma vez que Max Born, Frédéric Joliot-Curie e Joseph Rotblat haviam contribuído, no mínimo, tanto quanto Einstein.

[5] Citado em Joseph Rotblat, ed., Proceedings of the First Pugwash Conference on Science and World Affairs, Pugwash Council, 1982.

criado as condições que motivaram o Tratado de Não Proliferação de Armas Nucleares (TPN, 1970)[6]. No discurso de recebimento do Nobel da Paz, Rotblat explica:

> Há muito tempo, eu tive uma paixão pela ciência. Mas a ciência, o exercício do poder supremo do intelecto humano, sempre esteve relacionada, a meu ver, com o bem das pessoas. Eu via a ciência como estando em harmonia com a humanidade. Eu não imaginava que a segunda metade da minha vida seria dedicada a esforços para advertir sobre um perigo mortal à humanidade criado pela ciência[7].

**Duas formas de agir politicamente.** Comecei pelo Manifesto Russell-Einstein para lhes lembrar de duas coisas: primeiro, o trabalho técnico, por si mesmo, pode implicar em políticas; e a segunda é que alguns cientistas, em resposta, executam trabalhos explicitamente políticos. Essas duas formas de agir politicamente são diferentes (ainda que, para pessoas como Rotblat, elas caminhem lado a lado). Vamos observar cada uma delas.

**Políticas implícitas.** O cientista se engaja no que eu chamo de políticas implícitas ao influenciar relações de poder enquanto um subproduto do trabalho técnico. Políticas são sobre poder - quem tem o quanto e de que espécie. A bomba nuclear é a expressão mais radical do poder coercitivo; é a política encarnada. Tivesse Rotblat evitado toda atividade ostensivamente política em sua vida, seu trabalho ainda teria sido político. Imensamente -

---

[6] Butcher, op. Cit., Prefácio, p. 3.

[7] Joseph Rotblat, “Remember Your Humanity”. Discurso de aceitação do Nobel, 1995. Disponível em Nobelprize.org.

mesmo que implícito - político.

Mas não precisamos do espectro de nuvens de cogumelo para que estejamos lidando com tecnologias politicamente relevantes: o trabalho tecnológico e científico rotineiramente implica em políticas. Essa é uma ampla compreensão de décadas de trabalho sobre as correlações entre ciência, tecnologia e sociedade[8]. Ideias tecnológicas e coisas tecnológicas não são politicamente neutras: rotineiramente, elas têm fortes e intrínsecas tendências. Avanços tecnológicos são convenientemente considerados não apenas a partir das lentes de como funcionam, mas também porque passam a ser como são, quem beneficiam e quem prejudicam. Enfatizando a extensão da agência humana em escolhas tecnológicas, e tomando emprestado uma frase belíssima de Borges, tem-se dito que a inovação é um jardim de caminhos que se bifurcam[9].

Mesmo assim, ideias criptográficas podem ser consideravelmente matemáticas; poderia isso fazer delas relativamente apolíticas? Definitivamente não. A constatação de que o trabalho criptográfico é profundamente imbricado com a política é tão óbvia que apenas um criptógrafo poderia fracassar em percebê-la. Por isso, irei dedicar um tempo considerável a essa constatação. Mas antes, deixe-me falar sobre a segunda forma de agir politicamente dos cientistas.

[8] A literatura nesse sentido é consideravelmente vasta para ser listada. Programas de universidades nesse campo geralmente carregam o acrônimo de STS, para science and technology studies ou science, technology, and society. O trabalho de Langdon Winner se debruça particularmente sobre as relações entre artefatos tecnológicos e suas dimensões implicitamente políticas.

[9] A citação é de Robin Williams e David Edge: The social shaping of technology. Research Policy (25), 865-899, Elsevier Science B.V., (1966). A referência implícita é ao estranho conto de Borges "O jardim dos caminhos que se bifurcam (The Garden of Forking Paths) (1941).

**Políticas explícitas.** O cientista pode se engajar com políticas explícitas através de mecanismos de ativismo e de democracia participativa. Ao escrever o Manifesto Russell-Einstein e ao divulgá-lo da forma que ele fez, Russell estava trabalhando indiscutivelmente nesse domínio. Russell não era apenas um matemático: ele tinha amplas contribuições através da filosofia, havia ganhado o Prêmio Nobel em literatura e era um crítico social e ativista anti-guerra amplamente conhecido.

**A ética da responsabilidade.** A contribuição de Bertrand Russell foi extraordinária. Mas a mera existência de um intelectual politicamente engajado não sugere, de forma alguma, que esse exemplo seja, de alguma forma, representativo. Até que ponto cientistas e engenheiros são socialmente engajados? Até que ponto normas sociais exigem que eles o sejam?[10]

Atualmente, uma **ética da responsabilidade** é ensinada em cursos universitários e defendidas por organizações profissionais. É a visão doutrinária. A suposta norma afirma que os cientistas e engenheiros têm a obrigação de optar por trabalhos que promovam o bem social (um direito positivo), ou, pelo menos, evitar trabalhos que prejudiquem a humanidade ou o meio ambiente (um direito negativo)[11]. A obrigação se origina de três premissas básicas: que o trabalho de cientistas e engenheiros transforma a sociedade; que essa transformação pode ser para melhor ou para pior; e que o que fazemos é misterioso o suficiente para trazer uma perspectiva essencial ao discurso

[10] Alguns dos comentários do restante dessa seção têm referência em Matthew Wisnioski: Engineers for Change: Competing Visions of Technology in 1960s America. MIT Press, 2012.

[11] Embora essas duas possibilidades sejam muito diferentes, a distinção entre elas não será importante para a discussão deste ensaio.

público. Espera-se que o cientista socialmente engajado traga uma visão normativa de como o trabalho em sua área deve impactar a sociedade. Ele ou ela pretende, portanto, conduzir as coisas nessa direção.

De fato, tomar decisões sob a ética da responsabilidade não é fácil. Pode ser impossível prever se uma linha de pesquisa será usada para o bem ou para o mau. Além do mais, a dicotomia entre "para o bem e para o mau" pode ser simplista e subjetiva ao ponto de ser insignificante. Ainda assim, apesar de tais dificuldades, o cientista socialmente engajado teria que investigar, refletir e decidir que trabalho ele irá executar e para qual organizações ele irá ou não irá trabalhar. O julgamento será feito sem superestimar o interesse próprio de uma pessoa.

**Eventos históricos moldando a ética da responsabilidade.** A ascendência da ética da responsabilidade foi moldada por três eventos históricos da Segunda Guerra Mundial e por seus resultados.

**1.** O primeiro deles, já mencionado, foi a experiência dos cientistas atômicos. Depois da guerra, com a ciência deixada em uma posição tanto reverenciada quanto temida, físicos proeminentes se tornaram figuras públicas. Alguns se manifestaram abertamente em defesa pela paz ou em sua oposição à continuidade do desenvolvimento de armas. Lembre-se das preocupações bastante disseminadas dos físicos quanto à Iniciativa de Defesa Estratégica de Reagan (IDE)[12] ou da famosa carta

[12] O debate na comunidade científica ganhou atenção significativa da mídia a partir da publicação do estudo da Associação American Physical Society (APS) Study Group (N. Bloembergen, C. K. Patel, co-diretor) Report to the American Physical Society of the Study Group on Science and

de Hans Bethe a Bill Clinton, que argumentou contra uma nova rodada de desenvolvimento de armas nucleares pelos Estados Unidos[13]. Uma tendência de falar a verdade aos poderosos[14] tornou-se uma tradição entre físicos[15].

Como exemplo, destaco um incidente com spray de pimenta, em 2001, no meu próprio campus, na Universidade da Califórnia, Davis[16]. Obedecendo as instruções da reitora para dispersar manifestantes do movimento "Occupy", o oficial de polícia John Pike atingiu com spray de pimenta estudantes que sentavam, de braços cruzados, na praça central da universidade. Os vídeos do evento viralizaram[17], enquanto memes do oficial Pike disparando spray de pimenta em qualquer coisa se tornaram uma outra sensação na Internet. Mas a observação que eu gostaria de fazer é que, como consequência do incidente, o único departamento da Universidade - para além das áreas de humanidades - que condenou a reitora ou pediu pela demissão dela foi

Technology of Directeed Energy Weapons, APS, Nova York (Abril de 1987). O debate não partiu apenas de um lado: muitos dos físicos e fisicistas apoiavam a IDE e muitos sentiam que o estudo da APS seria muito negativo ou muito político.

[13] Ver http://fas.org/bethecr.htm#letter para a carta de Bethe de 1997.

[14] A popular expressão vem de um panfleto "Speak truth to power: a Quaker search for an alternative to violence", de 1955. http://www.quaker.org/sttp.html

[15] É claro que nem todo físico proeminente era opositor. Edward Teller reconhecidamente apoiou o desenvolvimento de bombas de fusão e a IDE. Essas posições eram divisoras de águas, com alguns dos colegas de Teller o vendo como irresponsável, chauvinista ou insano.

[16] O relato definitivo do incidente é: Reynoso, C., Blando, P., Bush, T., Herbert, P., McKenna, W., Rauchway, E., Balcklock, P., Brownstein, A., Dooley, D., Kolesar, K., Penny, C., Sterline, R., Sakaki, J.: Universidade da Califórnia, Davis, 2011 "Pepper Spray Incident" Task Force Report: The Reynoso Task Force Report. (Março de 2012) Disponível em http://www.ucsf.edu/sites/default/files/legacy files/reynoso-report.pdf (acessado em 07.08.2015)

[17] Há 2 milhões de visualizações em https://www.youtube.com/watch?v=6AdDLhPwpp4. N.T.: À data de publicação desta tradução, havia cerca de 2.684.500.

o departamento de Física[18]. A reitora ficou incrédula. Ela entendeu a forte reação do (insuficiente financiado e politicamente liberal) departamento de Inglês, mas não antecipava as reclamações do nosso (bem financiado e, em geral, conservador) departamento de Física[19]. O que a reitora talvez não conseguia internalizar é que os físicos carregam consigo um legado pós-guerra não apenas por se manterem próximos ao poder, mas também por terem seus calos pisados.

**2.** Um segundo evento histórico que ajudou a moldar a perspectiva sobre responsabilidade moral foram os julgamentos de Nuremberg (1945-1946). Embora a defesa repetidamente sustentasse que os acusados estavam simplesmente cumprindo ordens, essa visão foi rejeitada quase universalmente: obedecer a ordens não apagava a culpa legal ou moral. Os julgamentos de Nuremberg começaram com o Caso Médico, a acusação de 23 cientistas, médicos e outros altos funcionários por experiências médicas repulsivas e rotineiramente fatais em prisioneiros[20].

Anos depois, como em sequência, o mundo assistiria com ansiosa fascinação ao julgamento de Adolf Eichmann (1961). O polêmico retrato

[18] Nathan Brown: Op-ed: Reviewing the case for Katehi's resignation. Davis Enterprise newspaper (18 de dezembro de 2011). Departamento de Física da UC Davis, press release sem título (22 de novembro de 2011, disponível em http://tinyurl.com/ucd-physics-pepper-spray (acessado em 07.08.2015)

[19] A Chanceler expressou esses sentimentos em uma reunião entre ela e professores da Faculdade de Engenharia (data desconhecida, provavelmente início de 2012).

[20] Ver, por exemplo, Israel Gutman: Encyclopedia of the Holocaust, Macmillan Library Reference USA, 1990, termos: "Medical Experiments" por Nava Cohen, pp. 957-966, e "Physicians, Nazi" por Robert Jay Lifton e Amy Hackett, pp. 1127-1132

de Eichmann feito por Hannah Arendt se tornaria fundamental na formação de nosso entendimento sobre o que, eticamente, havia acontecido durante o Holocausto. Ela escreveu sobre a absoluta mediocridade do homem[21]. O livro de Arendt sobre o julgamento, com o memorável subtítulo "A Banalidade do Mal", seria publicado no mesmo ano (1963) dos experimentos clássicos de Stanley Milgram sobre obediência, onde Milgram chegou à impressionante (e amplamente reafirmada) descoberta de que uma grande fração de voluntários seguiria à gentil incitação de um cientista de jaleco branco para aplicar choques aparentemente fatais em alguém que eles pensavam ser um outro colega voluntário[22].

**3.** Finalmente, eu mencionaria a ascensão do movimento ambientalista como favorecedor da popularização de uma ética da responsabilidade. Ao passo que o ambientalismo data da metade do século 19 - ou mesmo antes, enquanto um movimento social relevante - a publicação do Silent Spring, de Rachel Carson, é um marco. Seu livro retratou o fim da vida não em razão da comoção do estado de guerra nuclear, mas a partir do desaparecimento de pássaros canoros, silenciados pelas crescentes atividades de fabricação de químicos e de uma variedade de pesticidas.

[21] Hannah Arendt: Eichmann em Jerusalém: um relato sobre a banalidade do mal. Companhia das Letras (1999)

[22] Stanley Milgram: Behavioral study of obedience. Journal of Abnormal and Social Psychology, 67(4), pp. 371-378 (1963).

**O bom cientista.** As três experiências que acabei de descrever implicam em uma democratização da responsabilidade. Cientistas tiveram que assumir a responsabilidade pelo que fizeram, por tecnologias que nos levariam a caminhos sombrios caso não o fizessem. Sem qualquer restrição de natureza ética, a ciência teria trazido à tona um mundo de pesadelos e bombas, câmaras de gás e experimentos humanos macabros. **Teria dado origem a um mundo envenenado, que padeceria.**

E assim, nas décadas que se seguiram à guerra, a ética da responsabilidade se tornou - pelo menos retoricamente - a norma doutrinária. Um número crescente de cientistas e engenheiros, bem como suas organizações profissionais, começaram a se engajar em questões de responsabilidade social. As Conferências de Pugwash começaram em 1955. A Sociedade Nacional de Engenheiros Profissionais adotou um código de ética em 1964, que deu prioridade à responsabilidade social. Como seu primeiro **imperativo**, o código estabelece que "Engenheiros, no cumprimento de suas funções profissionais, devem ter como prioridade suprema a segurança, a saúde e o bem-estar do público". Linguagem semelhante iria se expandir por outros códigos de ética, incluindo os da ACM e IEEE[23]. A **Union of Concerned Scientists** (União de Cientistas Preocupados) foi formada no MIT em 1969. No mesmo ano, uma greve de trabalho no MIT, coordenada com outras 30 universidades, teve considerável apoio dos alunos, do corpo administrativo e dos docentes. Exigia um realinhamento do rumo de pesquisa para longe de fins militares

[23] Nos Estados Unidos, apenas engenheiros de minas falharam em não adotar o código de ética, de acordo com o artigo da Wikipedia "Engineering ethics".

e em direção às necessidades humanas. A Computer Professionals for Social Responsibility (CPSR) iniciou seu trabalho se opondo à EDI, em 1983[24]. Naquele mesmo ano, o IACR foi fundado, com a expressa missão não apenas de fazer avançar a teoria e prática da criptologia, mas também, não esqueçamos, de servir ao bem-estar da coletividade[25]. A Electronic Frontier Foundation (EFF) e a Privacy International (PI) foram ambas fundadas em 1990 e se tornaram fortes defensoras de questões como a derrota do Clipper Chip. Tudo isso não é nada mais do que uma mostra de políticas explícitas que partem de cientistas e engenheiros.

Sob esse pano de fundo, a figura do cientista brilhante, porém humano, tornou-se um tema cultural. Jonas Salk erradicou a poliomielite. Einstein tornou-se um ícone cultural, inabalável mesmo com a sua morte inoportuna. A imagem dele esticando a língua pode ser a fotografia mais amplamente reconhecida de qualquer cientista de todos os tempos. Richard Feynman seria pintado de forma igualmente bem-humorada, o gênio austero batucando em um bongô e lançando algo preto emborrachado em água gelada[26]. Star Trek, de Gene Roddenberry, imaginou um futuro cujo herói cientista e humanista é, na verdade, uma equipe, e não um indivíduo. Carl Sagan, falando gentilmente para a câmera nos episódios de Cosmos (1980), parecia a verdadeira personificação deste conjunto de aspirações.

---

[24] A organização foi dissolvida em 2013.

[25] O Artigo II do Estatuto da International Association for Cryptologic Research: "A missão da IACR é avançar na teoria e prática da criptologia de suas áreas correlatas, além de promover os interesses de seus membros com respeito e servir ao bem comum." Revisado pela última vez em 18 de novembro de 2013. Disponível em www.iacr.org/docs/bylaws.pdf

[26] N. T. Disponível em https://www.youtube.com/watch?v=Q2Y2GRq-z6M&ab_channel=theatticroomstudios

Fria, nem em qualquer uma das guerras americanas subsequentes, as empresas norte-americanas tiveram dificuldades em recrutar ou manter os(as) centenas de milhares de cientistas e engenheiros(as) envolvidos na construção de sistemas armamentistas[27]. Universidades, como a minha, estavam felizes em aumentar seu apoio; a Universidade da Califórnia administraria, por décadas, os laboratórios de design de armas nucleares dos EUA[28]. Em quase 20 anos aconselhando alunos em minha universidade, observei que o desejo de um "meio de vida correto"[29] quase nunca surge nas escolhas de emprego dos alunos de graduação em ciência da computação. E isso não é exclusivo dos cientistas da computação: dos cinco sites mais bem classificados que encontrei em uma pesquisa do Google para decidir entre ofertas de emprego, nenhum sugere considerar os objetivos institucionais do empregador ou o valor social do que eles fazem[30].

Hoje em dia, questiono **candidatos à docência** no departamento de ciências da computação sobre suas perspectivas a respeito de responsabilidades

[27] Ver, por exemplo, Thomas P. Hughes: Rescuing Prometheus, 1998 (sobre o projeto Atlas)

[28] Na sequência de algumas brechas de segurança, agora fazem isso em parceria com a indústria, especificamente com Bechdel. Ver http://www.bechtel.com/projects/usnational-laboratories/

[29] O termo é associado ao Budismo, sendo o "meio de vida correto" uma das virtudes do Nobre Caminho Óctuplo. N.T.: No original, "right livelihood".

[30] Meu "top 5" de resultados de busca no Google para "decidindo entre duas ofertas de emprego", em 26 de agosto de 2015, foram: (1) "Help! How Do I Choose Between Two Job Offers." Site do CareerCast, www.careercast.com/career-news/help-how-do-i-choosebetween-two-job-offers. (2) "4 questions to help you decide between job offers." Natalie Wearstler, 16 de setembro de 2013. theweek.com/articles/460019/4-questions-helpdecide-between-job-offers. (3) "You Got the Jobs! How to Decide Between Offers." Forbes, 6 de junho de 2011. www.forbes.com/sites/prettyyoungprofessional/2011/06/06/you-got-the-jobs-how-to-decide-between-offers/. (4) "6 Secrets to Choosing Between Job Offers." 31 de julho de 2013. www.aegistech.com/how-to-choose-between-multiplejob-offers/. (5) "How to Choose Between Multiple Job Offers." Sam Tomarchio, Aegistech. www.aegistech.com/how-to-choose-between-multiple-job-offers/. Os sites não continham as palavras ética, moral, social ou qualquer comentário sobre o caráter ético ou valores morais do trabalho de uma pessoa. O autor reconhece que os resultados do Google não são reproduzíveis

Hoje em dia, questiono **candidatos à docência** no departamento de ciências da computação sobre suas perspectivas a respeito de responsabilidades éticas do(a) cientistas da computação. Alguns respondem que com surpresa, inseguros sobre o que tal pergunta sequer significa. Uma candidata recente, pesquisadora em mineração de dados e cujo trabalho parecia ser um compêndio de projetos financiados pelo Departamento de Defesa, **repreensíveis do ponto de vista social,** admitiu que ela não sentia qualquer responsabilidade social. “Sou um corpo sem alma”, ela respondeu honestamente. Foi sincero - e assustador.

