

A DEEP WEB E OS ARQUIVOS DIGITAS: ACESSIBILIDADE, USO E LEGITIMIDADE

Tainá de Sousa Santos (Universidade Federal do
Estado do Rio de Janeiro)

Patrick Dourado Ribeiro (Universidade Federal Rio de Janeiro)

1 INTRODUÇÃO

O artigo tem como objetivo analisar de que forma podemos fazer uso da *Deep Web* e dos documentos digitais encontrados nesse ambiente buscando fornecer acessibilidade e refletindo sobre a natureza e veracidade dessas informações. Tal preocupação se deu graças o papel globalizador que a internet vem ganhando através do século XXI e como espaços como a *Deep Web* e as redes que a compõem figuram em discursos sobre o direito e liberdade da informação. Tais reflexões misturam-se com o espaço que a arquivologia vem galgando em fornecer informação ao cidadão, garantindo seu direito e cidadania, mas também buscando maneiras de avaliá-la como autêntica e confiável.

Para a realização desse trabalho foi realizada revisão bibliográfica em cima do material selecionado e testes de acesso aos sites e redes selecionados. A cerca da *Deep Web* fez-se necessário utilizar produções como matérias de revistas e jornais, documentários, relatórios dentre outros. A fim de delimitar melhor o corpus documental desse trabalho foi decidido restringir o mesmo visto que a *Deep Web* é extensa e impossível de ser mapeada pela tecnologia atual. Para a realização deste trabalho utilizou-se apenas a rede *.Onion*, onde foram realizados os testes de acesso. Os dados coletados foram comparados

com o conteúdo do levantamento bibliográfico e então analisados a fim de retirarmos conclusões sobre o tema.

Para a análise usamos o modelo fornecido pelo Projeto Interpares (2007) que, com auxílio da Diplomática buscam destacar que os aspectos analisados são adaptações dos conceitos dos documentos analógicos e resultantes do estreitamento da Arquivologia com a Diplomática. E notar se os repositórios digitais onde tais documentos se encontram parecem amparados sobre as especificações de sua estrutura e dos metadados necessários para garantir a preservação e acesso aos materiais (CONARQ, 2015).

2 PARADIGMAS E MUDANÇAS

A revolução tecnológica da comunicação ampliou em massa a capacidade de produção, acumulação e veiculação de dados e informação. Innarelli (2011) destaca que, para todos os efeitos a informação, o conhecimento e a cultura que eram transmitidos ao longo do tempo através dos meios de comunicação evoluíram mediante a necessidade humana e o alvorecer de novas tecnologias.

Com o alvorecer do novo contexto tecnológico devemos considerar as mudanças de paradigmas da informação que serviram como importantes fatores. No fazer arquivístico há o surgimento do Documento Digital que ainda levanta debates na arquivologia devido a sua natureza dinâmica e que foge dos princípios dos quais a arquivologia sempre esteve debruçada: a teoria das três idades e o ciclo de vida dos documentos (FILHO, 2016).

Os avanços tecnológicos e o aumento das necessidades administrativas, jurídicas e científicas, proporcionaram o crescimento da documentação gerada nos dias atuais, o que afeta a Arquivologia (BELLOTTO, 2006). Essas mudanças, unidas a maiores demandas de acesso à informação e conteúdos distintos proporcionaram a popularização por formatos digitais.

Rondinelli (2013) caracteriza documento arquivístico digital como o documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por um sistema computacional. Este é constituído de suporte e componentes digitais, registrado em cadeias de bits que contêm dados de forma, de conteúdo e de composição do documento digital.

Santos e Flores (2015) identificam que esses documentos digitais necessitam de tratamentos especiais para que sejam asseguradas sua autenticidade e confiabilidade. Estas características poderiam ser atestadas através de repositórios digitais e o registro de metadados, que seriam capazes de garantir que o documento eletrônico ou digital não se transforme apenas em

informação e mantenha a sua fidedignidade, assegurando seu valor probatório legal.

