A PRIVACIDADE E A CRIPTOGRAFIA NA CONTEMPORANEIDADE

Eduardo Felipe Silvestre de Castro[*]

A privacidade é um aspecto criado para reger relações, interações e conexões que mantém uma enorme teia que engloba um número de pessoas. Comum e evidente durante o século XVIII como uma necessidade de manter uma imagem das famílias a ser passada para o meio externo, compreendendo então um conjunto de maneiras capazes manter apenas um grupo ou mesmo uma única pessoa ciente de determinados fatos, ou qualquer outro tipo de conhecimento que mereça sigilo para as visões estabelecidas na época.

No que abrange a contemporaneidade, o momento presente, que se dá de um passado próximo onde está a adesão à tecnologia nas relações sistemáticas que farão funcionar todo um *corpus* da civilização, até um momento futuro indeterminado, onde estarão os conceitos modificados no transcurso da informação segura. Construiremos um discurso sobre a importância da privacidade na história do presente, e no que abrange uma dinâmica do cotidiano.

Na atualidade a privacidade tem suas expressões em fatores que desenham a conexão entre duas pessoas, duas instituições ou mais. As relações de logística são as mais fortes candidatas ao posto de campeãs no que diz respeito à manutenção da privacidade, pois, o guardar de informações nesse campo é tão intenso e importante que gerou uma *revolução* na área da tecnologia e da matemática durante as décadas de 60 e 70, propiciando o início das intercomunicações seguras via internet. No segundo posto: os campos bélico-científicos que inusitadamente deram origem a um novo segmento das conexões entre computadores, permitindo a troca secreta de informação e de funções, conhecida como ARPANET[1], a *mãe* da World Wide Web, e por fim as relações pessoais, que movimentam grande parte do que conhecemos hoje como redes de telefonia e internet. Mas como se dá essa privacidade?

Durante um longo tempo, foi-se preciso enviar mensageiros com valises trancadas e algemadas ao braço, mensagens por telégrafo cifradas[2] em Código Morse, entre outras estratégias

---

[*] Aluno do I semestre do Curso de História (Licenciatura e Bacharelado) da Universidade Federal de Campina Grande

[1] ARPA: corresponde a Advanced Research Projects Área trata-se de uma organização de pesquisas de ponta Agência de Projetos Avançados de Pesquisa, financiada pela Agência de Segurança Nacional (NSA – National Security Agency).

[2] Cifradas – Cifra: Qualquer sistema em geral para esconder o significado de uma mensagem substituindo cada letra da mensagem original por outra letra o sistema deve ter uma flexibilidade de tradução embutida, conhecida como chave.

de comunicação segura. Quando, na década de 1960, o computador se torna mais acessível, temos a adesão deste equipamento em empresas, que o utilizarão na cifragem de informações importantes. Quando a cifragem é interna dentro de uma única empresa a criptografia é relativamente suficiente para manutenção de segredos, mas quando surge a necessidade de enviar essas informações a outras empresas? Como faremos? Para que entre duas empresas haja essa comunicação é preciso que a instituição que cifra a mensagem envie para a receptora uma chave do código. Mas como fazer isso? É aí que entram os homens como valises trancadas, os mensageiros, entre outros, e esse tipo de comunicação exige uma mudança periódica da cifra e da chave, e uma redistribuição das chaves para os receptores. Mas esse fluxo é perigoso, causa um grande risco de interceptação da chave, e uma posterior descoberta do conteúdo das mensagens e por fim o comprometimento das relações. Então como enviar a chave? Por telefone? A linha pode estar grampeada, e a chave descoberta por uma empresa ou exército adversário. Poderíamos então mandar a chave também cifrada, mas como o receptor a decifraria? Teria de haver uma segunda chave. Os problemas são infinitos, e até 1960 eram os grandes dilemas da cientificidade no mundo das comunicações[3].