Stanley Fish, um famoso teórico da literatura, professor e reitor, adverte pesquisadores a não buscar programas de pesquisa baseados em valores (seu livro de 2012 é intitulado “Salve o Mundo no Seu Próprio Tempo). Fish aconselha professores para que

> faça seu trabalho; não tente fazer o trabalho de outra pessoa...; e não deixe mais ninguém fazer o seu trabalho. Em outras palavras, não confunda suas obrigações acadêmicas com a obrigação de salvar o mundo; essa não é sua função como acadêmico... Famosa é a fala de Marx quando disse que nosso trabalho não é interpretar o mundo, mas mudá-lo. Na academia, porém, é exatamente o contrário: nosso trabalho não é mudar o mundo, mas interpretá-lo.[31]

Talvez essa amoralidade, por mais revoltante que seja, seja inofensiva na área intelectual de Fish: não se espera exatamente que a teoria literária mude

[26] Stanley Fish: Why we built the ivory tower. NY Times, Opinion Section, 21 de maio de 2004.

o mundo. Mas cientistas e engenheiros fazem precisamente isso. A recusa em conduzir a mudança que fazemos é moralmente falida e ingrata. Nosso trabalho enquanto acadêmicos, nunca devemos esquecer, é subsidiado pela sociedade[32].

Até agora eu não disse por que a ética da responsabilidade do pós-guerra não pegou. Eu poderia dar várias respostas, começando com o surgimento do individualismo radical[33]. Mas prefiro focar em outra coisa: o otimismo tecnológico extremo.

**O otimismo tecnológico.** Otimistas tecnológicos acreditam que a tecnologia vai tornar a vida melhor. De acordo com essa visão, nós vivemos melhor, temos mais liberdade, temos mais lazer. A tecnologia nos enriquece com mais artefatos, conhecimento e potencial. Associada ao capitalismo, a tecnologia tem se tornado essa ferramenta extraordinária para o desenvolvimento humano. A essa altura, é fundamental para a missão da raça humana. Enquanto tecnologias trazem algumas consequências imprevistas, a própria inovação irá nos levar adiante.

O otimismo tecnológico empolga a todos, de crianças colegiais a ganhadores do Prêmio Turing. A aceitar seu Prêmio Turing em 2021, Silvio Micali disse que

> A ciência da computação está marcando uma mudança épica na história da

[32] Elisabeth Pain: The social responsibility of scientists. Career Magazine of Science, 16 de fevereiro de 2013. Relatório da reunião do AAAS de 2013 e, especialmente, os comentários de Mark Frankel. O palestrante pede aos ouvintes, principalmente aos pós-graduandos, que tenham em mente que a pesquisa científica é uma instituição social e subsidiada pela sociedade.

[33] O individualismo radical é a crença de que os interesses pessoais de uma pessoa são mais importantes do que os da sociedade. Isso é bem ilustrado pelo discurso "Greed is Good" do filme "Wall Street" (1987), de Oliver Stone, ainda que o que o indivíduo queira possa ser algo para além da riqueza pessoal.

> humanidade. Estamos conquistando um novo e vasto continente científico. (...) Virtualmente, todas as áreas da atividade humana (...) [e] virtualmente todas as áreas do conhecimento humano (...) estão se beneficiando das nossas contribuições conceituais e técnicas (...) Vida longa à ciência da computação![34]

Se você é um otimista tecnológico, um belo futuro flui da nascente do seu trabalho. Isso implica em uma limitação sobre a responsabilidade ética. O mais importante é cumprir seu trabalho - e fazê-lo bem. Isso se torna, inclusive, um imperativo moral, uma vez que o trabalho em si seria sua contribuição social. Mas e se a ciência da computação não estiver beneficiando a humanidade? Pessimistas tecnológicos como Jacques Ellul, Herbert Marcuse e Lewis Mumford certamente não pensavam que ela estivesse. Eles viam a tecnologia moderna enquanto um sistema entrelaçado e fora de controle que, ao invés de satisfazer as necessidades humanas, acarretava em desejos sem sentido e armas mortais. O homem estaria se tornando não mais do que órgãos sexuais de um mundo maquínico[35].

Tomando um caminho um pouco menos extremo[36], contextualistas

---

[34] Silvio Micali, discurso de aceitação do Prêmio Turing da ACM. Cerimônia da ACM, São Francisco, 15 de junho de 2013. https://www.youtube.com/watch?v=W0N4WnjGHwQ. Terminando seu discurso com alegria, há, talvez, um elemento de jocosidade no otimismo desenfreado de Silvio. Ainda assim, o otimismo exagerado parece endêmico ao discurso sobre ciência da computação. A cerimônia de premiação aconteceu pouco mais de uma semana após a primeira notícia baseada em documentos de Snowden (6 de junho de 2013). Mas a ameaça de tecnologias computacionais não seria reconhecida, apenas festejada a sua promessa.

[35] Marshall McLuhan, Os meios de comunicação como extensões do homem. Cultrix, 1969. "É como se o homem se tornasse o órgão sexual do mundo da máquina, como a abelha do mundo das plantas, fecundando-o e permitindo o evolver de formas sempre novas."

[36] Esclarecendo, não acho que haja nada de extremo nessas perspectivas sobre um notável pessimismo tecnológico; antes de mais nada, parece-me que a prevalência de visões otimistas é que são muito menos razoáveis e mais extremas.

tecnológicos[37] reconhecem as preocupações dos pessimistas, mas enfatizam o agenciamento essencialmente humano e a maleabilidade da tecnológica. O contextualismo domina a dialética dos estudos em tecnologia.

A ética da responsabilidade é sempre pareada com o ponto de vista dos essencialistas sobre socio-tecnologias. Em algum nível, o seguinte deveria ocorrer: uma necessidade normativa desaparece se, no jardim dos caminhos que se bifurcam, todos os caminhos levam ao bem (ou, no mesmo sentido, ao mau). Mas é ao otimismo tecnológico que as pessoas normalmente aderem, especialmente cientistas e engenheiros. Um otimismo tecnológico desenfreado compromete a necessidade básica por responsabilidade social.

**Conclusão da parte 1.** No fim das contas, penso que a virada pós-guerra no sentido de uma responsabilidade social na ciência e engenharia foi menos uma virada e mais um flerte. Enquanto a retórica da responsabilidade ofereceria respaldo à crítica à tecnologia, poucos cientistas ou engenheiros iriam de fato internalizar que seus trabalhos envolvem valores socialmente relevantes. Se pesquisadores como nós devessem verdadeiramente saber e se importar sobre essas questões de uma forma operacionalmente significativa, bem, acho que nós não recebemos o memorando.

Deixe-me, então, retransmitir essa mensagem. Ela quer dizer que seus deveres morais vão além do imperativo de que você, pessoalmente, não causa

[37] Essa é uma frase usada por Ian Barbour: Ethics in an Age of Technology: The Gifford Lectures, Volume 2), HarperCollins (1993), que carrega uma boa descrição dos escritos dos contextualistas (que inclui o próprio autor). Langdon Winner fala de uma ideologia das políticas tecnológicas para praticamente um mesmo conceito de um contextualismo; ver Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought. MIT Press, 1977.

Deixe-me, então, retransmitir essa mensagem. Ela quer dizer que seus deveres morais vão além do imperativo de que você, pessoalmente, não causa danos: você deve também tentar promover o bem comum. Além disso, quer dizer que seus deveres morais derivam não apenas de sua estatura como indivíduo moral, mas, também, das comunidades profissionais às quais você pertence: criptógrafo, cientista da computação, cientista, tecnologista.

Com poucas exceções, os cientistas atômicos que trabalharam no desarmamento não foram os mesmos que construíram a  bomba. Seus colegas - companheiros físicos - sim. Criptógrafos não transformaram a Internet num instrumento de vigilância total, mas seus colegas - companheiros cientistas da computação e engenheiros - sim. E criptógrafos possuem certa capacidade de ajudar.

Mas você só vai acreditar nessa afirmação se reconhecer que a criptografia pode influenciar as relações de poder. Suspeito que muitos de vocês não enxergam qualquer relação real entre aquilo com que vocês trabalham e valores sociais, éticos e políticos. Você não constrói bombas, faz experiências com pessoas ou destrói o meio ambiente. Você não espiona o povo. Você é um hacker da matemática e escreve artigos. Isso não parece eticamente carregado. Eu quero te mostrar que é.

# Parte 2: O caráter político do trabalho criptográfico

**Cientista ou espião?** Há uma ironia em debater a alegação de que o trabalho criptográfico é político - no seguinte sentido: para alguém sem relação com o campo, e também para aqueles que se relacionam por mero hobby, a alegação pode parecer obviamente verdadeira. Mas para o jovem pesquisador que passa a vida escrevendo artigos sobre criptografia, a afirmação pode parecer obviamente falsa. O que acontece?

A perspectiva do outsider pode ser baseada em representações do cinema. Filmes como Sneakers (1992), Pi (1998), Uma Mente Brilhante (2001), Enigma (2001), Traveling Salesman (2012), Citizenfour (2014) e O Jogo da Imitação (2014) pintam a criptografia como um campo entrelaçado com a política. Criptógrafos são os brilhantes e belos matemáticos que o poder precisa ao seu lado. Nós somos - fico feliz em anunciar, gênios heroicos. Um pouco malucos, claro, mas isso só deixa mais brilhante.

De forma similar, os(as) que se relacionam por hobby podem ter lido relatos históricos sobre criptografia, como os livros de James Bamford ou David Kahn[38]. Tais relatos deixam claro que, historicamente, a criptografia é sobre poder.

[38] A série de livros de James Bamford sobre a história da NSA são The Puzzle Palace: A Report on America's Most Secret Agency (1982), Body of Secrets: Anatomy of the Ultra-Secret National Security

É um domínio no qual governos investem uma enorme quantidade de recursos[39] e, talvez, não inocentemente: o trabalho contribui diretamente para o resultado de guerras e possibilita manobras diplomáticas e econômicas[40].

Mesmo assim, nenhum criptógrafo acadêmico confundiria relatos históricos ou fictícios sobre a criptografia com o que realmente fazemos. Nossa disciplina investiga problemas acadêmicos que se enquadram em nossos limites disciplinares. Pegue um procedimento da Springer ou navegue por artigos do ePrint e nosso campo parecerá totalmente apolítico. Se o poder está em qualquer lugar, está nas capacidades abstratas de adversários hipotéticos[41] ou, em um ramo diferente de nossa área, no gasto de energia, medido em watts, para algum hardware. Trabalhamos em problemas que nos parecem interessantes ou cientificamente importantes. Não pretendemos promover nada além da própria ciência (ou, talvez, da própria carreira).

Afirmações tão variadas sobre a conexão da criptografia com o poder derivam, pelo menos em parte, de arquétipos radicalmente diferentes do que o criptógrafo é: cientista ou espião. O funcionário da NSA/GCHQ que hackeou a

Agency (2001), e The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America (2008). O livro clássico de David Kahn sobre a história da quebra de códigos é The Codebreakers: The

Story of Secret Writing (1967).[39] "Consolidated Cryptologic Program" dos Estados Unidos inclui cerca de 35.000 funcionários. O orçamento da NSA para 2013 foi de US$ 10,3 bilhões, com US$ 1 bilhão para "criptoanálise e serviços de exploração" e US$ 429 milhões para "pesquisa e tecnologia" em operações de inteligência entre 2004-2013. Ver Barton Gellman e Greg Miller, o resumo de "Black Budget' detalha os sucessos, fracassos e objetivos da rede de espionagem dos EUA; The Washington Post, 29 de abril de 2013. O orçamento da NSA para 2013 foi de US$ 10,3 bilhões, com US$ 1 bilhão para "criptoanálise e serviços de exploração" e US$ 429 milhões para "pesquisa e tecnologia" em operações de inteligência entre 2004-2013. Ver Barton Gellman e Greg Miller

[38] Para um relato da extrema utilidade dada à vigilância e criptografia nas recentes guerras dos Estados Unidos, ver Shane Harris: @War: The Rise of the Military-Internet Complex. Eamon Dolan/ Houghton Mifflin Harcourt (2014).

[38] Por exemplo, a frase "um adversário todo poderoso" geralmente significa um agente sem restrições computacionais, mas que se sujeita a um modelo especificado.

Gemalto para implantar um malware e roubar chaves SIM[42] é tão digno de ser chamado de criptógrafo quanto um teórico formado no MIT que concebe uma nova abordagem para a encriptação funcional. Ambos lidam com questões de privacidade, comunicações, adversários e técnicas inteligentes - e faríamos bem em enfatizar essas semelhanças se quisermos ver nosso universo disciplinar de forma contextualizado ou submetê-lo a uma relevância maior.

**A criptografia acadêmica costumava ser mais política.** A ascensão de um novo arquétipo do criptógrafo - o criptógrafo acadêmico - falha em realmente explicar nossa postura politicamente distanciada. Isso porque criptógrafos acadêmicos já estiveram mais preocupados com as dimensões sociopolíticas do nosso campo. Alguns até recorreram à criptografia justamente por isso. Considere, por exemplo, este fragmento do testemunho de Whit Diffie no julgamento de Newegg. Falando de sua esposa, Diffie diz:

> Eu disse a ela que estávamos rumando para um mundo onde as pessoas teriam relacionamentos importantes, íntimos e duradouros com pessoas que nunca haviam conhecido pessoalmente. Eu estava preocupado com a privacidade naquele mundo - e é por isso que estava trabalhando com criptografia.[43]

Diffie e seu orientador, Martin Hellman, há muito evidenciaram uma preocupação com os problemas sociopolíticos relacionados à tecnologia. Você

[42] Jeremy Scahill e Josh Begley: The great SIM heist: how spies stole the keys to the encryption castle. The Intercept, 19 de fevereiro de 2015.

[43] Joe Mullin: Newegg trial: crypto legend takes the stand, goes for knockout patent punch. Ars Technica, 24 de novembro de 2013.

vê isso em suas críticas ao comprimento da chave do DES[44], no ativismo de Hellman no desarmamento nuclear,[45] no livro de Diffie sobre as políticas das interceptações telefônicas, com Susan Landau,[46] e em sua co-invenção do sigilo futuro [forward secrecy, no original].[47] Você vê isso no artigo New Directions:[48] quando os autores enfaticamente iniciam-o com "Estamos hoje à beira de uma revolução na criptografia", a revolução antecipada não era, pelo menos em princípio, a comunidade teórica trazendo adiante noções que alterariam a mentalidade de segurança demonstrável, simulabilidade[49] ou computação multilateral.[50] Os autores estavam interessados nas mudanças tecnológicas que estavam ocorrendo e nas oportunidades e necessidades sociais daí derivadas.[51]

Ainda mais declaradamente político é o conjunto do trabalho científico de

[44] Whitfield Diffie e Martin Hellman: Exhaustive cryptanalysis of the NBS Data Encryption Standard. Computer 10(6), pp. 74-84 (1977).

[45] Ver, por exemplo, Anatoly Gromyko e Martin Hellman: Breakthrough: Emerging New Thinking: Soviet and Western Scholars Issue a Challenge to Build a World Beyond War, 1988.

[46] Whitfield Diffie e Susan Landau: Privacy on the Line: The Politics of Wiretapping and Encryption, MIT Press (2007)

[47] Whitfield Diffie, Paul van Oorschot, Michael Wiener: Authentication and authenticated key exchanges. Designs, Codes and Cryptography, 2(2), pp. 107-125 (1992)

[48] Whitfield Diffie e Martin Hellman: New directions in cryptography. IEEE Transactions on Information Theory, 22(6), pp. 644-654 (1976)

[49] N.T.: Técnica que objetiva provar a segurança de protocolos criptográficos. Executa-se o protocolo em "mudo ideal" para se argumentar que seu comportamento no "mundo real" seria indistinguível.

[50] Ainda assim, os autores pareciam antecipar essa possibilidade: "Ao mesmo tempo, desenvolvimentos teóricos na teoria da informação e na ciência da computação se mostram promissores em fornecer criptossistemas demonstravelmente seguros, transformando essa antiga arte em uma ciência." Ibid., p. 29.

[51] Eles escrevem, por exemplo, que "O desenvolvimento de hardware digital barato a libertou [a criptografia] das limitações de design da computação mecânica e trouxe para baixo o custo de dispositivos criptográficos de alto nível, onde eles podem ser usados para aplicações comerciais como caixas eletrônicos remotos e terminais de computador. (...) O desenvolvimento de redes de comunicação controladas por computador promete um contato fácil e econômico entre pessoas ou computadores em lados opostos do mundo (...)"

David Chaum, que incorpora profundamente preocupações com a democracia e a autonomia individual. O artigo Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, de Chaum[52] [Chaum81][53], sugere que uma meta de privacidade crucial, ao se enviar um e-mail, é ocultar quem está se comunicando com quem. Os metadados, na linguagem política moderna. O autor ofereceu as redes de mistura[54] como uma solução.[55]

Chaum continuaria provendo as ideias básicas para dinheiro eletrônico anônimo e votação eletrônica. Seus artigos comumente se baseavam em motivações abertamente políticas.[56] Em uma conversa recente, Chaum expressou surpresa com a extensão em que os acadêmicos gravitaram para um campo - a criptografia - tão conectado com questões de poder[57].

**Escanteando a política.** Mas, à medida que acadêmicos gravitavam para a criptografia, eles tendiam a higienizá-la, escanteando-se de sua pretensa

---

[52] O artigo aparece em Communications of the ACM (CACM), 24(2), pp. 84-88(1981).

[53] N.T.: A referência a "[Chaum81]" irá se referir, ao longo de todo ensaio, ao artigo Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, de 1981. Disponível em http://www.lix.polytechnique.fr/~tomc/P2P/Papers/Theory/MIXes.pdf.[48] Whitfield Diffie e Martin Hellman: New directions in cryptography. IEEE Transactions on Information Theory, 22(6), pp. 644-654 (1976)

[54] N.T.: Mix nets, no original.

[55] Em resumo, uma rede de mistura funciona assim: as comunicações de cada usuário passarão por uma série de roteadores. Para que o modelo agregue valor, esses roteadores, ou mixes, devem ter diversidade no controle administrativo, controle jurisdicional ou no código que executam. Os purotextos serão encriptados multiplamente, usando uma chave para cada roteador na série. Cada roteador removerá uma camada de encriptação. Antes de passar o resultado para o próximo roteador, ele esperará até que tenha um certo número de mensagens de saída e as reordenará em seguida. Um adversário que observe o tráfego da rede - até mesmo um que controle um subconjunto de roteadores - não conseguirá identificar quem enviou o quê para quem.

[56] Por exemplo: "Uma base está construída para uma sociedade do dossiê, na qual computadores podem ser usados para inferir estilos de vida, hábitos, localização e associações de indivíduos a partir de dados coletados em transações comuns de consumidores. A incerteza sobre se os dados permanecerão seguros contra abusos por aqueles que os mantêm ou os aproveitam pode ter um "efeito inibitório", fazendo com que as pessoas alterem suas atividades observáveis." David Chaum: Security without identification: transaction systems to make big brother obsolete. Communications of the ACM (CACM), 28(10), pp. 1030-1044, 1985.

conexão com o poder. O trabalho aplicado e relacionado à privacidade foi deixado de fora dos principais eventos do campo, as conferências IACR. É como se ocorresse uma sintetização química, transformando pólvora potente em poeira inofensiva.

Considere que existe agora uma conferência chamada "Real World Cryptography" (RRC)[58]. Chega a ser cômico - talvez tragicômico - que um campo com uma gênese e capacidade tão real quanto a nossa encontre uma razão para criar um evento chamado por esse nome[59]. Pergunte a um(a) colega(a) da área de Gráficos ou Computação em Nuvem como seria em sua comunidade se alguém iniciasse uma conferência chamada "Computação Gráfica do Mundo Real" (CGMR 2015) ou Computação Gráfica do Mundo Real (CNMR 2016). Eles vão rir.

Uma exclusão especialmente problemática do elemento político é a marginalização dentro da comunidade criptográfica do problema das mensagens seguras,[60] cujo exemplo foi abordado por [Chaum81]. Mensagens

[58] Tendo iniciado em 2012, o evento anual já atrai mais participantes do que a Crypto. O comitê gestor da RWS é composto por Dan Boneh, Aggelos Kiayias, Brian LaMacchia, Kenny Paterson, Tom Ristenpart, Tom Shrimpton, e Nigel Smart. O site http://www.realworldcrypto.com/ explica: "Esta conferência anual tem como objetivo reunir pesquisadores de criptografia com desenvolvedores que implementam criptografia em sistemas do mundo real. O objetivo da conferência é fortalecer o diálogo entre essas duas comunidades. Os tópicos abordados se concentram no uso de criptografia em ambientes do mundo real, como a Internet, nuvem e dispositivos incorporados."