Trazendo a questão para os documentos analógicos, encontramos na Diplomática ferramentas para estabelecer a confiabilidade e autenticidade de documentos. Junto desta, há também políticas públicas e estratégias de conservação que suprem as necessidades desse meio. Duranti (1994) diz que os documentos são imparciais no que diz respeito à criação, autênticos em relação aos procedimentos, e inter-relacionados no que tange ao conteúdo. Graças a essas características que atestam seu valor, os registros documentais são capazes de satisfazer os requisitos legislativos sobre seu valor probatório, logo constituem a melhor forma, não só de prova documental, mas de prova em geral.

Rondinelli (2013) destaca que a diplomática pode oferecer subsídios necessários para essas análises. A associação entre Diplomática e Arquivologia pode ser a resposta para um melhor gerenciamento dos documentos arquivísticos modernos, sobretudo os digitais. Apesar da diplomática ver os documentos arquivísticos como entidades individuais e a Arquivologia vê-los como agregações, o trabalho em conjunto das duas áreas pode ser visto como um caminho seguro para o gerencialmente arquivístico de documentos, inclusive os digitais (DURANTI; MACIEL, 1996 apud RONDINELLI, 2013).

Nos documentos arquivísticos digitais são analisados certos aspectos diplomáticos, estes atestam sua autenticidade e a posteriori ajudam a estabelecer estratégias de preservação cabíveis. Contudo, analisar o repositório digital e se este é confiável também auxilia na manutenção da autenticidade do próprio documento.

Flores e Santos (2016), destacam que os aspectos analisados são adaptações dos conceitos dos documentos analógicos e resultantes do estreitamento da Arquivologia com a Diplomática.

Os primeiros aspectos, Forma Fixa e Conteúdo Estável, são "características fundamentais para comprovação da integridade, autenticidade e fidedignidade dos documentos, atingindo os requisitos de confiabilidade (FLORES, SANTOS, 2016, p.71)".

De forma resumida, "um documento digital de forma fixa e conteúdo estável mantém a apresentação na tela do computador mesmo que mude de formato (RONDINELLI, 2013 apud FLORES, SANTOS, 2016). Sua forma fixa assegura a mesma aparência e apresentação sempre que for recuperado (INTERPARES, 2007b).

O conteúdo estável, contudo, diz respeito ao documento que torna a informação e conteúdo contidos nele imutáveis, não sendo possível alterá-los

ou produzir novas versões que não estejam justificadas e registradas dentro dos parâmetros cabíveis (INTERPARES, 2007b).

Essas duas características juntas configuram a fixidez. Portanto, o documento arquivístico digital mantém a apresentação, tal qual, este princípio de fixidez se encontra no conceito de documento arquivístico de maneira implícita e explícita, no âmbito da Arquivologia ou da Diplomática. (RONDINELLI, 2013 apud FLORES, SANTOS, 2016).

O outro aspecto analisado é se o documento digital é estático, ou seja, se estabelece certo grau de interação do usuário com a informação. Os documentos digitais podem ser dos mais diferentes formatos e extensões. Um documento digital estático possui um grau de interação limitado o qual não oferece grandes riscos a sua fixidez (FLORES, SANTOS, 2016).

A análise diplomática, porém, não irá se constituir de apenas um dos elementos para garantir a autenticidade e confiabilidade desses documentos. É importante salientarmos não só o seu uso, mas ele combinado com outras estratégias e ferramentas. Pensar em preservação digital, implica em refletir sobre políticas de preservação específicas para esse meio, uma vez que dada a sua composição diferenciada, os documentos digitais estão sujeitos a diversas questões, técnicas e teóricas, que acabam dificultando a ação de preservá-los.

Em relação aos repositórios digitais Flores (2017) destaca que deve ser desenvolvido segundo o modelo do *Open Archival Information System* (OAIS). O modelo OAIS define a estrutura de um repositório e a norma OAIS descreve as funções de um repositório e os metadados necessários para garantir a preservação e o acesso aos materiais, criando, portanto, um modelo funcional e informacional (CONARQ, 2015). Ele é considerado uma estratégia a longos prazos, cujas vantagens são as possibilidades de definir o plano de preservação, por exemplo, escolha de formatos disponibilizados e conversões para outros.