Em 1973 o trio de criptógrafos de Stanford: Whitifield Diffie, Martin Hellman e Ralph Merkley conseguiram inventar um sistema que facilitaria tudo. A criptografia de chave pública, que seria complementada pelo sistema matemático RSA[4] de Ronald Rivest, Adi Shamir e Leonard Adleman. O sistema consistia na — em termos que são suficientes para defini-lo — publicação do modo como a informação foi cifrada, porém é deixado em sigilo o modo de decifra-la. Mais especificamente, o sistema é assimétrico, ou seja, o modo de cifra-lo não é o mesmo para decifrá-lo, logo qualquer um pode cifrar um texto, mas só quem possui a segunda chave é capaz de compreender a mensagem. Desta forma, tudo se resume em uma pequena metáfora: Suponhamos que Alice, Bob e Eva são pessoas distintas, se Alice quer mandar uma mensagem cifrada para Bob, ela procurará pela chave pública de Bob, previamente publicada por ele, e cifrará um texto, e então o enviará, como Bob ao elaborar sua chave pública, que cifra o

[3] Comunicação: Aqui entendido como transmissão de informação. A filosofia da comunicação compreende, entre outras, as seguintes questões: determinar se a comunicação é essencial ao pensamento, se devemos nos contentar e tornar as palavras como meros veículos de pensamentos e idéias independentes delas, e determinar o que distingue sistemas de comunicação rudimentares , como aqueles que os animais podem possuir, de uma linguagem totalmente dotada de significado."

[4] RSA provém de Rivest, Shamir e Adleman, o trio que tornou possível matematicamente o uso da criptografia de chave pública, através de funções da geometria modular, conseguiram criar funções assimétricas que deram o principio para sistemas informacionais de hoje como o de compras via internet. A operação matemática irreversível torna o RSA a forma de cifra mais poderosa até agora.

texto, também elaborou uma chave particular, que decifra o texto, a mensagem enviada por Alice não pode ser lida por Eva, já que ela não tinha a chave particular de Bob para decifrar a mensagem, que é diferente da usada por Alice, que serve apenas para cifrar o texto. Assim a informação chega a Bob em segurança que irá lê-la. Foram seis homens, especialistas, em um período de 1974 a 1977 para que essa estória virasse realidade no campo informacional.

Essa última estória será a responsável pelo fluxo de informação de proporções colossais no qual vivemos hoje, conhecida com a Era da Informação. Quando fazemos compras pela internet, na verdade apenas ciframos nossos dados de cartão de crédito em uma chave pública da empresa da qual compramos algo, a mensagem chega à empresa que decifra tudo com sua chave particular, e em breve recebemos nosso produto em casa. As empresas e bancos fazem isso entre si, quando enviam por cabos de fibra-ótica procurações correspondentes a capital de investimento convertidos em uma infinidade de números para filiais em outros lugares do planeta. Mas o que torna essas operações de grande segurança são as possibilidades de a decifragem ser frustrada, na verdade quanto maior o número de possibilidades de arranjos numéricos que traduzem uma informação, menores são as chances de que uma pessoa não autorizada leia o conteúdo informativo. Sendo assim, quanto maiores forem as possibilidades de combinações numéricas, reorganizações dos elementos do texto seguindo um algoritmo, menores são as chances de decifragem sem o prévio conhecimento da chave. Mas isso não é impossível de se fazer. Os melhores softwares de cifragem que estabelecessem um poderoso sistema de comunicações estão nos Estados Unidos da América, e uma vez que a legislação americana inclui programas de cifragem no mesmo parâmetro de armamento bélico, ao lado de metralhadoras, mísseis, tanques de guerra e armas nucleares, não é permitido sobre qualquer hipótese a exportação de tais produtos. Nesse contexto, o pouco que chegou ao público fora dos EUA é trilhões de vezes menos seguro do que qualquer sistema norte-americano, deixando-nos anos-luz atrás de algumas instituições, e, como na Era da Informação em que vivemos o conhecimento se torna cada vez mais valioso, governos e suas divisões de segurança se digladiam em um cenário de alta tecnologia e vigilância informacional. Esse cenário pode ser bem definido na fala de Phil Zimmermann[5], alguém que está diretamente envolvido com essa batalha:

[5] - Phil Zimmermann é, na história da tecnologia, o responsável pela elaboração e difusão do software PGP, que permite o uso da cifra RSA por pessoas comuns, a mais poderosa do mundo, sem maneiras de ser quebrada até agora. O PGP bloqueia todos os grandes sistemas de interceptação de informação que constituem o cenário do Grande Irmão, causando a desespero das divisões de segurança dos governos, Phil foi alvo de uma investigação minuciosa de

> A criptografia costumava ser uma ciência obscura, de pouca importância para a vida diária. Historicamente ela sempre teve um papel especial nas comunicações militares e diplomáticas. Mas na Era da Informação, a criptografia está relacionada como o poder político, e em especial com a relação de poder entre o governo e povo. Ela se liga ao direito à privacidade, liberdade de expressão, liberdade de associação política, liberdade de imprensa, liberdade contra a busca e apreensão absurda e a liberdade de ficar sozinho. [...] Um futuro governo pode herdar uma infra-estrutura tecnológica otimizada para a vigilância, onde ele poderá vigiar os movimentos de seus opositores políticos, todas as transações financeiras, todas as comunicações, cada e-mail, cada chamada telefônica. Tudo poderia ser filtrado e escaneado, identificando automaticamente pela tecnologia de reconhecimento de voz e transcrito.
>
> [ZIMMERMANN, 2001: 322-323][6]

Após esse pronunciamento de Zimmermann temos a noção de constante vigilância, e de que nossas informações pessoais podem estar sendo interceptadas e depositadas em um enorme banco de dados mundial. Esse cenário, batizado de o Grande Irmão, que gerou livros, filmes e até um reality show, na verdade é bem mais sério. Divisões governamentais como a NSA, responsável por sondar os inimigos do país, a Agência de Segurança Nacional opera em uma enorme rede de escutas, grampos telefônicos, interceptações digitais, observações via satélite, e ainda em parceria com outros países como Grã-Bretanha, Canadá, Nova Zelândia e Austrália, que formam um sistema de observação com um raio de alcance capaz de cobrir todo o globo. O maior centro de espionagem — que nos faz relembrar a guerra fria — está em Yorkshire; a Base de Sinais de Informação de Menwith Hill, local que utiliza o sistema Echlon de espionagem. O Echlon é capaz de detectar palavras chaves em vários meios de comunicação, e-mails, telefonemas, qualquer um que seja interceptável, trabalhando com palavras-chave como "Hezbollah", "Hamaz", "Bush", "assassinato" e "Casa Branca", o sistema é capaz de selecionar inúmeras mensagens que passam por uma re-seleção de palavras, e uma outra, até cair finalmente na última instância que será uma análise posterior do texto propriamente dito. E ainda é capaz de direcionar suas interceptações para um determinado grupo político ou região, no contexto atual, podemos imaginar que o campeão é o Oriente Médio, e os grupos políticos são, provavelmente, facções terroristas. Ora, tendo em vista o ambiente conflitante que o EUA está inserido, e que sempre esteve, desde políticas como o Big Stick que é um plano de estratégias de intervenção na política de outros países que propiciaram guerras com países como Vietnã, Somália e Iraque, é

---

espionagem e tráfico de material bélico de 1993 até 1999. Sendo um dos maiores ativistas de que a criptografia atinja as camadas populares , argumentando o direito à privacidade de todos.

[6] ZIMMERMANN, Phil *apud* SINGH, Simon. *O Livro dos Códigos*. Tradução de Jorge Calife. Rio de Janeiro: Record, 2001.

fácil perceber um fluxo constante de ataques entre esses dois eixos de pensamento, dos quais, um é os EUA o outro são seus adversários. Aparentemente esses eixos colocaram o mundo em uma segunda bipolarização depois do que compreendemos por Guerra-Fria, porém, desta vez os pólos se distinguem em compreensões étnico-religiosas, análogo ao que entendemos por um período pós-Segunda Guerra até 1989, uma vez que nesta última já havia um embate entre interceptadores de informação e criptográfos. Embate que se compara a uma balança que ora oscila para qualquer um dos lados, baseada plenamente em desenvolvimento tecnológico.