[59] Alguns teóricos podem se ofender com a declaração de que a teoria criptográfica não é "mundo real", sugerindo que aqueles que trabalham com teoria devem estar estudando algo irreal ou não deste mundo (as névoas dos poltergeists?). As dicotomias implícitas da teoria criptográfica vs. a prática criptográfica, o mundo real e seus complementos (sejam lá quais forem), não sobreviveriam a uma avaliação crítica. Mesmo assim, discursos sobre o que as comunidades fazem parece inevitavelmente cheio de limites caprichosos.

[60] Surpreendentemente, o problema carece até mesmo de um nome amplamente conhecido. A versão do problema na segurança de mensagens em que Chaum estava interessado é uma versão de chave pública de alta latência.

seguras são o problema de privacidade mais fundamental em criptografia: diz respeito a como as partes podem se comunicar de forma que ninguém saiba quem disse o quê. Mais de uma década após a introdução do problema, Rackoff e Simon comentariam sobre a quase ausência de atenção dada a ele[61]. Mais de 20 anos depois, a situação é a seguinte: há, neste momento, uma montanha de trabalho sobre mensagens seguras, mas não está bem claro o que a maioria deles realmente **faz**. Um artigo recente sobre sistematização do conhecimento[62] pinta o retrato de uma aplicação criptográfica usufruindo do florescimento de soluções ad hoc, mas de forma em que pouco disso emerge da comunidade criptográfica, como suficientemente revisado ou embasado em muita teoria[63]. Embora se possa afirmar que isso seja verdade para quase todos os objetivos práticos de segurança que empregam criptografia, acho que o caso é diferente para mensagens seguras: aqui o trabalho parece ser quase intencionalmente colocado de lado.

**Filhos de [Chaum81] e [GM82].** Por que razão eu faria tal declaração? Um estudo de caso ilustrativo é feito ao se comparar trabalhos que citam o artigo de

[61] Charles Rackoff e Daniel Simon: Cryptographic defense against traffic analysis. STOC '93, pp. 72-681. A passagem é das páginas 672-673.

[62] Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg e Matthew Smith: SoK: Secure messaging. IEEE Symposium on Security and Privacy 2015, pp. 232-249

[63] Não muita, mas não nenhuma. Ver, por exemplo, Nik Unger e Ian Goldberg: Deniable key exchanges for secure messaging. ACM CCS 2015. N. Borisov, I. Goldberg, e E. Brewer: Off-the-Record communication, or, why not to use PGP. Privacy in the Electronic Society, pp. 77-84, 2004. Ron Berman, Amos Fiat, Marcin Gomulkiewicz, Marek Klonowski, Miroslaw Kutylowski, Tomer Levinboim e Amnon Ta-Shma: Provable unlinkability against traffic analysis with low message overhead. J. of Cryptology, 28(3), pp. 623-640, 2015. Jan Camenisch e Anna Lysyanskaya: A formal treatment of onion routing. CRYPTO 2005. Joan Feigenbaum, Aaron Johnson, e Paul F. Syverson: Probabilistic analysis of onion routing in a black-box model. ACM Transactions on Information and System Security (TISSEC), 15(3), 2012.

[Chaum81] e o Probabilistic Encryption, de Goldwasser e Micali [GM82][64]. Os dois artigos surgiram por volta do mesmo período e têm um número de citações semelhante[65].

[GM82] apresentou a abordagem centrada na definição e baseada na redução para lidar com problemas criptográficos. Tornou-se um trabalho seminal da comunidade criptográfica. Os artigos mais citados que o citam aparecem na Crypto e na Eurocrypt, FOCS, STOC e ACM CCS[66]. [Chaum81] avança no problema da segurança em e-mail e sugere uma solução. Esse trabalho seria tão seminal quanto o outro - mas em uma difusão mais notável fora da comunidade criptográfica. Os dez artigos mais citados que citam o artigo de Chaum aparecem em áreas cuja maioria eu nunca tinha ouvido falar. Áreas não focadas em criptografia, como MobiSys e SIGOPS. Na verdade, as áreas dos dez artigos mais citados citando [GM82] e as áreas para os dez artigos mais citados citando [Chaum81] são de uma interseção pouco explorada. Acho isso bem notável. Reflete uma comunidade de pesquisa dividida em fragmentos que inclui uma derivação de [GM] e uma derivação de [Chaum], a segunda delas não sendo, de forma alguma, parte da comunidade criptográfica.[67]

---

[64] Chaum, op. Cit. Shafi Goldwasser e Silvio Micali: Probabilistic encryption and how to play mental poker keeping secret all partial information. STOC 1982, pp. 365-377. Versão do periódico como: Probabilistic encryption, Journal of Computer and System Science (JCSS), 28(2), pp. 270-299, abril de 1984.

[65] De acordo com o Google Scholar: 4481 citações ao artigo de Chaum e 3818 citações para o artigo de Goldwasser-Micali (somando ambas as versões). Dados de 14 de outubro de 2014.

[66] A única exceção é o artigo de Perrig, Szewczyk, Tygar, Wen, e Culler na MobiCom.

[67] Mais precisamente, os dez que mais citavam [GM82] (as duas versões somadas) estavam na CCS, Crypto 3x, Eurocrypt, FOS (2x) MobiCom, STOC (2x). Apenas a MobiCom seria um espaço "não esperado". Os dez que mais citados que citavam [Chaum81] estavam na ACM Comp. Surveys, ACM J of Wireless Networks, ACM MobiSys, ACM Tran. on Inf. Sys., ACM SIGOPS, IEEE SAC, Proc. of the IEEE USENIX Security Symposium e nos workshops chamados IPTPS e Designing Privacy

E por que essa fragmentação ocorre? A explicação mais óbvia tem a ver com rigor: [GM82] ofereceu uma abordagem matematicamente precisa para seu assunto, enquanto [Chaum81] não. Portanto, uma segmentação pode parecer fazer sentido: o trabalho criptográfico que pode ser matematicamente formal vai por um lado; questões ad hoc, por outro.

Mas o problema com esta explicação é que ela está errada. [Chaum81] sustenta suficientemente bem o rigor. De fato, a segurança demonstrável acabaria por alcançar as redes de mistura, embora a primeira definição tivesse que levar mais de 20 anos para surgir (2003), em um artigo de Abe e Imai[68].
O fato de [Chaum81] em si não fornecer um tratamento formal não diz nada sobre a capacidade de formalização do problema ou quais comunidades iriam eventualmente adotá-la; no fim das contas, o artigo do Diffie e Hellman[69] descreveu apenas informalmente permutações de backdoor, criptografia de chave pública e assinaturas digitais, mas tudo seria incorporado à agenda criptográfica. Agora, pode-se argumentar que o problema abordado por [Chaum81] é mais difícil de formalizar do que qualquer um dos exemplos mencionados.
É verdade. Mas é mais simples formalizar do que MPC[70], digamos, que ganharia rapidamente entrada e estatura na comunidade criptográfica - mesmo sem

---

of the IEEE USENIX Security Symposium e nos workshops chamados IPTPS e Designing Privacy Enhencing Technologies. Nenhum desses dez espaços são focados em criptografia.

[68] Masayuki Abe e Hideki Imai: Flaws in some robust optimistic mix-nets. Information Security and Privacy (ACISP), pp. 39-50, 2003. Versão do periódico: Masayuki Abe e Hideki Imai: Flaws in robust optimistic mix-nets and stronger security notions. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science, vol. E89A, no. 1, pp. 99-105, janeiro de 2006.

[69] Diffie e Hellman, op. cit.

[70] Multiparty computation. Andrew Chi-Chih Yao: Protocols for secure computations (extended abstract). FOCS 1982, pp. 160-164. Oded Goldreich, Silvio Micali e Avi Wigderson: How to play any

definições ou provas. Em última análise, então, nem a "formalização" nem a "complexidade" são argumentos que têm muito sucesso ao explicar porque a questão sobre problemas de segurança de mensagens foi marginalizada.

Uma resposta melhor (mas de forma alguma a única resposta) é dada ao comparar a introdução dos dez artigos mais citados que citavam [GM82] e os dez que citavam [Chaum81]. Artigos que citam [GM82] enquadram os problemas cientificamente. Os autores afirmam que resolvem questões técnicas importantes. O tom é assertivo, com lapsos de otimismo tecnológico. Em um contraste notável, os artigos que citam [Chaum81] enquadram os problemas sociopoliticamente. Os autores abordam certos problemas e necessidades sociais. O tom é cauteloso e visões explicitamente contextualistas são habituais. Observa-se exatamente a mesma distinção no tom e nas motivações declaradas ao comparar artigos focados em revisão de literatura.[71]

Em 2015, participei do PETS (Privacy Enhancing Technologies Symposium) pela primeira vez. Ouvir as pessoas nessa comunidade interagindo se assemelha, um pouco, a observar a comunidade criptográfica através de uma lente que inverte magicamente a maioria das coisas. A comunidade PETS aborda de perto os valores embutidos no trabalho. Preocupam-se com artefatos que fortalecem os valores humanos. Seu foco são os usuários desses artefatos.

---

mental game or a completeness theorem for protocols with honest majority. STOC 1987, pp. 218-229. Michael Ben-Or, Shafi Goldwasser e Avi Wigderson: Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). STOC 1988, pp. 1-10. David Chaum, Claude Crépeau e Ivan Damgard: Multiparty unconditionally Secure protocols (extended abstract). STOC 1988, pp. 11-19.

[71] Por exemplo, compare as páginas iniciais de: Goldreich: Foundations of cryptography - a primer. Foundations and Trends in Theoretical Computer Science, 1(1), pp. 1-116, 2004. E dos: George Danezis e Seda Gürses: A critical review of 10 years of privacy technology. Proceedings of Surveillance Cultures: A Global Surveillance Society?, 2010.

Eles estão profundamente preocupados com política e tecnologias de vigilância. Para onde, depois de Chaum, foi o espírito moral da criptografia acadêmica? Talvez em direção ao PETS.

Há um aprendizado nisso tudo. Alguns podem pensar que o foco de uma comunidade é determinado principalmente pelo caráter técnico do tópico que ela pretende estudar. Não é. São as considerações extra científicas que moldam o que é tratado e onde.

**Os cypherpunks.** Mas há um grupo que tem trabalhado há muito sobre o nexo entre criptografia e política: os cypherpunks.[72] Os cypherpunks surgiram no fim da década de 1980, unidos por uma Os cypherpunks surgiram no fim da década de 1980, unidos por uma lista de e-mail e alguns valores difusos.  A crença central é que a criptografia poderia ser uma ferramenta-chave para proteger a autonomia individual ameaçada pelo poder[73].

Os cypherpunks acreditavam que uma questão-chave de nossa época era de se os interesses do Estado e das corporações iriam estripar as liberdades por meio da vigilância eletrônica e de suas consequências ou de se, em vez disso, as pessoas se protegeriam por meio do uso maestral da criptografia.
Os cypherpunks não buscavam um mundo de privacidade universal: muitos queriam privacidade para o indivíduo e transparência para o governo e para grandes corporações. Os cypherpunks imaginavam que seria possível hackear

[72] Andy Greenberg: This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information. Dutton, 2012. Steven Levy: Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Viking Adult, 2001. Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn, Jérémie Zimmermann: Cypherpunks: Freedom and the Future of the Internet. OR Books, 2012. Robert Manne: The cypherpunk revolutionary: on Julian Assange. The Monthly: Australian Politics, Society, & Culture. Março de 2011.

[73] É a mesma crença contida no trabalho, já mencionado, de David Chaum.

grandes corporações. Os cypherpunks imaginavam que seria possível hackear as relações de poder escrevendo o código certo. Criações no estilo Cypherpunk - pense no Bitcoin, PGP, Tor ou WikiLeaks - seriam disruptivas por que desafiam autoridades e pautam liberdades básicas: liberdade de expressão, associação e participação econômica.[74]

**Como** essas ferramentas exatamente moldam a sociedade nem sempre é óbvio. Considere o WikiLeaks. A esperança não é apenas que um público mais bem informado exija prestação de contas e mudança. Em vez disso, Assange vê o abuso governamental e corporativo como formas de conspiração que poderiam ser sufocadas pela mera ameaça de vazamentos. As conspirações seriam gráficos, os nós seriam conspiradores, e as relações de pares entre eles, as arestas. Em vez de remover nós ou desfazer correlações, você poderia enfraquecer qualquer conspiração ao atordoá-la com uma sempre constante ameaça de vazamentos. Quanto mais injusta a conspiração, maior a probabilidade de ocorrerem vazamentos e mais danos eles causarão. À medida que as elites ficam com medo de conspirar, elas o fazem com mais timidez. O sangue da criatura conspiratória engrossa e ela morre[75]. É uma visão fascinante.

São os cypherpunks, e não os criptógrafos, que normalmente são os maiores defensores da criptografia. Julian Assange escreve:

> Mas nós fizemos uma descoberta. Nossa única esperança contra o domínio

[74] Já ouvi acadêmicos criptógrafos dizerem que merecemos crédito por essas criações, pois, independentemente de quem escreveu o código, as ideias derivam de noções criptográficas que vêm de nós. Embora haja alguma verdade nisso, a afirmação ainda parece não ser genuína. O trabalho, em cada caso, surgiu de outro lugar, empregou apenas ferramentas antigas e básicas e foi, no máximo, modestamente adotado por nossa comunidade.

[75] Julian Assange: Conspiracy as governance. Manuscript, 3 de dezembro de 2006. http://cryptome.org/0002/ja-conspiracies.pdf. Finn Brunton: Keyspace: reflections on WikiLeaks and the Assange papers. Radical Philosophy 166, pp. 8-20, Março/Abril de 2011.

> total. Uma esperança que, com coragem, discernimento e solidariedade, poderíamos usar para resistir. Uma estranha propriedade do universo físico no qual vivemos.
>
> O universo acredita na criptografia.
>
> É mais fácil criptografar informações do que descriptografá-las.
>
> Notamos que seria possível utilizar essa estranha propriedade para criar as leis de um novo mundo.[76]
>
> De forma parecida, Snowden escreve[77]:
>
> Em termos tirados da história: não vamos mais falar na fé nos homens, e sim impedir que eles se comportem mal pelas correntes da criptografia.[78]

Quando encontrei esse tipo de discurso pela primeira vez, pensei, presunçosamente, que os autores prometiam além da conta: eles precisavam diminuir o tom dessa retórica para alcançar a precisão. Eu não penso mais assim. Mais envolvidos na implementação de sistemas do que eu jamais serei, os principais cypherpunks entendem mais do que eu sobre sistemas operacionais inseguros, malware, bugs de programação, subversão, canais laterais, usabilidade deficiente, pequenos conjuntos de anonimato e assim por diante. Os Cypherpunks acreditam que, apesar de tais obstáculos, a criptografia ainda pode ser transformadora.

---

[76] Julian Assange: Cypherpunks, op. cit

[77] Não sei se Snowden se considera um cypherpunk, mas o sentimento expresso nessa citação reflete muito bem o discurso cypherpunk.

[78] Edward Snowden, citado em Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, 2014. Snowden está reformulado uma citação de Thomas Jefferson: “In questions of power then, let no more be heard of confidence in man but bind him down from mischief by the chains of the Constitution.”

**A quem favorece a criptografia?** O discurso Cypherpunk parece, às vezes, supor que a criptografia beneficiará as pessoas comuns. Mas é preciso ter cautela aqui. A criptografia pode ser desenvolvida em sentidos que tendem a beneficiar os fracos **ou** os poderosos. Também pode apontar para sentidos que provavelmente não beneficiam a ninguém, exceto o criptógrafo. Vejamos alguns exemplos.

**Encriptação.** Uma razão pela qual as pessoas podem supor que a criptografia beneficia os fracos é que elas estão pensando na criptografia no sentido de uma encriptação convencional. Indivíduos com recursos mínimos podem encriptar textos simples de uma maneira que mesmo um adversário governamental, não será capaz de decriptar sem a chave.

Mas isso ocorre necessariamente desta maneira? Para funcionar, os recursos criptográficos básicos devem ser incorporados aos sistemas, e esses sistemas podem carregar arranjos de poder que não compactuam exatamente com o caráter da ferramenta. Schneier, com sua abordagem enérgica típica, lembra às pessoas que "a encriptação é apenas um monte de matemática, e a matemática não tem um agenciamento próprio."[79] Se um provedor de conteúdo transmite um filme encriptado para um usuário que mantém a chave de decriptação bloqueada em um hardware ou software que ele não tem uma real capacidade de penetrar[80], serão empoderados os provedores de conteúdo, não

[79] Bruce Schneier: Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015. A citação é da p. 131.

[80] Este era o sonho por trás do Trusted Platform Module (TPM), um coprocessador que implementa um conjunto padrão de operações criptográficas a partir de margens resistentes à adulteração. Ver o verbete da Wikipedia "Trusted Platform Module" e a FAQ de Ross Anderson: "Trusted Computing" Frequently Asked Questions. http://www.cl.cam.ac.uk/ rja14/tcpa-faq.html

os usuários. Se combinarmos criptografia de chave pública com um sistema de custódia de chave que o FBI e a NSA podem explorar, vamos empoderar os governos, não as pessoas[81].

Dito isso, acredito que seja correto dizer que a encriptação convencional incorpora uma tendência de empoderar as pessoas comuns. A encriptação oferece suporte direto à liberdade de expressão. Não requer recursos caros ou difíceis de obter. É possibilitada por algo que é facilmente compartilhado. Um indivíduo pode desviar de sistemas com backdoor.[82] Mesmo a linguagem corriqueira para falar sobre criptografia sugere uma visão de mundo em que às pessoas comuns as Alices e Bobs do mundo inteiro - deve ser dada a oportunidade de se comunicar privadamente. E vindo de outra direção, é preciso **trabalho** para incorporar a encriptação em uma arquitetura que eleva o poder, e pode-se encontrar grandes obstáculos para se conseguir isso. O Chipper fracassou completamente. A Computação Confiável, em sua maioria, conseguiu[83].

**IBE.**[84] E quanto à criptografia baseada na identidade (identity-based encryption), a IBE? Esse arranjo foi proposto anos depois por Shamir, com Boneh e Franklin,

[81] Para uma bela discussão sobre o Clipper Chip, ver Michael Froomkin: The metaphor is the key: cryptography, the clipper chip, and the constitution. University of Pennsylvania Law Review, 143(3), pp. 709-897, 1995.

[82] Isso pode ser teoricamente possível, mas difícil na prática: pode ser difícil de realizar por pessoas pouco treinadas tecnicamente. É por isso que se diz: quando a criptografia é criminalizada, apenas criminosos terão criptografia (ou privacidade, ou segurança) (atribuição original da frase desconhecida). N.T. Uma possível origem seria no texto “Why I Wrote PGP”, de Philip Zimmerman.

[83] Por outro lado, algumas outras formas de DRM (Digital Rights Management) criptograficamente habilitados, incluindo o CSS (Content Scrambling System), usado para dificultar a cópia de DVDs, tem sido razoavelmente eficaz (do ponto de vista dos proprietários de conteúdo).

[84] Ideias expressas neste tópico são de co-autoria de Mihir Bellare.

proporcionando um trabalho satisfatório e demonstravelmente seguro[85]. O objetivo é permitir que o endereço de e-mail de uma pessoa, por exemplo, sirva como sua chave pública. Portanto, se Alice já sabe o endereço de e-mail de Bob, ela não vai precisar conseguir sua chave pública para enviar a ele uma mensagem encriptada: ela apenas encripta com o endereço de e-mail de Bob.

Mas essa praticidade é possibilitada por uma mudança radical no modelo de confiança: a chave secreta de Bob não é mais escolhida por ele mesmo. É emitida por uma autoridade de confiança. Essa autoridade conhece a chave secreta de todos no sistema. A IBE incorpora a custódia de chave - de fato uma forma de custódia de chave onde uma única entidade implicitamente guarda todas as chaves secretas - mesmo aquelas que ainda não foram requisitadas. E mesmo que você **confie** na autoridade geradora de chaves, um adversário de nível governamental agora tem um lócus extremamente cobiçado para ser intimado ou subvertido. No final, do ponto de vista da privacidade pessoal, a IBE pode parecer um enorme retrocesso.