Contudo, devemos salientar que nenhuma dessas medidas isoladamente é capaz de suprir as necessidades de segurança de uma política de preservação competente. O que garantiria as características necessárias para uma preservação e acesso coerentes é a junção de políticas e recursos tecnológicos, juntos de estratégias de preservação. O repositório digital, será uma ferramenta e garantir que seja confiável em um ambiente seguro é garantir longa vida a essa documentação. A preservação dos documentos arquivísticos digitais, durante as 3 fases, deve ser fundamentada no uso de um repositório arquivístico digital confiável (CONARQ, 2015).

Para além destas discussões, outro ponto a ser abordado é a capacidade de criar, acumular, armazenar e comunicar dos documentos digitais exercem. Estas características relacionam-se diretamente com o direito ao acesso à

informação. A Lei Federal nº. 12.527/2011 - Lei de Acesso à Informação -, regula o acesso à informação, integrando uma política nacional de arquivos de forma consciente. Para a arquivologia, ela auxilia na elaboração e desenvolvimento de metodologias que garantam a produção, utilização, guarda e o acesso aos documentos de arquivo, como forma de garantir o direito constitucional de acesso à informação em detrimento à política que outrora estava alicerçada no segredo e no silêncio (FIDELIS, FERREIRA, DIAS, 2017). Contudo a legislação brasileira sobre os documentos digitais, seu acesso e sobre a internet em si, ainda está sendo aperfeiçoada.

3 INTERNET: SURFACE E DEEP WEB

A internet surgiu como um instrumento para que as instituições militares, pudessem se comunicar de maneira descentralizada. O uso da internet através do *World Wide Web* (WWW) e do protocolo TCP/IP1 popularizou-se a partir dos anos 2000. O uso comercial da internet nos Estados Unidos foi liberado apenas em 1987 e seu desenvolvimento foi exponencial criando uma rede mundial a qual podemos chamar de espaço cibernético ou ciberespaço (LOPES, 2013).

Atualmente, a internet vai muito além de seu uso público ou militar, ela está na vida privada dos indivíduos e as infraestruturas do Estado também dependem desta para se comunicar e operar, tanto nos Estados Unidos quanto no Brasil e em outros países. Com a disseminação da internet e seu uso crescente tanto na vida social quanto econômica e política, considera-se natural que os Estados e demais instituições comecem a pensar em formas de regularizar seu uso.

A ameaça da internet, ou a ameaça que poderia vir deste meio, justifica sua securitização, esse pensamento é explicado por Nissenbaum (2009) ao apontar que, a partir dos anos 1990 a internet se torna palco de políticos e corporações, agentes e instituições que podem afetar diretamente a soberania do Estado. Como resume Lynn (2011 apud RODRIGUES, 2017) *bits e bytes* podem ser tão ameaçadores quanto balas e bombas.

Diversos casos de vazamentos de informações, espionagem e venda de informações assolaram a sociedade. Como Snowden, *Wikileaks* e Assange além de diversas outras denúncias de espionagem e violação de privacidade. Pensar em securitizar a internet evidentemente também cruza a fronteira onde direito de informações e acesso esbarram com privacidade.

Paralelamente aos avanços com a internet surge um ambiente digital, *Deep Web*, cuja premissa é a troca de informação de forma segura através do anonimato, necessário uma vez que a maioria dessas informações pode

corresponder a alguma quebra na lei. A *Deep Web*, essa parte da internet que precisa ser acessada com software específico, fornece mais liberdade ao usuário. Liberdade do anonimato e de trocar informações sem o rastreamento dos acessos, coisa que na *Surface* não é tão simples. Suas origens remontam a um projeto norte-americano de troca de mensagens chamado *The Onion Routing* que daria origem ao projeto *The Onion Router* (TOR), software responsável pelo acesso a essa rede.

Diferente da *Surface Web*, a *Deep Web* se refere à porção da internet que não pode, ou não é indexada através de buscadores tradicionais. A maior parte de seu conteúdo está na *Deep Web*, fora do alcance dos navegadores convencionais. Isso pois o material na *Deep Web* não é indexado e o usuário precisa ter o endereço URL completo para acessar a página desejada (SWIRE, AHMAD, 2012).