Cercados nessa atmosfera de espionagem, temos casos clássicos da política americana, como as acusações de uso indevido de escutas telefônicas por presidentes como Lyndon Johnson, Richard Nixon e John F. Kennedy, ou ainda o caso Martin Luther King Jr. que teve a linha telefônica grampeada durante vários anos, resultando na reunião de várias informações sobre sua vida pessoal pelo FBI que as usou para desacreditar King frente a seus ouvintes políticos.

Não há como responder todas as perguntas acerca das transições da criptografia, existem inúmeros debates legislativos, e até em fóruns na rede mundial de computadores sobre este assunto e ainda não chegamos a uma conclusão. A intenção real desse artigo não é definir parâmetros, paradigmas, axiomas ou teorias, mas, levantar hipóteses, e hipóteses no sentido expresso por Russell:

> Uma hipótese explica enquanto salva as aparências e prediz o futuro. Se não é, em si, inexplicada. Quando, por sua vez, requer ser salva, não mais explica, mas sim de ser explicada em função de alguma outra hipótese que agora permanece inexplicada. Isto não é misterioso. Não se pode explicar tudo de uma só vez.
>
> [RUSSELL, 2002: 417][7]

Hipóteses que podem ou não ser descartadas, uma vez que surgem outras capazes de suplantar as previamente levantadas de acordo com a necessidade da cientificidade no momento. Como não podemos explicar, nem descrever tudo sobre a privacidade e a criptografia na contemporaneidade, e tentar fazê-lo seria um retorno claro ao Positivismo do séc. XIX, afinal, teríamos de negar todas as explicações que rodeiam e influenciam os fatos, já que não são plenamente conhecidos devido as práticas de sigilo das instituições de criptografia, e nos mantermos apenas em definições e descrições que estão muito ligados a corrente filosófica de Comte. É preferível que nos mantenhamos em breves fatos e especulações analíticas. A

[7] - RUSSELL, Bertrand: "O Período Contemporâneo" (pp. 411-449). In *História do Pensamento Ocidental*: A aventura dos pré-socráticos a Wittgenstein. Tradução de Laura Alves e Aurélio Rebello – Rio de Janeiro: Ediouro. 2002.

criptografia é uma ciência secreta, e se assim for fica aqui a necessidade de fontes históricas, de documentos, de análises mais aprofundadas da parte dos historiadores, ver e compreender o que é secreto estabelece a necessidade de olhar a criptografia em várias perspectivas, de pensar e especular sobre a presença de lacunas na história dessa ciência em todos os seus aspectos, não há como fazer um apanhado de seus acontecimentos e registra-los de forma fidedigna, afinal, é provável que a maioria dos fatos que no transcurso do tempo deixaram marcas claras na história dessa ciência estejam sob os cuidados de instituições que guardam de maneira ávida os seus segredos, mas não quer dizer que seja uma história incompleta ou falha, já passamos por uma revolução histórica que nos permite hoje ir além de fontes escritas, e mais, nos dá cabimento a fazer uso de nossa percepção, mesmo com os comentários daqueles que fazem parte do meio científico da criptografia que esclarecem o contrário como James Ellis[8]:

> A criptografia é uma ciência fora do comum. A maioria dos cientistas profissionais tenta estar entre os primeiros a publicar seu trabalho, porque é através da disseminação deste trabalho que ele se valoriza. Em contraste, a criptografia terá mais valor se for realizada com o mínimo de informação disponível para os adversários em potencial. Assim, os criptográfos profissionais normalmente trabalham em comunidades fechadas para fornecer suficiente interação profissional, e garantir a qualidade, enquanto se mantém o segredo para as pessoas de fora. A revelação desses segredos normalmente só é autorizada no interesse da precisão histórica, depois de se ter demonstrado que nenhum benefício será obtido com a manutenção do sigilo.
>
> [ELLIS, 2001: 318][9]