As descrições da IBE geralmente não enfatizam a mudança no modelo de confiança[86]. E a autoridade emissora da chave parece nunca ter um nome assim: é apenas o PKG, para “Private Key Generator”. Isso parece mais inócuo do que é - e mais como um algoritmo do que uma entidade. Em artigos científicos, o PKG cada vez mais perde destaque pelo fato de que é a sequência de algoritmos,

[85] IAdi Shamir: Identity-based cryptosystems and signature schemes. Crypto ’84, pp. 47-53, 1984. Dan Boneh e Matthew Franklin: Identity-based encryption from the Weil pairing. SIAM J. of Computing, 32(3), pp. 586-615, 2003. Ver também Ryuichi Sakai, Kiyoshi Ohgishi, Masao Kasahara: Cryptosystems based on pairing. The 2000 Symposium on Cryptography and Information Security, 2000.

[86] Por exemplo, o verbete “ID-based encryption” (em novembro de 2015) tem uma sessão principal que falha em até mesmo mencionar a presença de uma autoridade emissora de chave.

e não as entidades que supostamente os administram, que estabelece as definições e as provas formais.

Para esclarecer, não estou condenando a IBE como algum tipo de tecnologia fascista. Isso soaria bobo. Nem estou sugerindo que a IBE não possa ser refinada de forma a tornar o modelo de confiança menos autoritário.[87] No entanto, pode-se facilmente perceber a tendência autoritária embutida na IBE. E as tecnologias, embora adaptáveis, não o são infinitamente. À medida que evoluem, eles tendem a manter suas orientações tácitas.

**Privacidade diferencial.** Consideremos a privacidade diferencial[88]. Dwork diz que a Ɛ-privacidade diferencial "aborda as preocupações que qualquer participante possa ter sobre o vazamento de suas informações pessoais: mesmo se a participante houvesse removido seus dados do conjunto de dados, nenhuma saída (...) se tornaria significativamente mais ou menos provável"[89].

Em algum nível, isso parece ótimo: nós não queremos proteger os indivíduos de vazamentos de bases de dados de agentes privados ou governamentais que comprometem a privacidade? Uma perspectiva mais crítica e menos institucionalmente amigável, no entanto, faz com que essa linha de definição pareça insuficiente[90]. Basicamente, o modelo implicitamente

[87] Para muitos esquemas de IBE, é fácil distribuir o segredo do PKG, a chave mestra, por um conjunto de partes. Pode-se ainda organizar a geração distribuída desta chave, para que nenhuma das partes a tenha. Ambos esses pontos são feitos no artigo original de Boneh e Franklin: op cit., Seção 6, Distributed PKG.

[88] Ver, por exemplo, Cynthia Dwork: Differential privacy: a survey of results. Theory and Applications of Models of Computation, pp. 1-19, Springer, 2008.

[89] Ibid, p. 2.

[90] Para uma crítica bem diferente da privacidade diferencial, ver Jane Bambauer, Krishnamurty Muralidhar, Rathindra Sarathy: Fool's gold: an illustrated critique of differential privacy. Vanderbilt

retrata o proprietário do banco de dados (o agente detentor) como o mocinho, e os usuários que o consultam, o adversário. Se o poder simplesmente concordasse em camuflar as respostas da maneira correta, não haveria problema em manter grandes quantidades de dados pessoais sobre cada um de nós. Mas o histórico de violações de privacidade de dados sugere que a principal ameaça para nós vem dos próprios detentores dos bancos de dados e daqueles que ganham acesso total a eles (por roubo ou programas secretos governamentais, por exemplo).

Em segundo lugar, o dano que a privacidade diferencial busca evitar é concebido em termos inteiramente individualistas. Mas violações à privacidade causam danos a comunidades inteiras. O foco individualista pressupõe uma ideia estreita do valor da privacidade. Finalmente[91], a privacidade diferencial pressupõe implicitamente que a coleta de dados serve a algum bem comum. Mas, rotineiramente, esta é uma afirmação altamente contestável. A alternativa por menos - ou nenhuma - coleta de dados é raramente sequer mencionada. No fim do dia, é preciso comparar a redução de danos proporcionada pela privacidade diferencial com um aumento de danos resultantes de empresas terem meios adicionais de limparem sua reputação e de legisladores acreditarem, erroneamente, que existe algum tipo de cripto-mágica para proteger as pessoas do uso indevido de dados.

Recentemente, perguntei a um especialista em privacidade diferencial, Ilya Mironov, sobre sua reação à minha dura crítica. Ele explicou que as funções

Journal of Entertainment and Technology Law, 16(4), pp. 701-755, Summer 2014.

[91] Colleen Swanson, comunicações pessoais.

abstratas em arranjos de privacidade diferencial não precisam corresponder às relações comerciais dessa maneira “óbvia”. Por exemplo, uma organização preocupada com privacidade pode optar por fazer seus próprios analistas acessarem dados confidenciais por meio de uma API que fornece alguma garantia de privacidade diferencial, tratando efetivamente seus próprios funcionários como “adversários”. Mironov também explicou que existem noções variantes de privacidade diferencial que não consideram implicitamente o proprietário do banco de dados como “bom” e aqueles que o consultam como “mau”. Ele descreveu a privacidade diferencial no **modelo local**[92], onde cada um guarda seus dados para si mesmo. Eles podem calcular, de forma distributiva, as respostas em relação às consultas. Fundamentalmente, Mironov explicou que a definição de privacidade diferencial é agnóstica em relação ao modelo de dados.

Embora tudo explicado faça sentido, não acho que isso mude a paisagem. Nenhum mecanismo real pode ser independente de quais dados residem e onde. E à medida em que uma arquitetura e mecanismo de mineração de dados são estabelecidos, considerações sobre eficiência, familiaridade e economia - pra não mencionar o desejo básico das autoridades em possuir e manter os dados - tornam mais fácil prever o que acontecerá: quase sempre, um modelo centralizado surgirá. Para mim, a privacidade diferencial pode ser tão autoritária em seus fundamentos conceituais quanto a IBE.

[92] Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, e Moni Naor: Our data, ourselves: privacy via distributed noise generation. Eurocrypt 2006, pp. 486-503. Para uma exploração das limitações do modelo local, ver também Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, e Adam Smith: What can we learn privately? SIAM Journal of Computing, 40(3), pp. 793-826, 2011. Amos Beimel, Kobbi Nissim, e Eran Omri: Distributed private data analysis: on simultaneously solving how and what. CRYPTO 2008, pp. 451-468. Also arXiv:1103.2626

**FHE e iO.** Desde o seminal trabalho de Craig Gentry[93], a encriptação completamente homomórfica (FHE)[94] tem sido objeto de uma dados - encriptados por uma chave pública de sua escolha - a um provedor de serviços. Mais tarde, você pode pedir a esse provedor o que você quiser daquele purotexto. O provedor vai processar a resposta encriptada sem saber o que ela significa. E ela é devolvida a você para decriptação.

Do ponto de vista político, a FHE parece empoderadora - até mesmo uma utopia. É negado a uma parte poderosa - um provedor de serviços em nuvem, digamos - acessar seus dados. Você devolve a "barganha faustiana" que rotineiramente fundamenta a computação em nuvem.[95]

Mas a análise acima pode enganar. Ainda é bastante especulativo se a FHE algum dia vai evoluir para algo útil na prática. Se você quiser avaliar as inclinações políticas de algo de utilidade especulativa, não deve simplesmente presumir que isso vai dar origem às aplicações alardeadas e, em seguida, deve tentar ver quem ganharia e quem perderia. É muito conjectural. É melhor focar em como essa busca nos impacta aqui e agora.

E sobre isso, eu diria que a FHA, junto com a "iO"[96], tem engendrado uma

---

[92] Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, e Moni Naor: Our data, ourselves: privacy via distributed noise generation. Eurocrypt 2006, pp. 486-503. Para uma exploração das limitações do modelo local, ver também Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, e Adam Smith: What can we learn privately? SIAM Journal of Computing, 40(3), pp. 793-826, 2011. Amos Beimel, Kobbi Nissim, e Eran Omri: Distributed private data analysis: on simultaneously solving how and what. CRYPTO 2008, pp. 451-468. Also arXiv:1103.2626

[93] Craig Gentry: Fully homomorphic encryption using ideal lattices. STOC 2009.

[94] N.T.: Fully homomorphic encryption, no original.

[95] Refiro-me, claro, à transação de informações pessoais pelo serviço.

[96] O acrônimo é para indistinguishability obsfuscation. Sanjam Garg, Craig Gentry, Shai Halevi,

nova onda de exuberância. Em propostas de financiamento, entrevistas na mídia e palestras, os principais teóricos abordam o FHE e o iO como indicações disruptivas do ponto em que chegamos[97]. Ninguém parece enfatizar o quão especulativo é que qualquer uma dessas coisas terá algum impacto na prática. Tampouco as pessoas enfatizam o desaparecimento de nossa privacidade, nossa péssima segurança computacional ou quão pouco a criptografia moderna realmente fez para mudar esse cenário. E isso tem consequências. (a) Isso confunde o público sobre nossa situação. (b) Isso desvia fundos de áreas com mais chances de terem utilidade social. (c) Isso encoraja jovens e brilhantes pesquisadores(as) a trabalhar em caminhos que não são práticos. (d) E isso fornece uma proteção útil aos maiores oponentes da privacidade: agências de defesa e inteligência.

Deixe-me ampliar essa última alegação. Aqui está o que o Diretor de Programas da DARPA, Dan Kaufman, tem a dizer sobre a FHE em uma entrevista de 2014:

> Imagine um futuro que diga: ok, eu tenho que coletar tudo para que o big data funcione, porque se eu soubesse o que não é relevante, não seria o big data. Mas eu não quero que o governo bisbilhote meus e-mails: isso seria assustador. (...)

---

Mariana Raykova, Amit Sahai, e Brent Waters: Candidate indistinguishability obfuscation and functional encryption for all circuits. FOCS 2013, pp. 40-49. Trabalhos prévios introduzindo o iO: Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, e Ke Yang. On the (im)possibility of obfuscating programs. JACM, 59(2):6, 2012. Versão anterior na CRYPTO 2001.

[97] Ver, por exemplo, Erica Klarreich: Perfecting the art of sensible nonsense. Quanta Magazine, 30 de Janeiro, 2014. “Os pesquisadores estão saudando o novo trabalho como um divisor de águas para a criptografia. (...) Se o problema de ofuscação foi resolvido, o que resta para os criptógrafos?” Kevin Hartnett: A New Design for Cryptography’s Black Box. Quanta Magazine, 2 de setembro de 2015. “Novos avanços mostram como a segurança computador quase-perfeita pode estar surpreendentemente alcançável.”

> Então esse cara, Craig Gentry, (...) mostrou que você podia (...) pegar dados, encriptá-los, enviá-los pela rede, nunca decriptá-los, [mas] ainda trabalhar [o processamento] (...) neles. Parece loucura, exceto pelo fato dele ter mostrado que você pode fazer isso (...).
>
> Você poderia imaginar o seguinte (...) [Organizações] coletam (...) dados, mas apenas de (...) forma encriptada(...). Agora, digamos que você acredita que há um potencial criminoso escondido nesse conjunto de dados encriptados. Então, eu tenho um monte de termos de busca (...). Eu poderia então ir a um juiz (...) [e ele] poderia dizer "sim, parece razoável". Eu faço a pesquisa no mecanismo, mas (...) tudo o que sai é um número: quantas pessoas atendem a esses critérios (...) Você volta para o tribunal da FISA, e diz "ok pessoal, temos 12 (...)" Eu imagino a FISA inserindo uma chave e, em seguida, a Agência inserindo uma chave, e os dois a viram. E, [naquele] ponto, pela primeira vez, (...) aqueles 12 são agora revelados.[98]

É claro, isso é um absurdo total. Para começar, não há como entender quem possui qual chave e para quais dados seria aplicada a FHE. Também nos disseram: precisamos coletar tudo porque, se não o fizéssemos, não teríamos dados suficientes para ter muitos dados; que o governo terá cuidado, pois seria "assustador" se não o tivesse; que vão obter ordens judiciais - até mesmo para, aparentemente, descobrir o número de pessoas no conjunto de dados que satisfazem um critério de busca específico; e que, para terem informações que identificassem pessoas, vão precisar da cooperação da NSA e de uma Corte da FISA.

[97] Evelyn M. Rusli: A Darpa [sic] director on fully homomorphic encryption (or one way the U.S. could collect data). Wall Street Journal blog: blogs.wsj.com. 9 de março de 2014.

A entrevista, ainda incipiente, de Kaufman é apenas uma pequena parte de discursos de um oceano de ideias desorientadas sobre privacidade. Não refuta a FHE, mas sugere como o poder visa usar esse tipo de abordagem: deixá-los murmurar quaisquer palavras que pareçam amigáveis à privacidade. Fornecer fortes financiamentos para FHE e iO oferece proteção política livre de riscos. Oferece suporte a uma narrativa de que o armazenamento em nuvem e o processamento são seguros. Ajuda a consolidar valores que já se sobressaem na comunidade criptográfica: direções especulativas, centradas na teoria. E ajuda a manter acadêmicos inofensivos, os quais poderiam, caso fossem combativos, começar a inovar em direções mais importantes.

**Criptoanálise:** Finalmente, deixe-me mencionar brevemente a criptoanálise. Pode-se interpretar erroneamente o empreendimento criptoanalítico acadêmico como um ataque à privacidade de usuários legítimos - um ataque aos inofensivos Alice e Bob - o que favoreceria, então, aqueles que são poderosos.[99] Mas isso é o oposto da visão correta. A razão pela qual os criptógrafos acadêmicos fazem a criptoanálise é para informar melhor os projetistas e usuários de criptossistemas sobre o que é e o que não é seguro fazer. A atividade não é feita para vigiar as pessoas, mas para ajudar a garantir que as pessoas não sejam vigiadas - pelo menos por meios criptoanalíticos. E o trabalho rotineiramente tem exatamente esse efeito. A história do WEP é um bom exemplo.[100]

[99] Adi Shamir, comunicações pessoais. Dezembro de 2015.

[100] A WEP (Wired Equivalent Privacy) era um protocolo criptográfico defeituoso que acompanhou as primeiras redes 802.11 (Wi-Fi). Uma série de ataques devastadores resultou na substituição da WEP por um esquema melhor. O primeiro dos ataques foi: Scott Fluhrer, Itski Mantin, e Adi Shamir: Weaknesses in the key scheduling algorithm of RC4. Selected Areas of Cryptography (SAC 2001),

Quando o NSA ou o GCHQ se envolvem em criptoanálise, é para um propósito muito diferente e tem um efeito muito diferente. Isso significa que a criptoanálise feita por um grupo de pessoas (fantasmas) tenderá a favorecer a autoridade, enquanto a criptoanálise feita por outro grupo de pessoas (acadêmicos) tenderá exatamente na direção oposta? É verdade. O trabalho específico será diferente; sua disseminação será diferente; e seu impacto sobre os direitos humanos será diferente.

**Engajados de forma não ameaçadora.** Claro que não passou despercebido pelas agências de inteligência que a maioria da comunidade criptográfica acadêmica é engajada de forma não ameaçadora. Em um relatório de viagem sobre o Eurocrypt 1992, cujo sigilo foi suspenso, o autor da NSA opina, por exemplo:[101]

> Não houve propostas de criptossistemas, nenhuma nova criptoanálise de designs antigos e mesmo muito pouco sobre design de hardware. Eu realmente não vejo como as coisas poderiam ter sido melhores para nossos propósitos.

O boletim informativo da NSA no qual esse relatório aparece nunca mais mencionaria essa comunidade criptográfica acadêmica[102]. Nenhum documento divulgado derivado de Snowden discutiu qualquer coisa sobre nossa comunidade[103].

[101] Eurocrypt 1992 revisada. Nome do autor redigido. National Security Agency CRIPTOLOG. Primeira edição de 1994. Disponível em http://tinyurl.com/eurocrypt1992

[102] 136 edições da newsletter da NSA, CRYPTOLOG, estão disponíveis de forma redigida. O período coberto é entre 1974 e 1976. Um arquivo pode ser encontra em https://www.nsa.gov/public info/declass/cryptologs.shtml

[103] É claro que o Tor é amplamente discutido nos documentos de Snowden - mas seria errado

É como se tivéssemos progredido de um bando de filósofos[104], que valessem algumas páginas de comentários irônicos[105], para um grupo insignificante demais até mesmo para isso.

**Conclusão à parte 2.** Um ensaio de Arvind Narayanan, de 2013, sugere uma simples taxonomia ao trabalho criptográfico:[106] há **criptografia-para-segurança** e **criptografia-para-privacidade**. A criptografia-para-segurança é uma criptografia para fins comerciais. É a criptografia em TLS, cartões de pagamento e telefones celulares. A criptografia-para-privacidade tem objetivos sociais ou políticos. Aqui, o autor distingue entre **criptografia pragmática** - que trata de tentar usar criptografia para manter nossa privacidade em uma era pré-digital - e a **criptografia cypherpunk** - a grande esperança no uso de criptografia para causar amplas reformas sociais ou políticas. O autor sugere que a criptografia-para-segurança funcionou bem, mas a criptografia-para-privacidade se saiu mal.

Acho que a divisão de Narayanan é esclarecedora, mas ele deixa de mencionar que a maior parte da criptografia acadêmica não é realmente criptografia-para-segurança ou criptografia-para-privacidade: é, pode-se dizer, **criptografia-para-criptografia** - o que significa que não beneficia ostensivamente o comércio **ou** a privacidade, e ainda é bastante especulativo se algum dia vai evoluir para qualquer um dos dois caminhos. Talvez todo

enxergar o Tor como uma contribuição proveniente da comunidade criptográfica, ou mesmo algo algo muito trabalhado dentro dela.

[104] É com esse termo que se refere o autor da NSA acima citado.

[105] O uso do termo “snarky” [no original] aqui vem de Bruce Schneier: Snarky 1992 NSA report on academic cryptography. Post de blog, 18 de novembro de 2014. https://www.schneier.com/blog/archives/2014/11/snarky 1992 nsa.html

[106] Arvind Narayanan: What happened to the crypto dream? Part 1, in IEEE Security and Privacy Magazine, 11(2), pp. 75-76, 2013. Part 2 in IEEE Security and Privacy Magazine, 11(3), pp. 68-71, 2013

campo eventualmente se torne basicamente autorreferencial. Talvez até seja necessário, até certo ponto. Mas, para a criptografia, muito se perde quando nos tornamos tão introvertidos que quase ninguém está trabalhando em problemas que **poderíamos** ajudar, que atendam a alguma necessidade humana básica. A criptografia-para-criptografia mantém a criptografia-para-privacidade desassistida, deixando um buraco, tanto técnico quanto ético, no que fazemos coletivamente.

# Parte 3: O mundo distópico de vigilância pervasiva

A vigilância em massa motivou o conteúdo deste ensaio. Mas seria ela uma coisa tão séria? Antes das revelações de Snowden[107], eu realmente não pensava assim. Os problemas ambientais pareciam mais ameaçadores para o futuro do homem e as guerras intermináveis do meu país pareciam mais merecedoras de indignação moral. Foi só com Snowden que finalmente internalizei que o problema da vigilância era grave, estava intimamente ligado aos nossos valores e nossa profissão, assim como estava sendo enganosamente enquadrado.

**O enquadramento das forças de aplicação da lei.** O **enquadramento** da vigilância em massa determina os termos em que alguém pensa sobre tal questão[108]. E a vigilância em massa foi brilhantemente enquadrada por forças de autoridade, de modo a inclinar o discurso em uma direção específica e previsível. Deixe-me descrever o que chamarei de **enquadramento das forças de aplicação da lei** conforme regularmente promovido pelo [então] Diretor do FBI, James Comey:[109]

[107] Para uma revisão de informações centrais extraídas das revelações de Snowden, ver a webpage da EFF "NSA Spying on America", https://www.eff.org/nsa-spying, e a webpage da ACLU, "NSA Surveillance", https://www.aclu.org/issues/nationalsecurity/privacy-and-surveillance/nsa-surveillance.