A maioria dos sites na *Deep Web* usa um *software* específico de anonimato TOR (*The Onion Router*), que criptografa identidade do usuário agrupando os dados recebidos em pacotes criptografados, anonimizando as informações sobre o remetente removendo parte do cabeçalho do pacote, criptografando o restante das informações de endereço e enviando o pacote de dados criptografados por vários servidores. O TOR é uma ferramenta considerada importante para diversas profissões e atividades ao proteger as comunicações e a navegação online. Tanto jornalistas investigativos quanto policiais e agentes de inteligência usam o Navegador TOR para conduzir suas investigações sem alertar os sites investigados sobre suas visitas; ativistas e defensores de direitos humanos usam a ferramenta para se organizar e discutir temas controversos sem risco de represálias, prisão ou morte em regimes não democráticos (como no Irã, na China e na Síria).

4 ESTUDO DE CASO

A partir das análises e ponderações realizadas buscamos analisar um documento encontrado num repositório na *Deep Web*. Os pontos a serem analisados seguem as recomendações de Santos (2016) e do Projeto Interpares, buscando definir parâmetros de confiabilidade e autenticidade dos documentos e dos sites em que se encontram. Através deste estudo de caso pretende-se observar e analisar onde se pode utilizar as técnicas arquivísticas para garantir a autenticidade de documentos encontrados em ambiente digital, que não estão disponibilizados em instituições arquivísticas e de custódia. Bem como compreender até que ponto pode-se encarar esses documentos como legítimos e ratificar suas informações para uso.

O site escolhido é denominado *Cryptome*. O *Cryptome* é um *website* em atividade desde 1996, e age por uma fundação privada sem fins lucrativos que busca coletar informações sobre liberdade de expressão, privacidade, criptografia, tecnologias de uso duplo, segurança nacional, inteligência e sigilo governamental. Ele também possui uma versão na *surface* e é visto de forma dual na mídia e na política pelo seu discurso de não medir o uso da informação, divulgando informações sigilosas que partem desde a identidade de assassinos e terroristas localização e equipamentos de bases militares do Governo dos Estados Unidos.

O documento escolhido constitui-se de um *Indictment* (acusação, tradução), ou seja, uma acusação penal de que um indivíduo tenha cometido um crime. O documento consiste em uma declaração curta e breve de onde, quando e como o acusado cometeu o crime e cada ofensa é estabelecida em uma contagem separada. Este documento configura-se como uma acusação contra Julian Paul Assange, fundador do site *Wikileaks*, apresentado ao júri na Corte do distrito de Virgínia e data de março de 2018.

Como sugere o modelo de análise do projeto Interpares, o primeiro ponto pra identificar um documento como arquivístico, em uma entidade digital, é atestar que este tenha conteúdo estável e forma fixa e estar fixo em uma mídia estável. O presente documento possui forma física, mantendo a apresentação na tela do computador mesmo que mude de formato e tanto a sua apresentação como conteúdo não se alteram quando é recuperado. Seu conteúdo estável é atestado uma vez quer tornar-se impossível mudar os dados contidos no documento e disponibilizá-los no site. Seu grau de interação é limitado, portanto um documento digital estático, que não solicita entrada de dados.

O segundo ponto da análise é compreender a ação que envolve o documento, o objetivo de sua criação. Neste caso observa-se que o documento foi criado para dar início ao processo penal do réu, nele são listadas o que o réu é acusado e um *attorney* (advogado, tradução nossa), os apresenta mediante ao juiz a após ser endossado à um júri.

O terceiro ponto é destacar a relação orgânica do documento junto de outros. A análise do documento em estudo não permitiu identificar outros documentos que este mantenha relação. Apesar de fornecer algumas informações como número criminal, não há nenhuma outra informação que indique um elo orgânico do documento com outro, capaz de contextualizá-lo.