Assim trabalhar com história da criptografia se torna um tanto difícil, uma vez que os possuidores de fontes mais atualizadas não pretendem libera-las tão cedo, e desta maneira nossos anacronismos, e discrepâncias quanto à história da criptografia só são perceptíveis às pessoas que não estão autorizadas a revelar esse conhecimento. Cabe aqui pensarmos que a história não pode colocar-se capaz de perceber todas as coisas em seu discurso pós-Annalles, Lucien Febvre pode ter postulado:

> Toda uma parte, e sem dúvida a mais apaixonante do nosso trabalho de historiadores, não consistirá num esforço constante para fazer falar as coisas mudas, para fazê-las dizer o que elas por si próprias não dizem sobre os homens, sobre as sociedades que as produziram, e para constituir, finalmente, entre elas

[8] - James Ellis é criptográfo do GCHQ (General Comunications Head-Quarter), a divisão de segurança nacional da Grã-Bretanha, na história da criptografia teria inventou a criptografia de chave pública antes de Whitifield Diffie, Martin Hellman e Ralph Merkley, porém, por motivos de sigilo o GCHQ não permitiu a publicação de seu trabalho, que viria a conhecimento popular somente muito depois do patenteamento da chave pública pelo trio de Stanford.

[9] ELLIS, James *apud* SINGH, Simon. O Livro dos Códigos. tradução de Jorge Calife — Rio de Janeiro: Record. 2002.

> aquela vasta rede de solidariedade e de entreajuda que supre a ausência do documento escrito?
>
> [FEBVRE, 1953: 428][10]

Mas tomar isso como capaz de submeter todos os campos a serem estudados pelos domínios de Clio, seria um retorno ao Hegelianismo, um desejo idealista, tão inócuo à cientificidade do ponto de vista filosófico contemporâneo. Porém para relacionar criptografia e privacidade existe essa necessidade de fazer falar as coisas mudas mesmo ficando difícil negarmos um aspecto presente na Teoria da História de Certeau: "Desde então veio o tempo da desconfiança. Mostrou-se que toda interpretação histórica depende de um sistema de referência: que este sistema permanece uma 'filosofia' implícita particular: que se infiltrando no trabalho de análise, organizando-o á sua revelia, remete à 'subjetividade' do autor."[11]

Como uma boa gama de informação, de fatos pitorescos que historiadores medievalistas chamariam de *anecdotes*, fica difícil não se deixar levar pela imaginação dentro da história da criptografia, mas nos detenhamos as discussões de como ela tem atuado em nossas vidas.

"Sorria, você está sendo filmado!" Aí está mais um indício da atmosfera do Grande Irmão na qual vivemos, grande parte do nosso sistema de telefonia ainda está no formato analógico, que permite uma interceptação muito mais fácil, talvez até seja mais interessante esse sistema que a fibra ótica para repartições do governo brasileiro como a Polícia Federal e a Abin, todavia, capturar informações de pessoas comuns tem ficado cada vez mais fácil para interceptadores, o uso do e-mail é só um aspecto pequeno. Outro jovem estudante de Stanford, Orkut Bouykkuten, fez um grande favor criando um enorme banco de dados especificando inúmeras caracteríticas de cada membro de seu site de relacionamentos, como ele, através dos perfis, ou das comunidades do membro temos todo acesso ao cotidiano de uma pessoa, local de trabalho ou estudo, estado civil, bairro, cidade, e até outras informações mais triviais como marca de celular ou se o membro já subiu ou não no vão da porta. Fotologs, blogs, virtual life, entre outros sites e softwares espalhados pela rede, demonstram o que parece ser uma vontade de abster-se da privacidade, ou voltando-se para a mídia televisiva, inscrições para o Big Brother, podem ser relacionadas com o desejo de ser visto, observado e até controlado por um entidade maior.

---

[10] FEBVRE, Lucien apud LE GOFF, Jacques. "Documento/Monumento"(pp. 535-553). In *História e Memória*. Campinas, SP: Editora da UNICAMP, 1992.

[11] - CERTEAU, Michel de. "Operação Historiográfica" (pp. 65-109). In *A Escrita da História*. tradução de Mª de Lourdes Menezes — Rio de Janeiro: Forense Universitária: 2007.