[108] Collin Bennett: The Privacy Advocates: Resisting the Spread of Surveillance. The MIT Press, 2008

[109] James Comey: "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" Discurso no Brookings Institute, 16 de outubro, 2014. http://tinyurl.com/comey-going-dark

**1.** A privacidade é um bem pessoal. É sobre seu desejo de controlar informações pessoais sobre você.

**2.** A segurança, por outro lado, é um bem coletivo. É sobre viver em um mundo seguro e protegido.

**3.** Privacidade e segurança estão inerentemente em conflito. Ao fortalecer um, você enfraquece o outro. Precisamos encontrar o equilíbrio certo.

**4.** Tecnologias de comunicação modernas destruíram o equilíbrio anterior. Tem sido uma vantagem para a privacidade e um golpe para a segurança. A criptografia é especialmente ameaçadora. Nossas leis simplesmente não dão conta.[110]

**5.** Por causa disso, os bandidos podem vencer. Os bandidos são terroristas, assassinos, pedófilos, traficantes de drogas e os os que lavam dinheiro[111]. A tecnologia que nós, pessoas do bem, usamos, também é usada por bandidos para não serem detectados.

**6**. Neste ponto, estamos sob o risco do **obscurecimento.**[112] Mandados

[110] Comey fala especialmente sobre a CALE, a Communications Assistance for Law Enforcement Act, a lei norte-americana de 1994 que prevê obrigação de que capacidades de interceptação sejam previstas em aparatos de telecomunicações - mas que não obriga tais habilidades para emails encriptados, mensageria instantânea e outros da espécie.

[111] O elenco tradicional de malfeitores, os "quatro cavaleiros do info-pocalipse", omite assassinos desta lista de cinco; ver Assange et al., Cypherpunks, op. cit. Observe que, no discurso de Comey do Instituto Brookings, o orador adiciona assassinos a esta lista e subtrai os lavadores de dinheiro. A jogada é astuta; a lavagem de dinheiro é um crime tecnocrático e legalista em comparação com o assassinato.

[112] A frase é do discurso de Comey que acabamos de citar. N.T. Going Dark, no original.

> serão emitidos, mas, devido à criptografia, não farão sentido. Estamos nos tornando um país de cofres que não podem ser abertos. A criptografia por padrão pode ser um bom pitch de vendas, mas é um design imprudente. Isso nos levará a um lugar bastante obscuro.

A narrativa é inconsistente com a história da coleta de inteligência e com a própria declaração de missão da NSA[113]. No entanto, a desconfortável coexistência da narrativa com a realidade não foi levada em conta. Na verdade, a narrativa é eloquentemente elaborada para enquadrar as questões de uma forma que garanta o direcionamento do discurso para onde a autoridade deseja que ele vá. É um discurso brilhante sobre o medo: medo do crime, medo de perder a proteção de nossos pais, até mesmo medo do escuro. O engano da narrativa em si, bem elaborado, é uma forma de habilidade.[114]

**O enquadramento dos estudos de vigilância.** Claro que há diferentes formas de enquadrar a vigilância em massa. Considere a seguinte forma de fazê-lo, levando em conta construções recorrentes de cypherpunks e dos estudos de vigilância.[115]

**1.** A vigilância é um instrumento de **poder**[116]. É parte de um aparato de

[113] Church Committee Reports, 1975-1976. Disponível em http://www.aarclibrary.org/publib/church/reports/contents.htm. Frank Donner: The Age of Surveillance: The Aims and Methods of America's Political Intelligence System. Vintage Press, 1981. Classified NSA document: SIGINT Mission Strategic Plan FY2008-2013. 3 de outubro, 2007. http://tinyurl.com/sigint-plan

[114] "A artimanha verbal é, por si só, uma atividade de inteligência", explica Donner. op. cit., p. Xiv. Ver também seu Appendix I, pp. 464-466

[115] Michel Foucault: Discipline and Punish: The Birth of the Prison. Alan Sheriden, tradutor. 1975/1977. Frank Donner, op. cit. Assange et al., op. cit. David Lyon: Surveillance Studies: An Overview. 2007. David Murakami Wood e Kirstie Ball: A Report on the Surveillance Society. Set. 2006.

[116] Mesmo a etimologia da vigilância sugere isso: do francês: sur, que significa por cima, mais

controle. O poder não precisa estar na sua cara para ser eficaz: métodos sutis, psicológicos, quase invisíveis, podem, na verdade, ser mais eficazes.

**2.** Embora a vigilância não seja nenhuma novidade, as mudanças tecnológicas deram aos governos e corporações uma capacidade sem precedentes de monitorar a comunicação e o movimento de todos. Vigiar a todos ficou mais barato do que descobrir quem vigiar e o custo marginal agora é minúsculo[117]. A Internet, antes vista por muitos como uma ferramenta de emancipação, está se transformando no facilitador mais perigoso já visto para o totalitarismo.[118]

**3.** A vigilância governamental está fortemente ligada à ciberguerra. Vulnerabilidades de segurança que habilitam um também habilitam o outro. E, pelo menos nos EUA, os mesmos indivíduos e agências cuidam de ambos os trabalhos. A vigilância também está fortemente ligada à guerra convencional. Como explicou o general Michael Hayden, "nós matamos pessoas com base em metadados."[119] Vigilância e assassinato por drones são um só ecossistema tecnológico.

---

veiller, que significa observar. Assim: observar por cima, de uma posição de poder. Uma reviravolta interessante nessa concepção é a noção de sousveillance, conforme cunhada por Steve Mann. Veja o verbete da Wikipedia: Sousveillance.

[117] Adicionar mais um número de telefone a uma escuta telefônica é praticamente de graça. Kevin S. Bankston e Ashkan Soltani: Tiny constables and the cost of surveillance: making cents out of United States v. Jones. The Yale Law Journal, vol. 123, Jan. 2014

[118] Essa frase é ligeiramente modificada de Assange et al., Cypherpunks, op. cit.

[119] Michael Hayden: The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA. 9 de maio 9, 2014. Disponível em https://www.youtube.com/watch?v=kV2HDM86XgI

**4.** A narrativa das forças de aplicação da lei está errada ao posicionar a privacidade como um bem individual quando ela é, na verdade, um bem social. É igualmente errado considerar a privacidade e a segurança como valores conflitantes, já que a privacidade **eleva** a segurança com a mesma frequência com que a desafia.

**5.** A vigilância em massa tende a produzir pessoas uniformes, dóceis e superficiais[120]. Ela frustrará ou reverterá o progresso social. Em um mundo de monitoramento onipresente, não há espaço para descobertas pessoais, nem espaço para desafiar as normas sociais. Vivendo com medo, não existe liberdade genuína.

**6.** Mas a vigilância gradual e imperceptível é difícil de parar devido ao entrelaçamento de interesses corporativos e governamentais.[121] A criptografia oferece pelo menos alguma esperança. Com ela, pode-se criar um espaço livre do alcance do poder.

A história ensina que a vigilância governamental pervasiva se torna política por essência. Conforme o advogado de direitos civis Frank Donner e a Church Commission documentam exaustivamente, a vigilância doméstica sob a direção do FBI dos EUA, J. Edgar Hoover, serviu como um mecanismo para

[120] Para a última dessas afirmações: "Uma vida passada inteiramente em público, na presença de outras pessoas, torna-se, como diríamos, superficial. "Hannah Arendt, The Human Condition. Chicago University Press, 1959.

[121] É claro que empresas e governos também, ocasionalmente, têm interesses conflitantes, como quando a publicidade sobre vigilância espanta os clientes. Essa é a tônica que motiva os princípios enunciados em https://www.reformgovernmentsurveillance.com/

[122] Church, op. cit.; Donner, op. cit.; e Julian Sanchez: Wiretapping's true danger. Los Angeles Times, 16 de março de 2008. http://articles.latimes.com/2008/mar/16/opinion/ op-sanchez16

proteger o status quo e neutralizar os movimentos por mudança.[122] Apenas uma pequena parte dos esforços do FBI relacionados à vigilância foi dirigida à aplicação da lei: como as atividades vigiadas raramente eram ilegais, o comportamento indesejável resultaria em sabotagem, ameaças, chantagem e processos criminais inapropriados. Por exemplo, aproveitando as fitas de vigilância de áudio, o FBI tentou fazer com que o Dr. Martin Luther King Jr. se matasse.[123] As universidades americanas foram completamente infiltradas com informantes: alunos, professores, funcionários e administradores escolhidos se reportariam a uma extensa rede de encarregados do FBI sobre qualquer questão política acontecendo no campus. A vigilância da dissidência tornou-se um pilar institucional para a manutenção da ordem política. O programa COINTELPRO dos EUA duraria mais de 15 anos, reconfigurando permanentemente o cenário político dos EUA.[124]

**Nosso futuro distópico.** Tem sido brilhante explorado pela ficção os rumos para onde a vigilância em massa conduz, a começar pelo romance de Yevgeny Zamyatin, Nós (que inspirou Orwell em 1984), de 1921. Situados em um futuro de vigilância total, os habitantes do “Um Estado" internalizaram lições como: “nós" é de Deus e “Eu" é do diabo; que imaginação é uma doença; e que a chave para livrar o homem do crime é livrá-lo da liberdade.

Mas você não precisa recorrer a relatos fictícios ou históricos para prever

[122] Church, op. cit.; Donner, op. cit.; e Julian Sanchez: Wiretapping’s true danger. Los Angeles Times, 16 de março de 2008. http://articles.latimes.com/2008/mar/16/opinion/ op-sanchez16

[123] Nadia Kayyali: FBI’s “Suicide Letter” to Dr. Martin Luther King, Jr., and the Dangers of Unchecked Surveillance. 12 de novembro de 2014. Website da EFF, http://tinyurl.com/fbi-suicide-letter

[124] Church Committee Reports, op. cit., e Frank Donner, op. cit.

para onde estamos indo. Em uma coluna do boletim informativo de 2012, o "Filósofo da SIGINT" da NSA, Jacob Weber, compartilha sua própria visão. Depois de falhar em um teste de detector de mentiras da NSA, ele diz: informativo de 2012, o "Filósofo da SIGINT" da NSA, Jacob Weber, compartilha sua própria visão. Depois de falhar em um teste de detector de mentiras da NSA, ele diz:

> Desejei que minha vida fosse constante e completamente monitorada. Pode parecer estranho que um libertário autoproclamado deseje uma distopia orwelliana para si mesmo, mas aqui estava meu raciocínio: se as pessoas soubessem algumas coisas sobre mim, eu poderia parecer suspeito. Mas se as pessoas soubessem tudo sobre mim, elas veriam que não tinham nada a temer.
>
> (...) O alvo que[125] não tem más intenções para com os EUA, mas que está sendo monitorado, precisa de melhor e de mais monitoramento, não menos. Então é melhor "ir com tudo".[126]

Cercados por grandes segredos e complexidade, os contornos básicos do estado de vigilância são fundamentalmente desconhecidos. O que o indivíduo deveria fazer? Com os dispositivos de comunicação de todo mundo monitorados, ele sabe que é um alvo de fato. Milhões de observações são feitas de sua vida. Ele é analisado por técnicas que nem de longe consegue entender.

---

[125] Observe o uso do "o alvo que", ao invés de quem: o alvo não é uma pessoa, mas uma coisa.

[126] Jacob Weber (deanonimizado pelos leitores do The Intercept): The SIGINT Philosopher Is Back - with a New Face! SIDtoday. 29 de maio, 2012. goo.gl/TyBzig. Peter Maass escreve sobre o SIGINT Philosopher em: The Philosopher of Surveillance, The Intercept, 11 de agosto de 2015. Seu artigo pode ser o meu favorito de todo o corpus de artigos provenientes das revelações de Snowden. Funciona em vários níveis, dando ao leitor a desconfortável sensação de fazer para outro (e até mesmo gostar de fazer para outro) exatamente o que ele não gostaria que fizesse a si mesmo. "A vida moderna é uma mistura profana de voyeurismo e exibicionismo ", diz a personagem de Stella Gibson (Gillian Anderson) na série de TV de Allan Cubitt, The Fall (2014) (temporada 2, episódio 4).

Ele sabe que os dados de hoje e de ontem serão examinados pelos algoritmos de amanhã. Esses vão empregar processamento de linguagem natural sofisticado, mas provavelmente não entenderão o discurso humano. Com tudo isso, o indivíduo racional não tem escolha a não ser observar o que ele diz e tentar agir como todo mundo.

O filme Citizenfour (2014) atinge o seu auge quando consegue esboçar a forma desse mundo emergente. Um crítico escreve sobre o filme

> evocando o Estado moderno como uma presença invisível e onipresente, uma abstração com enormes recursos coercitivos à sua disposição. (...) Está em todo lugar e em lugar nenhum, o Leviatã cuja barriga é nossa atmosfera nativa. O Sr. Snowden - desligando o telefone de seu quarto, escondido sob um cobertor ao digitar em seu laptop, parecendo levemente em pânico quando um alarme de incêndio é testado em seu andar - pode parecer paranóico. Ele também pode parecer estar praticando uma espécie de bom senso de vanguarda.
> É difícil dizer a diferença, e [isto] (...) pode induzir uma espécie de vertigem epistemológica. O que sabemos sobre o que se sabe sobre nós? Quem é que sabe? Podemos confiar neles?[127]

Sendo mais prosaico: eu pego o telefone e ligo para meu colega, Mihir Bellare, ou escrevo um e-mail para ele. Quantas cópias desta comunicação serão armazenadas e por quem? Quais algoritmos irão analisá-los - agora e no futuro? Com quais outros dados serão combinados na tentativa de formar uma imagem

[127] A. O. Scott: Intent on defying an all-seeing eye: 'Citizenfour,' a documentary about Edward Snowden. New York Times movie review, 23 de outubro, 2014.

minha? O que faria um analista humano se envolver? Minha ligação ou e-mail pode contribuir para uma auditoria fiscal, uma decisão de negativa de financiamento, alguns truques sujos no estilo Hoover ou até mesmo um assassinato? Não há uma única pessoa que saiba a resposta a essas perguntas, e aqueles que mais sabem não estão dispostos a dizer.

**Conclusão à parte 3.** Em última análise, não estou muito interessado em queixas individuais sobre privacidade; estou muito mais preocupado com o que a vigilância faz à sociedade e aos direitos humanos. A vigilância totalizada diminui enormemente a possibilidade de dissidência política efetiva. E sem dissidência, o progresso social é improvável.

Considere um episódio como a invasão, em 1971, da filial do FBI em Media, Pensilvânia[128]. Com o grau de vigilância sob o qual vivemos agora, os denunciantes - começando por um professor de física, bastante combativo, que liderou a ação[129] - seriam prontamente presos e até acusados de espionagem. Eles teriam passado anos na prisão ou sido, até mesmo, executados. Diante da probabilidade desses resultados, os ativistas não teriam nem tentado uma invasão tão ousada. Em um ensaio que foca em soluções para a vigilância excessiva, Richard Stallman pergunta

> Qual é exatamente o nível máximo tolerável de vigilância, em que ela se torna uma opressão? Isso acontece quando a vigilância interfere no funcionamento da democracia: quando é provável que denunciantes (como Snowden) sejam pegos.[130]

[128] Betty Medsger: The Burglary: The Discovery of J. Edgar Hoover's Secret FBI. Knopf, 2014.

[129] William Davidon, como revelado em Medsger, The Burglary, Ibid

[130] Richard Stallman: How much surveillance can democracy withstand? Wired, 14 de outubro, 2013.

A vigilância online e por telefonia já resulta na prisão de dissidentes políticos em todo o mundo[131], e é a base do programa de assassinato por drones em meu próprio país.[132] Nos EUA, o policiamento como o de Miami[133] fez com que participar de protestos políticos (ou apenas estar perto de um em seu carro ou com seu telefone) se tornasse algo amedrontador. Com as comunicações de jornalistas monitoradas rotineiramente, o jornalismo investigativo está sob ataque.[134] Em tal ambiente, a democracia e o progresso social são social são possíveis?

Contudo, apesar de todos esses argumentos, sou cético quanto a uma abordagem racionalista sobre afrontas éticas, seja a vigilância em massa ou qualquer outra coisa. Se nos comportamos moralmente, não é por causa de análises racionais, mas por uma
preferência instintiva pela liberdade, empatia ou companhia.[135]
Como Schneier aponta, os animais não gostam de ser vigiados porque os fazem se sentir como presas, enquanto faz o vigilante se sentir - e agir como - um predador.[136] Acho que as pessoas sabem, em um nível instintivo, que uma vida

Ver também http://www.gnu.org/philosophy/surveillance-vs-democracy.html

[131] Reporters without Borders: The Enemies of Internet: Special Edition: Surveillance. 2013. http://surveillance.rsf.org/en/

[132] Jeremy Scahill e Glenn Greenwald: The NSA's secret role in the U.S. assassination program. The Intercept, 9 de fevereiro, 2014.

[133] Greg Elmer and Andy Opel: Preempting Dissent: The Politics of an Inevitable Future. Arbeiter Ring Publishing, 2008. Ver também o filme, Preempting Dissent (2014), by the same team. http://preemptingdissent.com/

[134] Human Rights Watch: With liberty to monitor all: how large-scale US surveillance is harming journalism, law, and American democracy. Julho de 2014.

[135] Michael Gazzaniga: The Ethical Brain: The Science of Our Moral Dilemmas. Dana

[136] Bruce Schneier, op. cit., parafraseando uma passagem da p. 127

na qual nossos pensamentos, discursos e interações que estão sujeitos a constante monitoramento, seja humano ou algorítmico, não é vida. Estamos correndo em direção a um mundo que sabemos, mesmo sem pensamento racional, que não é um lugar ao qual o humano pertence.

# Parte 4: Criando um campo mais justo e útil

O que nós, criptógrafos, podemos fazer de forma realista para aumentar, coletivamente, nossa contribuição à criptografia para a privacidade? Não digo que tenho respostas simples. Posso oferecer apenas ideias modestas.

**Envio de mensagens seguras em um modelo de "servidor não confiável".**

A escolha do problema é o aspecto mais óbvio para se determinar o impacto de nossa comunidade - e o envio de mensagens seguras, em todas as suas formas, continua sendo o problema mais importante para a criptografia-para-privacidade. Embora as redes de mistura o onion routing e as redes DC tenham se mostrado altamente úteis[137], não é tarde demais para se pensar em novas arquiteturas para comunicações seguras.

Considere o seguinte problema - que é inspirado no Pond e no protocolo PANDA que pode ser usado[138]. O objetivo é semelhante ao protocolo Pond de Adam Langley: criar uma alternativa para e-mails ou mensagens instantâneas, mas onde o "big brother" é incapaz de descobrir quem está se comunicando

[137] Joan Feigenbaum e Bryan Ford: Seeking anonymity in an Internet Panopticon. Communications of the ACM, 58(10), Outubro de 2015

[138] Adam Langley: Pond. Webpages rooted at https://pond.imperialviolet.org/. Para PANDA, ver Jacob Appelbaum and "another cypherpunk": Going dark: phrase automated nym discovery authentication: or, finding friends and lovers using the PANDA protocol to re-nymber after

com quem. Ao contrário do Pond, não quero contar com o Tor, já que buscamos segurança diante de um adversário ativo e global (bem como um tratamento de segurança demonstrável e transparente). O Tor sempre poderá ser adicionado, como uma medida heurística, para ocultar os participantes do sistema.