O ponto seguinte é identificar as pessoas envolvidas com o documento como o autor, redator, destinatário, produtor e o originador. Não é possível confirmar com clareza o papel dos responsáveis pelo documento. É notado

alguns nomes e assinaturas ao longo do documento, mas observa-se também que um deles, do possível autor ou produtor encontra-se censurado por uma tarja preta dando conhecimento apenas de pessoas que poderiam ocupar as posições de redator ou autor ou produtor do documento - sendo o advogado e o assistente que assinam o documento ao fim. Seu destinatário é a própria corte jurídica e, fora isso, é impreciso especificar os demais envolvidos com clareza.

O último ponto é o estabelecimento de contextos identificáveis. O contexto jurídico-administrativo são as regras que envolvem a produção de tal documento, como normas, lei, regimento interno, nesse caso não é possível mapeá-lo. O contexto de proveniência se refere à entidade produtora, seu mandato e estrutura, para tal documento podemos compreender que a acusação foi feita por parte de advogados de um órgão público, sendo, portanto, apresentado ao Tribunal do Distrito Leste da Virgínia, e essa é toda a informação que podemos compreender.

5 CONSIDERAÇÕES FINAIS

Apesar de fornecer informações que se assemelham a verídicas, a ausência de modelos pré-determinados estabelecidos na análise diplomática que sugere o Projeto Interpares faz com que o documento seja dúbio ele não se estabelece aos requisitos arquivísticos, e onde encontra-se disponibilizado tão pouco estabelece metadados e outras estratégias de gestão e de preservação capazes de garantir a confiabilidade e autenticidade de suas informações. É possível, porém, realizar uma análise através de outros moldes que cabem à outras ciências, mas a não capacidade de satisfazer os critérios supracitados coloca em xeque a capacidade do documento ser autêntico por mais que na internet existam outros documentos disponíveis da mesma tipologia documental que sigam a mesma estruturação de informação e suporte que este.

Buscando uma reflexão sobre tema voltamo-nos na afirmação de Innarelli (2011) em que, dada a complexidade dos documentos digitais, sua preservação, e para tal o monitoramento e avaliação de suas características, não será resolvida exclusivamente pela tecnologia. Torna-se passível de debate e consideração relacionar documentos digitais, acessibilidade e a *Deep Web* sobre o pretexto que essa rede de redes se faz, observando as relações que são construídas e a finalidade dos documentos que ali encontram-se.

Temos na Deep Web uma enorme difusão de conteúdo científico e conteúdo governamental que, por algum motivo, não está disponível para o cidadão apesar de ser seu por direito ou por dizer a respeito à o que este consome. Muitos destes documentos, em sua grande maioria digitalizados,

podem ser usados como referencial para a pesquisa científica e para qualquer outro uso que o cidadão queira fazer dele. Além disto, a *Deep Web* oferece um terreno livre onde se é capaz de disseminar a informação de cunho educativo e científico sem medo de represálias ou censura. Fato que também dialoga com a concepção de disseminação da informação das instituições arquivísticas.

Em todo caso, é notável que a Deep Web, em especial a rede *.onion* não são capazes de satisfazer os requisitos que a arquivologia propõe. Apesar de todos os avanços tecnológicos e outras pesquisas que buscam aumentar a quantidade de sites mapeados por motores de buscar e conectar-se à diversas bibliotecas e repositórios *onlines* disponíveis na internet, ainda não há meio seguro de garantir a autenticidade destes documentos e a veracidade das informações contidas neles, ao menos não apenas com os métodos arquivísticos e diplomáticos.

REFERÊNCIAS

BERGMAN, Michael K. White Paper: **The Deep Web: Surfacing Hidden Value**. The journal of electronic publishing, v. 7, n. 1, p 1-25, 2001. Disponível em: <http://dx.doi.org/10.3998/3336451.0007.104>.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Resolução nº 43, de 04 de setembro de 2015**. Altera a redação da Resolução do CONARQ nº 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>>

CHERTOFF, M. C.; SIMON, T. **The impact of the dark web on internet governance and cyber security**. Ontario: Centre for International Governance Innovation and Chatham House, n. 6, p. 1-18, 2015.