Mas enquanto pessoas toleram e atém caminham atreladas a extinção da privacidade, é travado um gigantesco debate em torno desse direito. Pessoas no mundo inteiro discutem com seus respectivos governos a necessidade de pessoas físicas terem o direito a cifragem RSA, no formato PGP[12], tão complexas, tão difusas são essas formas de cifra que os governos temem perder o controle sobre o fluxo da informação. A Comission Nationale de Contrôle de Interceptions de Securité estima que na França apenas ela faz cerca de 100.000 escutas ilegais todos os anos, um abuso ao nosso direito de nos manter distanciados do mundo, do nosso direito de estarmos sozinhos.

Mas algo que pode nos deixar estarrecidos é esse e-mail, enviado a Phil Zimmermann em 1991, no dia em Boris Yeltisin bombardeava o Parlamento Russo, depoimento que nos dá uma noção de como a criptografia age no percurso da história: "Phil, eu quero que você saiba. Espero que isso nunca aconteça, mas se a ditadura dominar a Rússia, o seu PGP já está instalado espalhado pelo Báltico ao Extremo Oriente e vai ajudar os democratas, se for necessário. Obrigado!"[13] Parece que uma privacidade civil completa daria campo à uma atuação política militante maior?

O PGP é o baluarte da batalha dos que são a favor da privacidade contra o Grande Irmão, o Echlon e contra os governos. Mas vale salientar que mensagens cifradas por completo e de forma não interceptável, dão oportunidade não só a privacidade, mas também a pessoas mal intencionadas chamados no debate como os Quatro Cavaleiros do Infocalipse[14]: traficantes de drogas, crime organizado, terroristas e pedófilos, que são os maiores usuários da rede mundial de computadores para organização de suas ações. Isso pode causar um aumento da impunidade, e por conseqüência desses crimes digitais. Hipoteticamente falando nos deixa expostos a ação deliberada contra a lei nos meios de informação , o que pode acarretar em uma "terra de ninguém", onde a influência da lei não é capaz de chegar. Por fim, podemos concluir que O Grande Irmão apesar de nos privar de nossa privacidade, nos mantém seguros, por outro a frase de Descartes toma uma nova forma na contemporaneidade: "Penso, logo a NSA já sabe!"

---

[12] PGP é a sigla para Pretty for Good Privacy: Uma Ótima Privacidade. O software PGP usa da sigla RSA em formato capaz de ser processado por um computador comum, liberado na rede desde de junho de 1991, o PGP é alvo de grandes discussões sobre a manutenção da privacidade e sobre o uso dele por criminosos.

[13] *apud* SINGH, Simon. "Uma Ótima Privacidade" in *O Livro dos Códigos*. Tradução de Jorge Calife – Rio de Janeiro: Record. 2002.

[14] Infocalipse é um termo meramente jornalístico sensacionalista usado no debate entre ativistas da liberdade do uso da criptografia e dos Governos que acreditam que a segurança se aplica através do conhecimento de toda informação circulante.

Bibliografia:

BLACKBURN, Simon; Dicionário Oxford de Filosofia; tradução de Desidério Murcho – Rio de Janeiro: Jorge Zahar. 1997.

CERTEAU, Michel de; A Escrita da História; tradução de Mª de Lourdes Menezes; — 2ª edição . Rio de Janeiro; Forense Universitária, 2007.

JABINET, Marie Paule Caire-. Introdução à Historiografia. Tradução de Laureano Pelegrin – Bauru: SP: EDUSC, 2003.

LE GOFF, Jacques. História e Memória. Tradução de Bernardo Leitão et Alii. — Campinas, SP: Editora da UNICAMP, 1994.

RUSSELL, Bertrand. História do Pensamento Ocidental. A aventura das idéias dos Pré-Socráticos a Wittgenstein. Tradução de Laura Alves e Aurélio Rebello — Rio de Janeiro: Ediouro, 2002.

SINGH, Simon. O Livro dos Códigos. Tradução de Jorge Calife — Rio de Janeiro: Record, 2001.

Sites Consultados:

http://www.nai.com/products/security/phil/phil.asp

http://www.pgpi.com/