A intenção é esta. Presume-se que pares de pessoas que desejam se comunicar compartilham inicialmente uma senha. Eles não falam diretamente um com o outro; ao invés disso, todas as comunicações passarão por um servidor **não confiável**. Primeiramente, as partes atualizam a sua senha compartilhada para uma chave forte com um protocolo rendezvous anônimo. Depois disso, o remetente pode depositar uma mensagem criptografada (de comprimento constante) no servidor. Quando uma parte deseja recuperar sua i-ésima mensagem, ela irá interagir com o mesmo servidor, o que lhe dá uma sequência de caracteres calculada a partir do conteúdo do banco de dados. O valor permite ao receptor recuperar a mensagem pretendida - ou, alternativamente, uma indicação de que não há a tal i-ésima mensagem para ele. Mas, do começo ao fim, tudo o que o servidor vê são partes depositando as

---

everything is lost: or, discovering new Pond users easily. Manuscript, Fev 21, 2014. https://github.com/agl/pond/tree/master/papers/panda

sequências aparentemente aleatórias no servidor e partes coletando sequências aparentemente aleatórias do servidor, calculadas ao aplicar alguma função não secreta ao banco de dados igualmente não secreto do servidor. Nem o servidor nem um adversário global e ativo podem descobrir quem se comunicou com quem, ou mesmo se uma comunicação ocorreu. O objetivo é fazer tudo isso da forma mais eficiente possível - particularmente com muito mais eficiência do que quando o servidor apenas entrega a cada destinatário o seu inteiro banco de dados de mensagens encriptadas.

Em trabalhos em andamento, eu e alguns colegas estamos elaborando um tratamento de segurança demonstrável para a abordagem acima. Ele usa uma definição convencional baseada em jogos, não os conceitos confusos ou o vocabulário de grande parte da literatura sobre anonimato[139]. Esperamos que as mensagens anônimas neste modelo de servidor não confiável acabem se revelando práticas para configurações de alta latência. Veremos.

**Criptografia de chave longa.** Deixe-me descrever um recente trabalho de Mihir Bellare, Daniel Kane e meu, que chamamos de criptografia de chave longa.[140]A intenção da criptografia de chave longa é permitir que as operações criptográficas dependam de chaves enormes - do comprimento de megabytes a terabytes. Queremos nossas chaves tão grandes que se torne inviável para

[139]Uma tentativa ambiciosa, mas informal de unificar terminologia e conceitos em privacidade e anonimato é fornecida por Andreas Pfitzmann e Marit Hansen: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management | a consolidated proposal for terminology. Version v0.34. 10 de Ago. 2010. Manuscript at http://dud.inf.tu-dresden.de/Anon Terminology.shtml

[140] Mihir Bellare, Daniel Kane, Phillip Rogaway: Bigkey cryptography: symmetric encryption with enormous keys and a general tool for achieving key-exfiltration resistance. Manuscript, 2015.

um adversário extraí-las. Não obstante, usar uma chave tão grande não poderá retardar o processo. Isso implica que, com cada uso, apenas uma pequena fração dos bits da chave longa será inspecionada.

A ideia básica não é nova: o conceito é geralmente referido como segurança em um bounded-retrieval model[141]. Mas nossa ênfase **é** nova: ferramentas práticas e gerais, com limites concretos e bem definidos. Não temos nenhuma objeção em usar o modelo de oráculo aleatório para atingir esses objetivos.

Suponha que você tenha uma chave longa ***K.*** Você deseja usá-la para algum protocolo ***P*** que foi projetado para usar uma chave de comprimento convencional ***K.*** Então escolha um valor aleatório R (talvez 256 bits) e faça um hash para obter um número *p* de sondas ***[probes]*** na chave longa:

$$i_1 = H(R, 1)\ i_2 = H(R, 2)\ \ldots\ i_p = H(R, p)\ .$$

Cada sonda $\mathbf{i}_j$ aponta para ***K:*** é um número entre 1 e |***K***|. Então você pega os bits de *p* nessas posições e faz um hash deles, junto com R, para obter uma chave K derivada.

[141] Stefan Dziembowski: Intrusion-resilience via the bounded-storage model. TCC 2006. Giovanni Di Crescenzo, Richard J. Lipton, Shabsi Walfish: Perfectly secure password protocols in the bounded retrieval model. TCC 2006. David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard J. Lipton, Shabsi Walfish: Intrusion-resilient key exchange in the bounded retrieval model. TCC 2007. Jo ̈el Alwen, Yevgeniy Dodis, Daniel Wichs: Survey: leakage resilience and the bounded retrieval model. ICITS 2009. Trabalhos no modelo “bounded-retrieval” tem raízes anteriores no modelo de “bounded-storage” de Maurer: Ueli Maurer: Conditionally-perfect secrecy and a provably-secure randomized cipher. Journal of Cryptology, 5(1), pp. 53-66, 1992.

$$K = H'(R, \mathbf{K}[i_1], \ldots, K[i_p]) = XKEY(\mathbf{K}, R) .$$

Onde você alternativamente teria usado o protocolo P com uma chave compartilhada ***K***, agora você usa P com uma chave longa compartilhada ***K***, uma R recentemente escolhida, isso determinando a chave convencional K = XKEY (***K***, R).

Nós mostramos que a chave derivada K é indistinguível da chave uniformemente randomizada ***K'***, mesmo se o adversário tiver R e possa aprender sobre muita coisa sobre a chave longa ***K***. O resultado é quantitativo, medindo o quão boa é a chave derivada como parte de uma função do comprimento da chave longa, o número de bits vazados dela, o número de sondas ***p***, o comprimento de R e o número de chamadas do "oráculo aleatório".

No centro desse resultado está uma questão de caráter informacional-teorética que nós chamamos de problema da predição de subchaves. Imagine uma chave randômica ***K*** onde um adversário pode exportar bits $\ell < |\mathbf{K}|$ sobre a informação. Após o vazamento, selecionamento posições ***p*** para ***K***, damos essas posições para o adversário e pedimos ao adversário para prever esses bits ***p***. O quão isso pode dar certo?

Acontece que o adversário **pode** fazer melhor do que apenas gravar $\ell$ bits da chave ***K*** e esperar que várias sondas caiam aí. Mas ele não poderia fazer **muito** melhor. Não tivesse nada sido vazado ao adversário, $\ell = 0$, então cada sonda iria contribuir com cerca de um bit de entropia à variante randômica que o adversário deve descobrir. Mas se, digamos, metade da chave seja vazada,

$\ell \leq |\boldsymbol{K}|/2$, cada sonda agora contribui com cerca de 0.156 bits de entropia[142]. A chance do adversário de vencer o jogo da predição da subchave será limitada a algo como $2^{-0,156}p$. Uma pessoa precisa de cerca de $\boldsymbol{p} = 820$ sondas para uma segurança de 128 bits, ou o dobro para uma segurança de 256 bits.

Eu acho que o problema de previsão de subchaves e o algoritmo de encapsulamento de chave baseado nele darão origem a bons recursos para encriptação autenticada resistente à exfiltração e geradores pseudoaleatórios.[143] Em geral, eu vejo a criptografia de chave longa como uma ferramenta com a qual os criptógrafos podem contribuir para tornar a vigilância em massa mais difícil.

**Mais exemplos.** Aqui estão mais alguns exemplos de trabalho de **Riposte**, de Corrigan-Gibbs, Boneh e Mazières[144]. Um usuário, falando com outras pessoas na Internet, deseja transmitir uma mensagem, como para vazar um documento, sem revelar sua identidade. A rede está sujeita a um amplo monitoramento. Os autores desenvolvem definições, protocolos e provas para o problema, garantindo minuciosamente a eficiência[145]. Eles implementam seus esquemas.

---

[142] A constante de aparência peculiar é o valor (aproximado) de - lg (1 - c) onde c ≈ 0.1100 é o número real em [0; 1 = 2] satisfazendo $H_2$ (c) = 0: 5 onde $H_2$ é a função de entropia binária, $H_2$ (x) = −x lg x - (1 - x) lg (1 - x)

[143] O tipo de PRG que recebe a entrada e mantém o estado, que agora incluirá uma chave longa. Ver Boaz Barak, Shai Halevi: A model and architecture for pseudo-random generation with applications to /dev/random. ACM CCS 2005. Yevgeniy Dodis,David Pointcheval, Sylvain Ruhault, Damien Vergnaud, Daniel Wichs: Security analysis of pseudo-random number generators with input: /dev/random is not robust. ACM CCS 2013.

[144] Henry Corrigan-Gibbs, Dan Boneh, David Mazières: Riposte: An anonymous messaging system handling millions of users. IEEE Symposium on Security and Privacy, pp. 321-338, 2015.

[145] As técnicas vêm principalmente de PIRs, do corpo de trabalho para tornar os PIRs mais eficientes e da noção recente de uma função de ponto distribuída, de Gilboa e Ishai. Benny Chor, Eyal Kushilevitz, Oded Goldreich, Madhu Sudan: Private information retrieval. JACM 45(6), pp. 965-981, 1998. Versões anteriores de FOCS 1995. Niv Gilboa, Yuval Ishai: Distributed point functions and their applications. EUROCRYPT 2014, pp. 640-658.

Combinar todos esses elementos é raro - e muito necessário.[146]

Ou considere o trabalho de Colin Percival no qual ele apresentou a função hash scrypt.[147] Percival explicou que, ao aplicar uma função hash intencionalmente lenta para computar a uma senha e fazer com que seja maior o custo dos ataques de dicionário, seria melhor se a função hash não puder ser acelerada tanto mesmo com um hardware personalizado. Para atingir este objetivo, computar a função hash não deve apenas computar a função hash não deve apenas levar muito tempo, mas também muita memória acessada sequencialmente). Essa grande ideia vem de Abadi, Burrows, Manasse e Wobber, que queriam ter certeza de que, para uma variedade de situações, computar uma função hash intencionalmente lenta em um sistema de ponta levaria aproximadamente o mesmo tempo que computá-la em um sistema de desempenho inferior[149]. Recentemente, uma Password Hashing Competition ((PHC) acabou elegendo um esquema, o **Argon2**[150], que segue esse caminho.

---

[146] Outro artigo recente que faz um belo trabalho na interseção de sistemas, privacidade e criptografia é Nikita Borisov, George Danezis, Ian Goldberg: DP5: A private presence service. Proceedings on Privacy Enhancing Technologies (PETS) vol. 2, pp. 4-24, 2015. Esse artigo depende crucialmente de PIRs - dessa vez para criar um serviço para lhe informar - não pelo provedor do serviço - qual dos seus "amigos" estão online, usando um serviço como o Facebook.

[147] Colin Percival: Stronger key derivation via sequential memory-hard functions. BSDCan'09, Maio, 2009. http://www.tarsnap.com/scrypt/scrypt.pdf

[148] A técnica vem desde a funcionalidade UNIX crypt(3).

[149] Martínn Abadi, Mike Burrows, Mark Manasse, e Ted Wobber: Moderately hard, memory-bound functions. ACM Trans. on Internet Technology, 5(2), pp. 299-327, Maio, 2005. Este artigo inclui uma construção concreta para uma função hash de disco rígido de memória. Uma proposta anterior para uma função hash parametrizada tanto pelo tempo quanto pelo espaço de que ela precisa é fornecida em uma proposta por Arnold Reinhold entitled HEKS: A Family of Key Stretching Algorithms, 15 de julho, 1999 (revised July 5, 2001), http://world.std.com/ reinhold/HEKSproposal. html.

[150] Alex Biryukov, Daniel Dinu, Dmitry Khovratovich: Argon2. 8 de julho, 2015. https://www.cryptolux. org/index.php/Argon2

Enquanto isso, a teoria para esse tipo de função hash têm progredido bem[151]. Embora ainda não tenhamos bons limites em esquemas como scrypt e Argon2, acho que estamos chegando lá[152].

Ou considere o artigo, meu e de alguns colegas, sobre a suscetibilidade da criptografia simétrica à vigilância em massa.[153] Discutimos **ataques de algoritmos de substituição**, em que o "big brother" substitui um algoritmo de criptografia simétrica **real** por um **subvertido**. O objetivo do big brother é decriptar secretamente todo o tráfego encriptado. A ideia remonta a Young e Yung[154]; tudo o que fizemos foi explorar rigorosamente a ideia no contexto da criptografia simétrica. No entanto, o que descobrimos foi perturbador: quase todos os esquemas de criptografia simétrica podem ser facilmente subvertidos. Ainda assim, mostramos que é fácil fazer esquemas onde isso não aconteça.

E há o artigo de **Logjam**, mostrando, pela enésima vez, que devemos estar atentos ao valor criptoanalítico da precomputação[155]. Os ataques devem ser rotineiramente considerados como um processo de duas etapas: um processo

---

[151] Joël Alwen e Vladimir Serbinenko: High parallel complexity graphs and memoryhard functions. TOC 2015, pp. 595-603.]

[152] Em primeiro lugar, trata-se de ajudar os indivíduos a evitar que suas contas sejam comprometidas. Em segundo lugar, para criptoativos, ajuda a manter a mineração em pequena escala mais competitiva em termos de custos com as operações em grande escala. Isso não é verdade para o bitcoin, onde a mineração tende a ser centralizada e consome muita energia. O pool de mineração GHash.IO exibe em seu site uma taxa de mineração de 6,35 Ph/s ($2^{52.5}$ hashes por segundo), and the overall rate is about 465 Ph/s ($2^{58.7}$ hashes per second).

[153] Mihir Bellare, Kenneth G. Paterson, e Phillip Rogaway: Security of symmetric encryption against mass surveillance. CRYPTO 2014.

[154] Adam Young, Moti Yung: The dark side of black-box cryptography, or: should we trust capstone? CRYPTO 1996. Adam Young, Moti Yung: Kleptography: using cryptography against cryptography. EUROCRYPT 1997.

[155] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béuelin, Paul Zimmermann: Imperfect forward secrecy: how Diffie-Hellman fails in practice. Computer and Communications Security (CCS '15), 2015.

dispendioso, que depende de parâmetros amplamente compartilhados, e então um ataque menos custoso e individualizado.[156] Esse pensamento remonta aos primeiros trade-offs entre memória e tempo,[157] e à preferência de muitos criptógrafos por adversários não uniformes. Isso ocorre na prática, como em ataques ao A5/1 em telefones GSM[158]. E é também o modelo para o qual as agências de inteligência parecem gravitar, como sugerido pelo ataque da NSA ao esquema FPE-FF2[159]e o fato de que consideraram esse ataque bastante sério.[160]

**Escolha bem.** Como eu espero que ilustrem os exemplos que dei, existem problemas importantes de criptografia-para-privacidade e eles são bastante diversos. Escolha bem seus problemas. Deixe que valores sociais guiem sua escolha. Muitas vezes falei com pessoas que parecem não ter a menor **ideia** do porquê de estarem estudando o que estão estudando. A resposta que geralmente dão é que elas têm capacidade de fazê-lo, que o trabalho será publicado e que outras pessoas já fizeram isso antes. Esses são péssimos motivos para se fazer algo.

A introspecção não pode ser apressada. Na pressa de publicar artigo

---

[156] Além disso, sempre que possível, o ataque ativo deve ser algo detectável - algo que querer interação.

[157] Martin Hellman: A cryptanalytic time-memory trade-off. IEEE Trans. on Information Theory, 26(4), pp. 401-406, 1980.

[158] Karsten Nohl: Breaking GSM phone privacy. Black Hat USA 2010. Available on youtube, URL https://www.youtube.com/watch?v=0hjn-BP8nro

[159] N.T.: Trata-se de um algoritmo específico (FF2) para encriptação que preserva o formato (PFE): uma forma de se encriptar dados sem mudar sua representação ou exigir mudança no conjunto de dados que os armazena. Ex: cartões de crédito.

[160] Morris Dworkin, Ray Perlner: Analysis of VAES3 (FF2). Cryptology ePrint Archive Report 2015/306. 2 de abr., 2015. FPE significa Format-Preserving Encryption.

atrás de artigo, quem tem tempo? Acho que devemos respirar, escrever menos artigos e fazer com que tenham mais importância.

- **Observe o valor social dos problemas. Faça pesquisa antivigilância.**

- **Seja introspectivo a respeito do porquê você está trabalhando nos problemas que você se dedica.**

Ao listar direções para pesquisas antivigilância, não incluí o tipo de trabalho, mais comum na literatura das PET (privacy-enhancing technologies), que assume que haverá uma coleta pervasiva de informações e, em seguida, tenta fazer o que se pode para minimizar usos ilegítimos[161]. Como a imoralidade acontece no momento da coleta de dados, o objetivo aqui é tentar amenizar o impacto do mal já feito. Mas é difícil saber como isso se desenrola. Estou preocupado com a chance de que o trabalho caia nas mãos daqueles que procuram base técnica para uma posição que diz, efetivamente, que "a abordagem de 'coletar tudo' é inevitável e problemática apenas temporariamente, já que, uma vez que descobrirmos como resolver tudo isso, será lidado com a privacidade no fim da linha, onde os dados são usados." Mas a própria coleta pervasiva, por si só, retrai a liberdade de expressão e ameaça a democracia liberal, independentemente do que se afirme que acontecerá no fim da linha[162].

[161] Ver, por exemplo, Seny Kamara: Restructuring the NSA metadata program. Financial Cryptography Workshops 2014, pp. 235-247, 2014

[162] Refletindo isso, a Quarta Emenda dos EUA fala não apenas de mandados sendo exigidos unicamente para busca, mas também para apreensão.

**Segurança demonstrável orientada à prática.** Não são apenas os tópicos em que trabalhamos, mas como os executamos que molda a direção do nosso campo. Por quase 25 anos, Mihir Bellare e eu desenvolvemos o que chamamos de segurança demonstrável orientada à prática. Em um ensaio e palestra de 2009[163], eu debati sobre como várias escolhas não necessárias engendraram uma teoria da criptografia que era menos útil do que o necessário. Hoje em dia, eu posso enumerar entre as escolhas históricas importantes: **(1)** uma preferência por análises assintóticas e teoremas e as correspondentes concepções de segurança grosseiras com as quais isso está associado; **(2)** uma preferência pelo minimalismo, esteticamente construído, como ponto de partida para reduções; **(3)** a rejeição de primitivas simétricas e funções finitas como objeto de investigações rigorosas; **(4)** uma tradição de usar linguagem não construtiva para demonstrar resultados; **(5)** a marginalização de mensagens seguras; e **(6)** uma atitude condenatória em relação ao modelo de oráculo aleatório, modelo de permutação aleatória, modelo de cifra ideal, modelos de Dolev-Yao[164], e qualquer outro modelo considerado não padrão.

A segurança demonstrável orientada à prática inverte essas escolhas. Ele mantém o foco da segurança demonstrável em definições e provas, mas estas são entendidas como ferramentas que ganham seu valor principalmente por sua utilidade para a segurança ou privacidade. A abordagem é igualmente adequada nesses dois domínios, mas tem sido subutilizada para problemas de privacidade, como o envio de mensagens seguras.

---

[163] Phillip Rogaway: Practice-oriented provable security and the social construction of cryptography. Manuscript, Maio, 2009, e palestra na Eurocrypt 2009.

[164] Danny Dolev, Andrew C. Yao: On the security of public key protocols. IEEE Trans. on Information Theory, IT-29, pp. 198-208, 1983.

Lidar melhor com redes de mistura e onion routing é um ponto de partida óbvio. É o que eu e alguns alunos estamos fazendo.

### Aplique segurança demonstrável orientada à prática aos problemas antivigilância.

**Financiamento**[165]**.** Nos Estados Unidos, parece que a maior parte do financiamento à criptografia extramural pode agora vir das forças armadas[166]. De 2000 a 2010, menos de 15% dos artigos na CRYPTO que reconhecem o financiamento extramural dos EUA reconheceram o financiamento do (DoD)[167]. Em 2011, esse índice subiu para 25%. De 2012 a 2015, aumentou para 65%[168]. Hoje em dia, muitos criptógrafos montam uma grande colcha de retalhos de financiamento, a maior parte geralmente é do Departamento de Defesa. O reconhecimento de financiamento a seguir não é tão atípico:

> este trabalho foi apoiado pela NSF, pelo programa DARPA ROCEED por um prêmio AFOSR MURI, uma bolsa do ONR, um projeto IARPA fornecido via DoI/NBC e pela Samsung[169].

---

[165] Esta seção trata exclusivamente do financiamento acadêmico da criptografia nos EUA. Eu sei muito pouco sobre o financiamento da criptografia em outros países.

[166] Não consegui encontrar estatística sobre isso.

[167] DoD [no original] = Department of Defense. Isso inclui organizações como AFOSR, IARPA, DARPA, e ONR

[168] Esses dados são baseados em uma contabilidade que eu mesmo fiz, à mão, passando por todos esses processos antigos.

[169] Os acrônimos são para AFOSR = Air Force Office of Scientific Research; DARPA = Defense Advanced Research Projects Agency; DoI/NBC = Department of Interior National Business Center; IARPA = Intelligence Advanced Research Projects Activity; MURI = Multidisciplinary University Research Initiative; NSF = National Science Foundation; ONR = Office of Naval Research; and PROCEED = Programming Computation on Encrypted Data. Após a declaração, vieram outras

O financiamento militar da ciência invariavelmente a redireciona[170] e cria riscos de caráter moral[171]. No entanto, sugerir a alguém que ele(a) reconsidere seu financiamento pelo Departamento de Defesa pode enfurecer até mesmo um colega normalmente tranquilo, pois será encarado como um ataque tanto ao caráter de alguém quanto à sua capacidade de ter sucesso.

Não importa o que as pessoas digam, nossa atividade científica **muda** em detrimento dos objetivos institucionais do patrocinador. Esses objetivos podem não ser seus. Por exemplo, a missão da DARPA é "investir em tecnologias inovadoras que podem criar a próxima geração de recursos de segurança nacional [dos EUA]." Tendo começado na esteira do Sputnik, a agência fala em evitar **surpresas tecnológicas** - criando-as para os adversários dos Estados Unidos.[172] Nos EUA, a NSA assessora outras agências do Departamento de Defesa sobre financiamentos relacionados à criptografia. Pelo menos às vezes, eles aconselham a NSF. Em 1996, a NSA tentou anular meu próprio prêmio NSF CAREER. Aprendi isso com minha ex-gerente de programas da NSF, Dana Latch, que não apenas recusou o pedido da NSA, mas, indignada com isso, me reportou. Um histórico interno da NSA conta sobre o erro cometido por eles que terminou dando origem à concessão de financiamento que levou à RSA.

---

35 palavras de cunho legalista, incluindo uma declaração de que o artigo havia sido liberado "Aprovado para Divulgação Pública." http://eprint.iacr.org/2013/403.pdf [170] Daniel S. Greenberg: Science, Money, and Politics: Political Triumph and Ethical Erosion. University of Chicago Press, 2003

[171] Um risco moral é uma situação em que uma parte obtém os benefícios e outra assume o risco. O termo é comum na economia.

[172] Darati Prabhakar: Understanding DARPA's Mission. http://tinyurl.com/darpamission YouTube version http://tinyurl.com/darpa-mission2

> A NSA havia analisado o pedido [de financiamento] de Rivest, mas o texto era tão geral que a Agência não identificou ameaças e a devolveu à NSF sem comentários. Uma vez que a técnica havia sido financiada conjuntamente pela NSF e pelo Office of Naval Research, o novo diretor da NSA, o almirante Bobby Inman, visitou o diretor da ONR para garantir um compromisso de que a ONR teria a coordenação da NSA em todas as propostas de financiamento futuras.[173]

As pessoas costumam ficar felizes quando conseguem um financiamento, independentemente de sua fonte. Mas eu sugeriria que, se uma agência de financiamento adota valores inconsistentes com os seus, então talvez você não deva aceitar esse dinheiro. nstituições **têm** valores, não menos que as pessoas. Talvez, na era moderna, elas tenham ainda mais.

As grandes organizações têm objetivos múltiplos e, às vezes, conflitantes. As organizações militares com funções ofensivas e defensivas em cibersegurança têm COIs[174] inerentes ao seu design. Estão errados aqueles que presumem que seu trabalho não é militar, financiado erroneamente pelos militares.

Em seu discurso de despedida, em 1961, o presidente Dwight D. Eisenhower apresentou a frase e o conceito de complexo militar-industrial. Em uma versão anterior desse discurso, Eisenhower chamou, de forma bastante sugestiva, de complexo militar-industrial-**acadêmico**[175]. Se os cientistas

---

[173] Tom Johnson: Book III: Retrenchment and Reform, 1998. O livro era confidencial, tornado disponível a partir de um pedido via FOIA [Freedom of Information Act], em http://cryptome.org/0001/nsa-meyer.htm

[174] Nota do Autor.: Acrônimo para Communities of Interest.

[175] Henry A. Giroux: The University in Chains: Confronting the Military-IndustrialAcademic Complex, Routledge, 2007.

desejam reverter nossa cumplicidade nessa convergência de interesses, talvez precisemos nos afastar dessa vala.

Nada disso estava claro para mim quando entrei para a universidade. Há alguns anos, participei de uma proposta de financiamento ao DoD (felizmente, sem sucesso), o que eu não faria hoje em dia. Levei muito tempo para perceber o que acabou se tornando óbvio para mim: que o financiamento que recebemos afeta nossas crenças e se reflete nelas.

No final, um dos principais motivos para que a criptografia-para-privacidade não tenha decolado bem pode ser pelo fato das agências de financiamento poderem não querer ver progresso nessa direção[176], e a maioria das empresas também não quer progresso nesse sentido. Os criptógrafos internalizaram isso. Principalmente, estamos no ramo de ajudar as empresas e o governo a manter as coisas seguras. Governos e empresas tornaram-se nossos "clientes", não um grupo desordenado de ativistas, jornalistas ou dissidentes, e não alguma noção abstrata do povo. A criptografia-para-privacidade vai se sair melhor quando os criptógrafos pararem de receber fundos do DoD e, mais do que isso, começarem a pensar em um estatuto diferente para nossa produção.

**Pense duas vezes - e então uma vez mais - quanto a receber financiamento militar.**[177]

[176] É claro que as pessoas vão apontar o Tor como um anti-exemplo; recebeu financiamento da DARPA, ONR e do Department of State. Não acho que haja muito o que explicar. Toda grande burocracia tem dentro de si direções concorrentes e conflitantes. Alguns segmentos do governo dos EUA podem pensar que o Tor é ótimo, mesmo quando outros gostariam de interromper o financiamento, desmantelá-lo ou subvertê-lo.

[177] Nos Estados Unidos, isso significa AFOSR, ARO, DARPA, IARPA, MURI, NSA, ONR, e outros.

**Tenha em vista pessoas comuns como aqueles(as) cujas necessidades você quer, no fim do dia, atender.**

**Liberdade acadêmica.** Aqueles(as) de nós que são acadêmicos(as) em universidades desfrutam de uma tradição de liberdade acadêmica. Isso se refere ao seu direito - e até mesmo a sua obrigação - de pensar, falar e escrever sobre o que você quiser que esteja ligado ao seu trabalho, mesmo que vá contra a vontade dos poderosos: que esteja ligado ao seu trabalho, mesmo que vá contra a vontade dos poderosos: sua universidade, grandes corporações ou o Estado. Embora a liberdade acadêmica pareça estar em declínio[178], pelo menos por enquanto, ela reconhecidamente persiste. Normalmente, cientistas e outros(as) acadêmicos(as) não exatamente precisam ou lançam mão de sua liberdade acadêmica: tudo o que realmente precisam é de financiamento e habilidades[179]. Mas a criptografia-para-privacidade pode ser um raro tópico onde a liberdade acadêmica **é** útil[180]. Eu sugiro que as pessoas façam uso dessa qualidade. A liberdade acadêmica que não é exercida pode murchar e, então, morrer.

Muitos não acadêmicos também têm algo semelhante à liberdade acadêmica: autonomia suficiente para trabalhar no que eles acham que é importante, sem perder seus empregos, mesmo que não seu empregador não

[178] Frank Donoghue: The Last Professors: The Corporate University and the Fate of the Humanities. Fordham University Press, 2008. Ou veja: The Center for Constitutional Rights and Palestine Legal: The Palestine exception to free speech: a movement under attack in the US. 30 de Set, 2015. https://ccrjustice.org/the-palestine-exception

[179] Lorren R. Graham: Money vs freedom: the Russian contradiction. Humanities, 20(5), Set/Out, 1999

[180] Para uma descrição do incidente envolvendo Matthew Green, veja: Jeff Larson e Justin Elliott: Johns Hopkins and the Case of the Missing NSA Blog Post. ProPublica, Set, 2013. Para uma descrição de um incidente envolvendo Barton Gellman, veja seu artigo: I showed leaked NSA slides at Purdue, so feds demanded the video be destroyed. Ars Technica, Out, 2015. http://tinyurl.com/gellman-at-purdue

exatamente deseje ou goste disso.

## Faça uso da liberdade acadêmica que você tem.

**Contra o dogma.** Acho que muitos criptógrafos fariam bem ao apoiar uma atitude mais aberta em relação a modelos, abordagens e objetivos desconhecidos. O estreitamento disciplinar nos espaços de primeiro nível da criptografia foi pronunciado[181]. Muitas pessoas parecem ter crenças bastante estridentes sobre quais tipos de trabalho são **bons**. Às vezes, beira a tolice, como quando as pessoas se recusam a usar a palavra prova para **provas** no modelo de oráculo aleatório. (Obviamente, uma prova no modelo de oráculo aleatório não é menos uma prova do que uma prova em qualquer outro modelo.)

Como criptógrafos, devemos sempre ser sensíveis - e céticos - sobre a relação entre nossos modelos e as reais definições de privacidade e segurança. Isso não significa que não devemos levar os modelos a sério. Isso significa que deve vê-los como provisórios e dialéticos. Há um aforismo adorável do estatístico George Box, que disse que **todos os modelos estão errados, mas alguns são úteis.**[182]

A criptografia precisa de modelos úteis. Mas a avaliação da utilidade de

[181] Na grande maioria, já não há hardware, já não há abordagens formalistas para a criptografia (a menos que eles reivindiquem uma relaçao com a criptografia "real"), a criptoanálise dos esquemas do mundo real é pouco endereçada e assim por diante.

[182] George E. P. Box: Robustness in the strategy of scientific model building. In: Launer, R. L.; Wilkinson, G. N., Robustness in Statistics, Academic Press, pp. 201-236, 1979. Box não foi o primeiro a expressar esse sentimento. Por exemplo, Georg Rasch explicou, em 1960, que “Quando você constrói um modelo, você deixa de fora todos os detalhes que você, com o conhecimento à sua disposição, considera desnecessários. (...) Os modelos não devem ser verdadeiros, mas é importante que sejam aplicáveis e, se eles são aplicáveis para um determinado propósito, devem ser investigados. Isso também significa que um modelo nunca é aceito definitivamente, é apenas em teste." Georg Rasch: Probabilistic models for some intelligence and attainment tests. Copenhagen: Danmarks Paedogogiske Institut, pp. 37-38, 1960. University of Chicago Press,

um modelo é, em si, problemática. Pedimos definições: o quão limpo é? O quão compreensível? Quão geral? Quais aspectos do ambiente de computação são considerados? O que significa e o que não significa? O esforço de definir recai sobre uma intercessão entre matemática, estética, filosofia, tecnologia e cultura. Situado dessa forma, o dogma é uma doença.

Tem-se afirmado que a missão da criptografia teórica é definir e construir protocolos e esquemas criptográficos demonstravelmente seguros[183]. Mas essa é uma atividade de criptografia teórica, não sua missão. Existem muitas outras atividades. Pode-se trabalhar em modelos e resultados que são completamente rigorosos, mas estão fora da estrutura de segurança demonstrável[184]. Ou pode-se encarar um importante protocolo como consolidado e, em seguida, analisá-lo em qualquer estrutura que funcione melhor. O objetivo do meu próprio trabalho é desenvolver ideias que, espero, contribuam para a construção de sistemas de computação seguros. Na adorável simbologia do jardim de flores de Amit Sahai[185], criptógrafos teóricos podem ser jardineiros, cultivando sementes (suposições de firmeza) para germinar flores (objetivos criptográficos); mas eles também podem fazer muitas outras coisas. O que é uma sorte, já que a prática criptográfica não tem se beneficiado tanto das nossas atividades de horticultura.

**Esteja aberto à diversidade de abordagens. Encare todos os modelos como suspeitos e dialéticos.**

[183] Shafi Goldwasser, Yael Tauman Kalai: Cryptographic assumptions: a position paper. Cryptology ePrint Archive Report 2015/907, 16 de setembro, 2015

[184] Toda a tradição da criptografia na teoria da informação segue essa tendência.

[185] Amit Sahai: Obfuscation II. Talk at the Simons Institute. Maio, 2015. Disponível em https://simons.berkeley.edu/talks/amit-sahai-2015-05-19b

**Uma visão mais expansiva.** Eu encorajaria criptógrafos - especialmente os(as) jovens de nossa área - para tentar alimentar uma visão a nível sistemático do que está acontecendo quando a criptografia é utilizada. Você precisa de uma visão muito melhor das coisas do que um tecnófobo como eu jamais terá.

Lembro-me de ler aquele artigo de 2012 de Dan Boneh e colaboradores, **O Código Mais Perigoso do Mundo**[186], e de me sentir pequeno pelo fato de que havia todo esse universo de códigos - esse **middlewares** - que eu nem sabia que **existia**, mas que poderia – e que frequentemente acontecia - anular a criptografia que estava ali. Quando as revelações da NSA levaram as pessoas a especular sobre como a criptografia da Internet estava sendo derrotada, ocorreu-me que talvez a NSA não precisasse de nenhuma criptoanálise superinteligente - o que eles precisavam, acima de tudo, era comprar exploits e contratar pessoas com uma visão do ecossistema de computação a nível sistemático.

Uma abordagem que pode ser útil para obter uma boa vantagem é ter uma visão das coisas centrada em APIs[187]. Não apenas as questões mal compreendidas de APIs são um comum problema de segurança, mas as lacunas entre as formalizações criptográficas e as APIs podem produzir sérios problemas criptográficos[188]. E em uma direção construtiva, a noção de online-AE, por exemplo[189], efetivamente flui de uma visão centrada em APIs. APIs e a

---

[186] Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, Vitaly Shmatikov: The most dangerous code in the world: validating SSL certificates in nonbrowser software. ACM Conference on Computer and Communications Security, pp. 38-49, 2012

[187] API significa application programming interface, a interface construída entre componentes de código.

[188] Serge Vaudenay: Security flaws induced by CBC padding: applications to SSL, IPSEC, WTLS..., Eurocrypt 2002.

[189] Viet Tung Hoang, Reza Reyhanitabar, Phillip Rogaway, Damian Vizár: Online authenticated-

criptografia “séria” precisam de laços mais estreitos.

As comunidades de pesquisa têm uma tendência geral de se voltarem para dentro. Como uma comunidade, temos buscado nos comprometermos seriamente com algoritmos e com a teoria da complexidade, mas temos feito pouco na busca por pesquisas em privacidade, linguagens de programação ou no direito. Teremos um papel social maior se aumentarmos nossas conexões com os vizinhos.

Recentemente, vi uma boa palestra de Chris Soghoian em que ele descreveu sua frustração ao tentar fazer com que a mídia cobrisse - ou que qualquer outra pessoa se importasse - o amplamente conhecido fato (que na verdade não é bem conhecido) de que conversas por telefone celular não têm, essencialmente, qualquer privacidade.[190] Os criptógrafos deveriam estar ajudando com tais comunicações. Mas eu me pergunto sobre o quanto nós prestamos atenção. Para a maioria de nós, se não é no que se está trabalhando, realmente não há importância. Não se tem tempo.

**Tenha uma visão a nível sistemático. Lide com aquilo que tangencia nossa área.**

encryption and its nonce-reuse misuse-resistance. Crypto 2015, vol. 1, pp. 493-517, 2015. Guido Bertoni, Joan Daemen, Micha¨el Peeters, Gilles Van Assche: Duplexing the sponge: single-pass authenticated encryption and other applications. Selected Areas in Cryptography 2011, pp. 320-337, 2011

[190] Chris Soghoian, Workshop on Surveillance and Technology (SAT 2015), Drexel University, 29 de junho, 2015. Ver também: Chris Soghoian: How to avoid surveillance... with your phone. TED talk. https://www.youtube.com/watch?v=ni4FV5zL6lM. Stephanie K. Pell e Christopher Soghoian: Your secret Stingray’s no secret anymore: the vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy. Harvard Journal of Law and Technology, 28(1), Fall 2014.

**Aprenda sobre ferramentas de privacidade.** Eu gostaria de gentilmente sugerir que nós, criptógrafos, faríamos bem em aprender e usar as ferramentas contemporâneas de privacidade. Poucos de nós usam ferramentas como OTR, PGP, Signal, Tails e Tor. É meio constrangedor - e eu suspeito que nosso trabalho coletivo sofre por isso. Christopher Soghoian observa bem isso: "É como se toda a comunidade médica acadêmica fumasse 20 cigarros por dia, usasse drogas na veia com agulhas compartilhadas e fizesse sexo desprotegido com parceiros aleatórios regularmente."[191]

Devo ser uma pessoa bizarra para defender isso - é definitivamente o caso do sujo falando do mal lavado. Pessoalmente não tenho interesse em usar tecnologias e vou ser incompetente se eu for tentar. Eu nem tenho um smartphone. Ainda assim, suspeito que não haja nada como a experiência para motivar os criptógrafos a identificar e resolver os problemas de privacidade que nos ajudarão a transformar ferramentas de nerds, difíceis de usar, em mecanismos transparentemente incorporados às massas. O primeiro problema que sugeri na Seção 4 é algo em que pensei alguns dias depois de começar a usar o Pond.

### Aprenda sobre ferramentas de privacidade. Use-as. Melhore-as.

**Sem adversários simpáticos.** Existe uma longa tradição de "simpatia" em nosso campo. As pessoas contam histórias divertidas e fantásticas. Os participantes

[191] Christopher Soghoian, comunicações pessoais, Nov. 2015.

do protocolo são uma caricatura de Alice e Bob. Os adversários são pequenos demônios, com direito a chifres e um tridente. Algumas conversas criptográficas são tão recheadas de arte que você mal consegue encontrar o conteúdo. Nunca gostei disso, mas, depois das revelações de Snowden, começou a me irritar como nunca antes.

A criptografia é algo sério, com ideias geralmente difíceis de entender. Quando tentamos explicá-las com desenhos e narrativas engraçadas, não acho que tornamos nossas contribuições mais fáceis de entender. O que realmente fazemos é adicionar uma camada de ofuscação que deve ser removida para que seja entendido o que realmente foi feito. Pior ainda, a criptografia com muitos desenhos animados pode remodelar nossa visão interna de nosso papel. O adversário enquanto um complexo de vigilância industrial-militar de US$53 bilhões por ano e o adversário enquanto um demônio vermelho com chifres induzem processos de pensamento totalmente diferentes. Encarando o adversário de uma dessas maneiras, realmente vemos um conjunto diferente de problemas para se trabalhar se comparado ao outro. Adversários extravagantes geram um campo de estudos quimérico.[192]

Quando eu era um estudante de graduação, queria que nosso campo fosse fantástico. Eu queria uma disciplina cheia de alienígenas e milionários que se comunicavam. Não apenas foi divertido, mas também alimentou meu ego, efetivamente incorporando o sentimento: Eu sou um cientista inteligente demais para ter que lidar com preocupações mesquinhas.

[192] Apesar de todos esses comentários, acho que seria incrível uma graphic novel sobre criptografia. Algo como o trabalho de Keith Aoki e James Boyle: Bound By Law: Tales from the Public Domain, 2006.

A essa altura, acho que faríamos bem em nos colocar na mente de um adversário real, não um adversário imaginário: a agência de inteligência bem financiada, a multinacional obcecada por lucros, o cartel de drogas. Você tem um orçamento gigante. Você controla muitas infraestruturas. Você tem equipes de advogados mais do que dispostos a interpretar a lei de forma criativa. Você tem um portfólio enorme de zero-days[193]. Você tem uma montanha de convicções arrogantes. Seu objetivo é Coletar Tudo, Explorar Tudo, Saber Tudo[194]. O que o frustraria? Que problemas você não quer que um bando de acadêmicos superinteligentes resolva?

### Pare com ilustrações fantasiosas. Leve os adversários a sério.

**Um commons criptográfico.** Muitas pessoas veem a Internet como uma espécie de commons magnífico. Isso é uma fantasia. Existem alguns bens comuns de sucesso na Internet: a Wikipedia, o movimento do software livre, o Creative Commons, OpenSSL, Tor e muitos outros. Mas a maioria das pessoas recorre quase exclusivamente a serviços mediados por um punhado de corporações que fornecem, por exemplo, e-mail, envio de mensagens instantâneas, e armazenamento e computação em nuvem. E eles fornecem o hardware no qual todas essas coisas estão.