COSTA FILHO, C. M. A. **O ciclo vital ante o documento digital: o modelo Records Continuum como recurso de elucidação**. Acervo, v. 29, n. 2, p. 155-167, 2016

DAS NARAYAN, N.; KUMAR, E. Hidden Web Query Technique for Extracting the Data from Deep Web Data Base. In: **Proceedings of the World Congress on Engineering and Computer Science**, 2012, San Francisco. Anais [...]. San Francisco: WCECS, 2012. p. 1-5. Disponível em: http://www.iaeng.org/publication/WCECS2012/WCECS2012_pp410-414.pdf

DOS SANTOS, H. M.; FLORES, D. **Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo**. Perspectivas em ciência da Informação, Belo Horizonte, v. 20, n. 2, p. 198- 218, 2015. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2341>.

_____. **Preservação de documentos arquivísticos digitais autênticos: reflexões e perspectivas.** *Acervo*, v. 28, n. 1, p. 241-253, 2015. Disponível em: <http://oaji.net/articles/2016/3932-1475261404.pdf>

DOS SANTOS, C. H. A.; MARCHI, K. R. da C. **O Que a Deep Web Pode Oferecer Além da Surface Web.** In: XV Semana de Informática; XII Mostra de Trabalhos de Iniciação Científica, 2013, Paranavaí. Anais [...]. Paranavaí: UNIPAR, 2013. p. 1-5. Disponível em: https://www.academia.edu/15658434/O_Que_a_Deep_Web_Pode_Oferecer_Al%C3%A9m_da_Surface_Web.

DURANTI, L. **Registros documentais contemporâneos como provas de ação.** *Revista Estudos Históricos*, v. 7, n. 13, p. 49-64, 1994.

FUNARI, Pedro Paulo A. Heloisa Liberalli Bellotto, **Arquivos permanentes. Tratamento documental.** Segunda edição revista e ampliada. Rio de Janeiro: FGV, 2004, 320pp. ISBN 85-225-0474-1. *Revista CPC*, n. 2, p. 129-132, 2006.

INNARELLI, H. C. **Preservação digital: a influência da gestão dos documentos digitais na preservação da informação e da cultura.** *Revista digital de biblioteconomia e ciência da informação*, Campinas, v. 9, n. 1, p. 72-87, 2011. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/1934>.

INTERPARES. **Projeto InterPARES 2.** [S.l.: s.n.], 2006. Disponível em: http://www.conarq.arquivonacional.gov.br/images/publicacoes_textos/Diretrizes_produtores.pdf

FIDELIS, M. B.; FERREIRA, J. S.; DIAS, D. M. **Patrimônio documental e cidadania: importância do acesso pleno à memória das conquistas sociais e trabalhistas no SINTECT-PB.** In: Congresso nacional de arquivologia, 2016, Fortaleza. Anais eletrônicos [...] *Revista Analisando em Ciência da Informação*, João Pessoa, v. 4, p. 794-805, 2016. Disponível em: http://racin.arquivologiauepb.com.br/edicoes/v4_nesp.

LOPES, G. **Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá.** Dissertação de mestrado (Mestrado em Ciências Políticas) – Universidade Federal de Pernambuco, Recife, 2013. Disponível em: <https://repositorio.ufpe.br/handle/123456789/12489>

NISSINBAUM, H. **Privacy in context: Technology, policy, and the integrity of social life.** California: Stanford University Press, 2010. 22p

RODRIGUES, J. R. **A cibersegurança americana e a escola de Copenhague: do paradigma da securitização ao caso Edward Snowden.** UNINTER, p. 1-14, 2017. Disponível em: <https://repositorio.uninter.com/handle/1/270>.

RONDINELLI, R. C. **Fidedignidade e autenticidade do documento eletrônico: uma abordagem arquivística.** In: 3º Integrar Congresso

Internacional de Arquivos, Bibliotecas, Centros de Documentação e Museus. 2002. Anais [...] São Paulo: Universidade Presbiteriana Mackenzi, 2002. p. 471-483

SWIRE, P.; AHMAD, K. **Going Dark** Versus a **'Golden Age for Surveillance**. Center for Democracy and Technology, p. 1-5, 2011. Disponível em: [https://fpf.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-forSurveillance-Peter-Swire-and-Kenesa-A.pdf](https://fpf.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf).