Segurança da Informação

Márcio Moretto Ribeiro

9 de Agosto de 2017

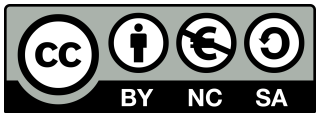
Apresentação

Essas são notas de aula da disciplina Segurança da Informação ministrados no segundo semestre de 2017 para as turmas do período diurno e noturno do curso de Sistemas de Informação da Escola de Artes Ciências e Humanidades (EACH) da USP. A primeira versão desta apostila foi escrita para o curso de verão ministrado entre os os dias 2 e 6 de fevereiro de 2015 também no campus leste da Universidade de São Paulo. O curso de verão foi oferecido como parte das atividades do projeto de Privacidade e Vigilância do Grupo de Políticas Públicas em Acesso à Informação (GPoPAI) e foi inspirado pelo curso online oferecido gratuitamente pela plataforma Coursera e ministrado pelo professor D. Boneh.

Aos alunos que pretendem se aprofundar no tema sugerimos as seguintes referências bibliográficas:

- J. Katz e Y. Lindell - *Introduction to Modern Cryptography*
- W. Stallings - *Criptografia e Segurança da Informação*
- C. Paar e J. Pelzl - *Understanding Cryptography*

Agradecemos aos alunos que participaram do curso de verão em 2015 e dos cursos de gradução em 2016 e 2017, suas contribuião serviram de importante feedback para escrita dessas notas.



Capítulo 1

Introdução

1.1 Privacidade

As primeiras tentativas de conceitualizar a privacidade datam do final do século XIX. Em um famoso artigo de 1890, os colegas da faculdade de direito de Bosto, Louis Brandeis e Samuel Warren denunciam que o advento da fotografia instantânea e o jornalismo haviam "invadido o recinto sagrado da vida privada" ferindo o que eles apontam como o direito individual de "ser deixado em paz". Assim, eles argumentam que o escopo do direito comun (*Common Law*), que originalmente se concentrava apenas na proteção contra agreções e já havia sido ampliado para incluir a proteção à propriedade deveria ser novamente alargado para finalmente reconhecer a "natureza espiritual do homem" [].

Essa visão da privacidade como proteção à intimidade ou, nas palavras dos autores, como o "direito de ser deixado em paz" é a chave de interpretação que prevalece no debate público. Duas contribuições que não fogem a esse espírito, porém, merecem destaque nessas notas introdutórias. Em um influente artigo de 1977, Richard Posner propõe que as disputas sobre direito à privacidade sejam interpretadas em sua dimensão econômica. Para Posner, as informações privadas possuem valor. De um lado há o interesse de quem busca construir uma imagem pública sobre si, uma reputação e, de outro, há o interesse de se conhecer o outro para melhor saber como se relacionar com ele ou aprender sobre sua trajetória. Caso fosse permitido qualquer tipo de intrusão à privacidade, o efeito seria um esforço maior em não revelar, ou inclusive não produzir, dados potencialmente valiosos. Assim, a questão

da privacidade, se resumiria a uma questão de eficiência econômica. Caberia ao legislador regular o direito ao controle da reputação procurando um equilíbrio que maximizasse os fluxos de informação [].

O risco tanto para o indivíduo cuja paz é perturbada pelas fotos não autorizadas, quanto para aquele que perde o controle sobre sua reputação é de que algo que pertencia a sua esfera privada se tornasse pública. Para Nissenbaum, essa dicotomização entre público e privado não dá conta dos problemas associados a quebra de privacidade. Por exemplo, um paciente espera que as informações sobre sua condição de saúde sejam eventualmente compartilhadas com outros médicos ou médicas com o intuito de melhor diagnosticá-lo, assim como um cliente espera que seu gerente de banco use suas informações bancárias para sugerir-lhe melhores investimentos. Porém, há uma flagrante quebra de privacidade se as informações médicas forem compartilhadas com o banco, com quem eventualmente o paciente negociará um plano de saúde. Esse cenário exemplifica o que a autora chama de rompimento da "integridade contextual do fluxo de informações" [].

1.2 Vigilância

Associado ao tema da privacidade, mas ligado a outra matriz teórica, estão os debates sobre vigilância. Diferente dos estudos sobre privacidade cujos principais autores são juristas preocupados com o direito individual, os esttudos sobre vigilância focam em relações de poder. Foucault descreve a vigilância como uma técnica que teria alterado profundamente as formas de exercer o poder durante os séculos XVII e XIX. O poder do senhor feudal durante a idade média era exercído por meio do suplício, a pena corporal em que o açoitado pedia misericórdia eventualmente concedida. Após a revolução francesa o suplício foi sendo substituido pela prisão e aos poucos seria desenvolvida a técnica da disciplina e da vigilância. Para o autor, a imagem que melhor descreve a técnica é uma estrutura arquitetônica proposta por Jeremy Bentham no final do século XVII. Bentham arquitetou um modelo de prisão em que os vigias ficariam no centro aonde poderiam observar todas as celas, porém, aqueles que ocupam as celas não poderiam observar o vigia. A sensação constante de estar sendo vigiado introgetaria a disciplina, outra técnica deste período, nos condenados. O propósito da vigilância e da disciplina é o de produzir corpos dóceis e obedientes [].

Em 1992, em um curto texto, Giles Deleuze propos uma atualização dos

conceitos de Foucault que anteciparam o que hoje compreendemos como vigilância. Na sociedade disciplinar, descrita por Foucault, durante a vida o indivíduos passa de uma instituição disciplinar a outra: da escola, ao exército, do exército à fábrica e da fábrica ao hospital. Cada instituição disciplina o indivíduo e o modela da maneira mais eficiente à instituição. Na sociedade do controle, conforme descrita por Deleuze, o poder é exercido de maneira mais intermitente e mais sutil. O indivíduo prototípico da sociedade do controle seria o endividado cujo controle atravessa as instituições [].

1.3 Marco Regulatório

Antes ainda dos primeiros computadores, as chamadas máquinas Hollerith revolucioram a capacidade de processamento de dados. Durante a década de trinta elas dinamizaram o processamento dos dados do censo nos EUA e na década de 40 foram usadas pelos nazistas para classificar aqueles, principalmente judeus, mas também comunistas e homossexuais, que deveriam ser transportados para os guetos, dos guetos para os campos de concentração e finalmente para as câmaras de gás []. Finda a guerra, a evolução dos modernos Estados de bem estar social Europeu e seu necessário processamento massivo de dados casou muito bem com o desenvolvimento computacional e assustou os cidadãos com sua centralidade de processamento. Assim, começaram a surgir as primeiras leis de proteção de dados pessoais.

Mayer-Schonberger argumenta que, uma vez que as leis de proteção de dados pessoais na Europa partem todas das mesmas bases e diferem apenas em detalhes, é mais frutífero estudá-las em conjunto do que seguindo uma análise comparativa. Ele propõe uma abordagem geracional como se existisse uma tendência evolutiva das normas. A primeira geração, no começo dos anos 70, focou na regulamentação técnica dessas bases centralizadas de dados. O surgimento de mini-computadores, que favorecia o processamento descentralizado, levou a uma adaptação na legislação. A segunda geração, no final dos anos 70, focou na liberdade negativa, o direito civíl de "ser deixado em paz"nas palavras de Brandeis e Warren. A autonomia do indivíduo é, porém, contraposta a sua inclusão nos programas sociais do Estado. Então, a terceira geração legislativa, em meados dos anos 80, foge um pouco das liberdades negativas e foca em uma abordagem participativa de autodeterminação informacional. A pergunta deixa de ser se alguém quer participar ou não de processos sociais, mas como. Ainda assim, porém, os indivíduos

estavam em uma posição frágil nas relações de negociação o que os levava, via de regra, a abdicar dos seus direitos. A quarta geração, de meados dos ano 90, procurou de um lado equalizar as posições de negociação ainda apostando na autonomia do indivíduo, mas também incluiu diversos mecanismos mais paternalistas excluindo certas liberdades participativas e as sujeitando à proteção juridica obrigatória. Nessa fase surgem órgãos de defesa, não apenas de auxílio aos cidadãos, mas com papel decisório para delibera contra violações [].

No Brasil, o Marco Civil da Internet aprovado em 2013 não aborda diretamente as questões de proteção de dados pessoais. Carecemos de um marco legal que imponha, pelo menos, que o uso de dados pessoas dependa necessariamente do consentimento explicito e informado. Além disso, a autorização dos dados pessoais deve ser dada para um fim específico.

1.4 Vigilância Digital em Massa

Em 2013 Edward Snowden revelou ao mundo o alacance dos programas de vigilância em massas das agências de espionagem dos EUA. O jornalista Glen Greenwald e a cineasta Laura Poitras divulgaram o caso em uma serie de matérias e um documentário []. O vazamento demonstra que a agência de segurança nacional dos EUA (NSA) tem acesso a toda a comunicação por telefone e pelos principais meios de comunicação online do mundo. O moderno modelo de negócios das empresas de internet baseado na propaganda direcionada depende da construção de perfis digitais que por sua vez dependem da produção e aquisição de uma grande escala dados pessoas. Essa competição por dados pessoais cria o que chamamos de pontos únicos de falha. A violação dessas bases permitiu à NSA produzir um banco de dados pesquisável da agência possui toda comunicação pública e privada que passa pelos servidores da Google, do Facebook, da Microsof e da Apple.

A vigilância digital em massa eleva o problema da privacidade para um outro patamar. Não se trata apenas de proteger a intimidade, ou a inviolabilidade do lar, ou do controle na construção da reputação. Nesse contexto, o problema da privacidade é também coletivo. A privacidade deve ser também enchergada como um direito civil, uma limitação ao poder do estado de antecipar as ações de grupos políticos. Para tanto, é preciso de ação politica de concientização, de regulamentação para restringir o poder das empresas que controlam o armazenamento dos dados pessoais e também desnvolvimento

técnico.

1.5 Segurança da Informação

A internet é um meio intrinsecamente promíscuo []. Por uma decisão de projeto, não temos controle por onde nossas informações passam quando nos comunicamos pela rede. Conforme produzimos mais informações pessoais e permitimos que elas circulem, maior o risco de quebra da integridade dos fluxos contextuais. Em particular há atores poderosos com capacidade conhecida de observar a comunicação em escala global o que traz um risco coletivo tanto à soberania nacional dos países periférCos, como o Brasil, quanto à democracia. A regulamentação, absolutamente necessaria para controlar minimamente esses processos e garantir pelo menos o consentimento no uso de nossas informações pessoais, certamente não é suficiente. A compreensão, o desenvolvimento e a difusão de ferramentas de segurança da informação podem colaborar nesse sentido. Concluiremos o capítulo com uma história motivadora.

Após as denúncias de Snowden houve uma espécie de consenso nos meios ativistas sobre a importância de focar forças em desenvolver ferramentas que garantissem a criptografia ponta a ponta. O paradigma mais comum de comunicação na rede é criptografar a comunicação entre cada cliente e o servidor. Como já dissemos, conforme poucos servidores consentram a maior parte da comunicaçõ online, a informação armazenada nesses servidores passa a ser um bem muito requisitado. A ideia para superar isso seria criptografar a comunicação entre clientes. Assim, a informação armazenada nos servidores não seria compreensível seja pelos engenheiros das empresa que controla a comunicação, seja para um ator externo como um hacker ou a NSA. O principal protocolo de criptografia ponta a ponta na época era o PGP, que havia sido criado no começo da década de 90, antes do advento da web. As tentativas mal sucedidas de ressucitar o protocolo logo foram substituídas por um esforço em atualizá-lo. Duas aplicações que garantiam criptografia ponta a ponta em celulares se popularizaram nesse período: Telegram e o Textsecure. A primeira foi desenvolvida por uma compania russa e oferece serviço de criptografia ponta a ponta em comunicação síncrona usando um protocolo desenvolvido por seus engenheiros. A segunda foi desenvolvida por uma pequena empresa no Vale do Silício e se inspirou no protocolo OTR, que por sua vez se inspirou no PGP, adaptando-o para o contexto assíncrono mais

adequado para a comunicação móvel. Os esforços de ativistas em promover esse tipo de ferramenta culminou com a adoção do protocolo do Textsecure, rebatizado como Signal, no Whatsapp, a ferramenta de comunicação móvel mais usada no mundo todo. A popularização da criptografia ponta a ponta em grande parte da comunicação interpessoal muda muito o cenário de proteção de direitos civis e de liberdade de organização. É certo que os metadados das comunicações - quem fala com quem, quando e de onde - não estão protegidos, é certo que a maior parte da comunicação interpessoal não está livre de intrusão seja de hackers, seja de agências governamentais, é certo que há serviços - como agenda online - em que simplesmente não há alternativa segura e, portanto, é necessaria muita ação política e desenvolvimento técnico nessa área.