Precisamos erguer um bem comum muito mais amplo na Internet. Precisamos realizar serviços populares de forma segura, distribuída e

[193] Exploits que ninguém mais sabe sobre sua existência.

[194] A frase é de alguns slides da NSA revelados por Snowden. Re-impresso na p. 97 de Glenn

descentralizada, movida por softwares e hardwares livres/abertos. Precisamos construir sistemas além do alcance de grandes empresas e de agências de espionagem. Esses serviços devem ser baseados em criptografia forte. pré-requisito, precisamos expandir nossos recursos **criptográficos comuns.**

Os sonhos de tal bem comum remontam aos cypherpunks, que construíram remailers, por exemplo, como um serviço comunitário para permitir comunicações seguras. Mais recentemente, Feigenbaum e Koenig articulam essa visão[195]. Depois de explicar que os serviços em nuvem centralizados desempenham um papel central em tornar possível a vigilância em massa, eles defendem um esforço de base para desenvolver novos serviços em nuvem em escala global baseados em ferramentas de configuração e gerenciamento de código aberto e descentralizadas.

Podemos começar modestos, fazendo nossa parte para melhorar os commons que temos: a Wikipedia. Pode se tornar uma tarefa de rotina em conferências e workshops do IACR, ou na reunião de Dagstuhl, para que pessoas se reúnam por uma tarde ou noite para escrever, revisar e verificar páginas selecionadas da Wikipedia sobre criptografia. É o tipo de esforço que valerá a pena de múltiplas e invisíveis maneiras.

### Projete e construa bens comuns criptográficos que sejam amplamente úteis.

**Comunicações.** No caminhar de nosso campo, noções bem definidas sempre foram importantes. Basta pensar no conhecimento

[195] Joan Feigenbaum, Jérémie Koenig: On the feasibility of a technological response to the surveillance morass. Security Protocols Workshop 2014, pp. 239-252, 2014

zero [zero-knowledge] (e no termo concorrente revelação mínima de inforamação [minimal-disclosure]) para lembrar como uma bela frase pode ajudar a catapultar uma bela ideia à notoriedade. Da mesma forma, a frase de seis letras "33 bits" faz um trabalho notavelmente bom em incorporar um conceito importante sem passar perto de um vocabulário contestado[196]. Tanto na criptografia quanto na privacidade, a linguagem é formativa e substancial.

A palavra **privacidade**, com seu significado abstrato e debatido, suas conotações frequentemente negativas, não é uma palavra atraente. Privacidade é para registros médicos, toalete e sexo - não para a liberdade ou democracia. A palavra **anonimato** é ainda pior: a linguagem política moderna pintou isso quase como uma conotação de terrorismo. **Segurança** é uma palavra mais atraente e, na verdade, falei de mensagens seguras em vez de mensagens privadas ou anônimas porque acho que captura melhor o que quero transmitir: que uma comunicação cujas partes são relevadas não é, absolutamente, segura. Uma pessoa se sentirá insegura caso utilize esse canal.

Mas mesmo a palavra segurança não enquadra bem nosso problema: devemos tentar falar em impedir a vigilância em massa mais do que em aumentar a privacidade, o anonimato ou a segurança. Conforme dito antes, sabemos instintivamente que a vigilância onipresente é incompatível com a liberdade, a democracia e os direitos humanos[197]. Isso torna a vigilância uma

[196] O valor se refere, é claro, ao número de bits necessários para identificar um ser humano. Ver o website de Arvind Narayanan, 33bits.org.

[197] Para uma exposição brilhante dessa ideia, ver Eben Moglen: Privacy under attack: the NSA files revealed new threats to democracy. The Guardian, Maio, 2014. O artigo é derivado de uma palestra em quatro partes: Eben Moglen: Snowden and the future, delivered 9 e 30 de outubro, 4 e 13 de novembro, 2013, Columbia Law School. http://snowdenandthefuture.info/

coisa contra a qual se pode lutar. Câmeras de vigilância e data centers tornam mais visual nossa distopia emergente, enquanto a privacidade, o anonimato e a segurança são tão abstratos que quase desafiam a representação visual.

Concretamente, pesquisas que visam minar a vigilância podem ser chamadas de pesquisas de antivigilância[198]. As ferramentas para esse fim seriam as tecnologias antivigilância[199]. E a escolha dos problemas com os quais se trabalha com base em uma visão ética pode ser chamada de pesquisa baseada em consciência.

### Escolha bem a linguagem. A comunicação é fundamental para se ter um impacto.

**Valores institucionais.** Este ensaio pode parecer dar ênfase no peso da ética nas escolhas pessoais e profissionais de cada cientista. Mas, na verdade, estou mais preocupado com a forma como nós, enquanto criptógrafos e cientistas da computação, agimos em conjunto. Nosso comportamento coletivo incorpora valores - e as instituições que criamos também.

Não pretendo criticar nenhum indivíduo em particular. As pessoas devem e vão trabalhar naquilo que consideram de maior valor. O problema ocorre quando nossa comunidade, como um todo, desvaloriza sistematicamente a utilidade ou o valor social. Então temos um fracasso coletivo. O fracasso não recai sobre ninguém em particular, mas recai sobre todos.

**Conclusão de tudo.** Muitos, antes de mim, discutiram a importância da ética, da

[198] Essa sugestão, assim como a pesquisa baseada em consciência, são de Ron Rivst.

[199] Embora o termo já esteja em uso, o termo mais comum é privacy-enhencing technologies.

da cultura disciplinar e do contexto político em moldar o que fazemos. Por exemplo, Neal Koblitz afirma que, em 1981, as bases da conferência CRYPTO foram, em si, um ato de provocação. Ele alerta para o potencial de corrupção que o financiamento pode desempenhar. E ele conclui seu próprio ensaio com uma afirmação de que o drama e o conflito são inerentes à criptografia, mas que isso também contribui para a instigar o campo[200]. Susan Landau nos lembra que a privacidade vai muito além da engenharia, do direito, da economia e assim em diante. Ela nos lembra que minimizar a coleta de dados faz parte do Código de Ética e Conduta Profissional da ACM[201].

Como cientistas da computação e criptógrafos, somos duplamente culpados quando se trata de vigilância em massa: a ciência da computação criou as tecnologias que fundamentam nossa infraestrutura de comunicação - e que agora está sendo transformada em um aparelho de vigilância e controle; enquanto isso, a criptografia contém em si o potencial, subutilizado, para ajudar a redirecionar esta trágica virada[202].

Escritores, cineastas, futuristas e cientistas estabeleceram muitas visões concorrentes para a morte do ser humano. Por exemplo, Bill Joy se preocupa com a nanotecnologia transformando a biosfera em uma gosma cinza, ou robôs superinteligentes decidindo que o homem é um incômodo ou um animal de estimação[203]. Não perco o sono com essas possibilidades. Não as vejo como o

[200] Neal Koblitz: The uneasy relationship between mathematics and cryptography. Notices of the AMS, 54(8), pp. 972-979, Setembro de 2007.[198] Essa sugestão, assim como a pesquisa baseada em consciência, são de Ron Rivst.

[201] Susan Landau: Privacy and security: a multidimensional problem. Communications of the ACM, 51(11), Novembro de 2008

[202] É claro que nós, criptógrafos, não somos os únicos nesse meio. Pessoas que trabalham com “data science" e “big data" estão especialmente envolvidas.

[203] Bill Joy: Why the future doesn’t need us. Wired, 8.04. Abril de 2000.

nosso fim provável. Mas uma vigilância rastejante, que cresce organicamente nos setores público e privado, que se torna cada vez mais abrangente, entrelaçada e preditiva, que se torna um instrumento de assassinato, controle político e manutenção do poder - bom, essa visão não somente parece ser possível, mas parece acontecer diante dos nossos olhos.

Eu não sou otimista. A figura do criptógrafo heroico chegando para salvar o mundo da vigilância totalitária é ridícula[204]. E em um mundo onde agências de inteligência armazenam e exploram incontáveis vulnerabilidades, obtêm chaves privadas de autoridades certificadoras, subvertem mecanismos de atualização de software, infiltram-se em empresas privadas com espiões, redirecionam discussões online em direções favoráveis e exercem enorme influência sobre órgãos de padronização, a criptografia, por si só, será uma resposta ineficaz. Na melhor das hipóteses, a criptografia pode ser uma ferramenta para criar possibilidades dentro de contornos circunscritos por outras forças.

Mesmo assim, ainda há motivos para sorrir. Um bilhão de usuários estão recebendo mensagens instantâneas encriptadas usando o WhatsApp e seu protocolo Axolotl[205]. Dois milhões de usuários se conectam usando o Tor todos os dias[206]. Artigos sobre criptografia inspirados nas revelações de Snowden estão começando a aparecer rapidamente. Mais de 50 pesquisadores de criptografia e segurança dos EUA assinaram uma carta aberta que co-organizei, condenando

[204] Dito isso, há um drama considerável nas experiências de pessoas como Julian Assange, William Binney, William Davidon, Tom Drake, Daniel Ellsberg, Mark Klein, Annie Machon, Chelsea Manning, Laura Poitras, Jesselyn Radack, Diane Roark, Aaron Swartz, Edward Snowden, e J. Kirk Wiebe.

[205] Moxie Marlinspike e Trevor Perrin: The TextSecure Ratchet (webpage). 26 e novembro de 2013. https://whispersystems.org/blog/advanced-ratcheting/. Numero de usuários disponível em http://www.statista.com/statistics/260819/number-ofmonthly-active-whatsapp-users/

[206] Dados de https://metrics.torproject.org/userstats-relay-country.html, 01-11-2014 a 29-11-2015.

a vigilância de toda sociedade[207]. A publicação **Keys Under Doormats**[208], de 15 autores, é uma tentativa explícita de fazer com que a experiência criptográfica contribua com a formulação de políticas.

E não é que a criptografia-para-privacidade seja algo novo ou que perdeu o valor em nossa comunidade. Criptógrafos como Ross Anderson, Dan Bernstein, Matt Blaze, David Chaum, Joan Feigenbaum, Matt Green, Nadia Heninger, Tanja Lange, Arjen Lenstra, Kenny Paterson, Ron Rivest, Adi Shamir, Nigel Smart e Moti Yung, para citar apenas alguns, têm lidado com a privacidade voltada para a prática muito antes dela começar a ser popular (se é que isso está acontecendo). A conferência RWC (Real World Cryptography) está criando uma nova e saudável gama de participantes.

Palestras, workshops e painéis de discussão sobre vigilância em massa estão ajudando os criptógrafos a perceber que lidar com a vigilância em massa é um problema inerente à nossa disciplina. Bart Preneel e Adi Shamir têm dado palestras intituladas Post-Snowden Cryptography e houve painéis de discussão com este título no Eurocrypt 2014 e na RSA-CT 2015.

Artigos estão surgindo com títulos como “Cryptographers have an ethics problem."[209] Quando um ataque ao Tor por pesquisadores do CMU foi

---

[207] Uma carta aberta de pesquisadores em criptografia e segurança da informação. 24 de janeiro de 2014. http://masssurveillance.info/.

[208] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D. J. Weitzner: Keys under doormats: mandating insecurity by requiring government access to all data and communications (2015). Disponível em http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf. 2015. Um report de antes: H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier: The risks of key recovery, key escrow, and trusted third-party encryption (1997). Disponivel em http://academiccommons.columbia.edu/catalog/ac:127127.

[209] Antonio Regalado: Cryptographers have an ethics problem. MIT Technology Review. 13 de setembro, 2013. John Bohannon: Breach of trust. Science Magazine, 347(6221), 13 de janeiro, 2015.

supostamente usado para fornecer dados anônimos em massa para o FBI, o CMU e os pesquisadores envolvidos foram publicamente vaiados[210]. O próprio IACR tem se tornado mais vocal, tanto com a Resolução de Copenhague[211] quanto com a declaração sobre a Defence Trade Controls Act, da Austrália[212].

Embora nossa comunidade tenha abraçado a criptografia-para-privacidade menos do que eu gostaria, essa tem sido uma questão cultural - e a cultura pode mudar.

Eu ouvi dizer que se você acha que a criptografia é a sua solução, você não entende o seu problema[213]. Se essa sacada for verdade, então nosso campo teve um sério desvio. Mas podemos corrigir isso. Precisamos fazer da criptografia a solução para o problema: “como tornar a vigilância mais custosa?"
Dan Bernstein fala sobre uma **criptografia interessante** e uma **criptografia enfadonha**. Criptografia interessante é a criptografia que suporta muitos trabalhos acadêmicos. Criptografia enfadonha é “criptografia que simplesmente funciona, resiste a ataques com eficiência e nunca precisa de atualizações." Dan pergunta, em seu jeito tipicamente irreverente:

> O que acontecerá se os usuários de criptografia convencerem alguns

[210] Tor security advisory: “relay early" traffic confirmation attack. 30 de julho, 2014. http://tinyurl.com/tor-attack1. Tor project blog: Did the FBI pay a university to attack Tor users? 11 de novembro, 2015. http://tinyurl.com/tor-attack2. Esse artigo inclui “Qualquer que seja a pesquisa acadêmica em segurança no século 21, certamente não inclui "experimentos" pagos que colocam indiscriminadamente estranhos sem seu conhecimento ou consentimento.” Ver também reações como: Joe Papp: The attempt by CMU experts to unmask Tor project software was appalling. Pittsburgh Post-Gazette. 5 de agosto, 2014. http://tinyurl.com/papp-letter.

[211] A declaração, adotada em 14 de maio de 2014 em uma reunião de negócios em Copenhague, na Dinamarca, diz: A filiação ao IACR repudia a vigilância em massa e o enfraquecimento das soluções e padrões criptográficos. A vigilância em toda a população ameaça a democracia e a dignidade humana. Solicitamos o avanço de pesquisas e implantação de técnicas eficazes para proteger a privacidade pessoal contra o alcance governamental e corporativo. https://www.iacr.org/misc/statement-May2014.html

[212] Ver https://www.iacr.org/petitions/australia-dtca/

> pesquisadores de criptografia a criar uma criptografia enfadonha? Não haveria mais ataques no mundo real. Não haveria mais atualizações de emergência. Um público limitado para quaisquer breves melhorias contra ataques e para uma substituição de criptografia. Esta é uma ameaça existencial contra futuras pesquisas criptográficas.[214]

Se esta é uma criptografia enfadonha, precisamos de um pouco dela.

A criptografia-cypherpunk foi descrita como "crypto with an attitude."[215] Mas é muito mais do que isso, pois, mais do que qualquer outra coisa, o que os cypherpunks queriam era uma criptografia com valores. E valores, profundamente sentidos e profundamente inerentes ao nosso trabalho, é o que a comunidade criptográfica mais precisa. E talvez uma dose daquela verve cypherpunk.[216]

Já foi dito que só porque você não se interessa por política, isso não significa que a política não vai se interessar por você[217]. Dado que a criptografia é uma ferramenta para redistribuir o poder, as pessoas que conhecem bem o assunto, gostemos ou não, herdam um pouco desse poder. Como criptógrafo, você pode ignorar essa paisagem de poder e todas as dimensões políticas e morais de nosso campo. Mas isso não fará elas irem embora. Isso apenas tornará seu trabalho menos relevante ou socialmente útil.

---

[214] Dan Bernstein: Boring crypto. Talk at SPACE 2015. Malaviya National Institute of Technology, Jaipur. Slides e audio em http://cr.yp.to/talks.htm

[215] Steven Levy: Crypto rebels. Wired, 01 de fevereiro, 1993

[216] John Perry Barlow: A declaration of the independence of cyberspace. Fev, 1996. Eric Hughes: A cypherpunk's manifesto. Março, 1993. Timothy May: The Cyphernomicon. Setembro, 1994. Aaron Swartz: Guerilla open access manifesto. Julho de 2008.

[217] Barry Popik aponta que a citação "foi atribuída ao líder grego Péricles (495-429 a.C.), mas apenas desde o final dos anos 1990. A fonte grega nunca é identificada nas frequentes citações. A citação parece ser de origem moderna." Verbete em blog, 22 de junho, 2011. http://tinyurl.com/not-pericles

Minha esperança para este ensaio é que você internalize esse fato e o reconheça, como o ponto de partida, para o desenvolvimento de uma visão eticamente orientada no que você deseja realizar com seu trabalho científico.

Comecei este ensaio falando do manifesto Russell-Einstein, então deixe-me terminar por aí também, com o apelo de Joseph Rotblat em seu discurso de aceitação do prêmio Nobel:

> Em uma época em que a ciência desempenha um papel tão poderoso na vida da sociedade, quando o destino de toda a humanidade pode depender dos resultados da pesquisa científica, é responsabilidade de todos os cientistas estarem plenamente conscientes desse papel e se comportarem de acordo. Apelo aos meus colegas cientistas para que se lembrem de sua responsabilidade para com a humanidade.[218]

[218] Joseph Rotblat: Remember Your Humanity. Discurso de aceitação do Nobel, 1995. Disponivel em Nobelprize.org

# Agradecimentos

Primeiramente, meus agradecimentos a Mihir Bellare pelas inúmeras discussões sobre o tema deste ensaio. Durante anos, não apenas colaboramos estreitamente em questões técnicas, mas também discutimos muito sobre os valores e sensibilidades implicitamente intrínsecos ao trabalho criptográfico. Sem Mihir, não apenas teria feito muito menos tecnicamente, mas também teria entendido muito menos quem são os criptógrafos.

Ron Rivest não apenas forneceu comentários úteis, mas tem estado muito em minha mente enquanto eu agonizava com este ensaio. Muitas outras pessoas me deram sugestões e ideias importantes. Gostaria de agradecer a Jake Appelbaum, Ross Anderson, Tom Berson, Dan Boneh, David Chaum, Joan Feigenbaum, Pooya Farshim, Seda Gürses, Tanja Lange, Chip Martel, Stephen Mason, Chanathip Namprempre, Ilya Mironov, Chris Patton, Charles Raab, Tom Ristenpart, Amit Sahai, Rylan Schaeffer, Adi Shamir, Jessica Malekos Smith, Christopher Soghoian, Richard Stallman, Colleen Swanson, Björn Tackmann, Helen Thom, Jesse Walker, Jacob Weber e Yusi (James) Zhang por seus comentários, discussões e correções.

Weber e Yusi (James) Zhang por seus comentários, discussões e correções.

Minha visão do que é ciência e o que o cientista deve ser foi fortemente moldada por assistir Jacob Bronowski quando eu era criança [219].

Todo o trabalho técnico original mencionado neste ensaio (por exemplo, o que é descrito nas primeiras páginas da Parte 4) foi apoiado pela NSF Grant CNS 1228828. Mas eu enfatizo que todas as opiniões, descobertas, conclusões e recomendações neste ensaio (e este ensaio é composto, sobretudo, de opiniões e recomendações) refletem apenas as opiniões do autor, não necessariamente as opiniões da National Science Foundation.

Agradeço à equipe de Schloss Dagstuhl e aos participantes do workshop 14401, Privacy and Security in an Age of Surveillance, onde ideias relacionadas a este ensaio foram discutidas.[220]

Parte do trabalho neste ensaio foi feito enquanto eu era professor convidado na ENS, em Paris, recebido por David Pointcheval.

Meus agradecimentos ao Conselho do IACR pelo privilégio de ministrar a Distinguished Lecture do IACR deste ano. É uma honra que acontece no máximo uma vez na carreira de um criptógrafo - e tentei o meu melhor para fazer uso dessa oportunidade com sabedoria. sabedoria.

Este ensaio deve sua existência à coragem de Edward Snowden.

[219] Jacob Bronowski: The Ascent of Man. TV series. BBC and Time-Life Films, 1973.

[220] Bart Preneel, Phillip Rogaway, Mark D. Ryan, e Peter Y. A. Ryan: Privacy and security in an age of surveillance (Dagstuhl perspectives workshop 14401). Dagstuhl Manifestos, 5(1), pp. 25-37, 2015.

IP.rec

INSTITUTO DE PESQUISA EM
DIREITO & TECNOLOGIA DO RECIFE