LOGEION
Filosofia da Informação

ARTIGO

DOI: https://doi.org/10.21728/logeion.2016v2n2.p80-90

CONSENTIMENTO INFORMADO. PODEMOS FAZER MELHOR EM DEFESA DA PRIVACIDADE

Dr. Frederik Zuiderveen Borgesius,

Instituto do Direito da Informação da Universidade de Amsterdam

E-mail: f.j.zuiderveenborgesius@uva.nl

Este artigo tem como base um artigo de Frederik Zuiderveen Borgesius para o IEEE, "Informed Consent: We Can Do Better to Defend Privacy", *IEEE Security & Privacy*, vol.13, no. 2, pp. 103-107, Mar.-Apr. 2015, doi:10.1109/MSP.2015.34

Resumo

Precisamos repensar a nossa abordagem quanto à proteção da privacidade na internet. Atualmente, os formuladores de políticas vêm se aprofundando na ideia de consentimento informado como um meio para proteger a privacidade. Por exemplo, em diversos países, as empresas são obrigadas por lei a obter o consentimento de um indivíduo antes de fazer uso dos seus dados; com base nessas requisitos de consentimento informado, a lei tem por objetivo empoderar as pessoas a fazerem escolhas de privacidade tendo em vista os seus melhores interesses. No entanto, estudos comportamentais colocam em cheque a eficácia desta abordagem de empoderamento como um meio para proteger a privacidade. Este artigo defende uma abordagem conjunta de proteção e empoderamento dos indivíduos para aprimorar a proteção da privacidade. Este artigo aborda problemas práticos do consentimento informado como um meio para proteger a privacidade, e ilustra problemas com os atuais regulamentos de proteção à privacidade dos dados, concernentes à segmentação comportamental. Primeiramente, discutem-se os problemas de privacidade relativos à segmentação comportamental, e o papel central do consentimento informado ao abrigo da lei de proteção à privacidade. Em seguida, enfatizam-se os problemas práticos referentes ao consentimento informado. Por fim, o artigo argumenta que os formuladores de políticas devem dar mais atenção aos regulamentos que protegem as pessoas, e menos aos que as empoderam.

Palavras-chave: Privacidade na internet. Proteção da privacidade. Lei de proteção à privacidade.

INFORMED CONSENT: WE CAN DO BETTER TO DEFEND PRIVACY

Abstract

We need to rethink our approach to defend privacy on the internet. Currently, policymakers focus heavily on the idea of informed consent as a means to defend privacy. For instance, in many countries the law requires firms to obtain an individual's consent before they use data about her. With such informed consent requirements, the law aims to empower people to make privacy choices in their best interests. But behavioural studies cast doubt on this approach's effectiveness, as people tend to click OK to almost any request they see on their screens. To improve privacy protection, this article argues for a combined approach of protecting and empowering the individual.

Keywords: *Privacy on the internet. Privacy protection. Privacy protection law.*

1 Segmentação comportamental e privacidade

Segmentação comportamental é uma técnica de marketing que envolve o rastreamento do comportamento das pessoas na Internet para usar as informações recolhidas e exibir anúncios direcionados a cada indivíduo.[1] As informações captadas para fins da segmentação comportamental dizem respeito a diversas atividades on-line: o que as pessoas leem, os vídeos que assistem, o que pesquisam, etc. Os perfis individuais podem ser enriquecidos com dados atualizados da localização dos usuários de dispositivos móveis, e outros dados que são coletados on e off-line. Alguns provedores de e-mail ou serviços de redes sociais analisam o conteúdo das mensagens para fins de marketing. Recolhe-se uma vasta quantidade de informações sobre centenas de milhões de pessoas para fins da segmentação comportamental.

Em princípio, a segmentação comportamental pode beneficiar empresas e consumidores. As pessoas podem desfrutar do acesso a ferramentas de tradução on-line, jornais e contas de e-mail, bem como assistir vídeos e ouvir música na Internet sem custo algum. A publicidade suporta diversos serviços de Internet. No entanto, é também possível haver uma publicidade que não exija o monitoramento do comportamento das pessoas, como por exemplo, a publicidade contextual: anúncios de carros em sites sobre carros. Portanto, não está claro se a segmentação comportamental se faz necessária para financiar sites e serviços "gratuitos".

A segmentação comportamental, no entanto, levanta questões relativas à privacidade. Três delas são: (i) os efeitos inibidores, (ii) a falta de controle sobre as informações pessoais, e (iii) o risco de discriminação e manipulação injustas. Em primeiro lugar, a segmentação comportamental implica a enorme coleta de informações sobre as atividades das pessoas na Internet. À semelhança de outros tipos de vigilância, esse fato pode causar efeitos inibidores: as pessoas podem adaptar o seu comportamento caso suspeitem que as suas atividades estejam sendo monitoradas.[2]

---

[1] Quanto à segmentação comportamental, ver: J Turow, The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth (New Haven, Yale University Press, 2011); Zuiderveen Borgesius FJ, Improving Privacy Protection in the Area of Behavioural Targeting (Tese de Doutorado na Universidade de Amsterdam), Kluwer law International (no prelo).
[2] Ver Richards NM, 'Intellectual privacy' (2008) 87 Texas Law Review 387.

Em segundo lugar, as pessoas não têm controle sobre os dados que lhes dizem respeito. Não sabem quais informações são capturadas, como são usadas e com quem são compartilhadas. O armazenamento de dados pessoais em grande escala impõe riscos. Por exemplo, pode haver violação de dados, ou os dados podem ser usados para fins inesperados, como falsidade ideológica. Além disso, a sensação de perda de controle é um problema de privacidade.

Em terceiro lugar, a segmentação comportamental permite a seleção social e práticas discriminatórias: as empresas podem classificar as pessoas como "alvos" e "rejeitados", e tratá-las em conformidade. Por exemplo, um anunciante pode usar descontos para atrair pessoas endinheiradas com o intuito de transformá-las em clientes regulares - mas pode excluir as pessoas humildes dessa campanha. [3] E alguns temem que a segmentação comportamental possa ser usada para manipular as pessoas. A publicidade personalizada pode ser eficaz ao ponto de os anunciantes obterem vantagem injusta sobre os consumidores.[4] Outros temem que a personalização excessiva possa levar a uma "cápsula da informação,[5] ou a uma "bolha filtradora": "um universo único de informações relativas a cada um de nós.[6] Este receio parece mais pertinente quando as empresas personalizam não somente os anúncios, mas também outros conteúdos e serviços. Resumidamente, a ideia é que a publicidade personalizada e outros conteúdos podem guiar os pensamentos das pessoas de forma velada.

2 O consentimento informado ao abrigo da lei de proteção à privacidade dos dados

O consentimento informado e a escolha individual desempenham um papel central em diversos regulamentos de proteção à privacidade dos dados em todo o mundo. Por exemplo, as Diretrizes OCDE de Proteção à Privacidade afirmam que os dados pessoais devem ser obtidos "se for o caso, com o conhecimento ou consentimento do titular dos dados."[7] Nos Estados Unidos, a carta de lei de proteção à privacidade do consumidor enfatiza (em um relatório da Casa Branca) a importância da escolha individual a respeito de como os seus

---

[3] J Turow, *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth* (New Haven, Yale University Press, 2011).
[4] Calo MR. 'Digital market manipulation', George Washington Law Review, 82 George Washington Law Review 995 (2014).
[5] CR Sunstein, *Infotopia: How many minds produce knowledge* (Oxford, Oxford University Press, 2006), p 9.
[6] E Pariser, *The Filter Bubble* (London, Penguin Viking, 2011), p 9.
[7] Princípio de Limitação à Coleta (n° 7), Diretrizes da OCDE que regem a proteção da privacidade e os fluxos transfronteiriços de dados pessoais.

dados devem ser usados.[8] Um conjunto de causas da Comissão Federal de Comércio sinaliza que a agência defende que o aviso proeminente e a adesão voluntária do usuário são imprescindíveis para recolher informações pessoais sigilosas."[9]

A Portaria de Proteção à Privacidade e Comunicações Eletrônicas da UE é outro exemplo do papel central do consentimento informado nos termos da lei de proteção à privacidade dos dados. A portaria exige que qualquer parte que armazene ou acesse informações a partir do dispositivo de um usuário obtenha o consentimento informado desse usuário.[10] O regulamento se aplica a diversas tecnologias de rastreamento, incluindo os cookies. Um consentimento válido exige a indicação livre, específica e esclarecida da vontade do usuário.[11] As pessoas podem expressar a sua vontade de qualquer forma, no entanto, o mero silêncio ou inatividade não são uma expressão da vontade. Algumas empresas sugerem poder presumir o consentimento "implícito", caso os usuários não bloqueiem os *cookies* de rastreamento no seu navegador.[12] Mas esta interpretação da lei parece incorreta. As Autoridades de Proteção dos Dados da UE afirmam que o simples fato de uma pessoa deixar as configurações do navegador intocadas não significa que tenha expressado a sua vontade de ser rastreada.[13]

Além disso, a legislação da UE exige que o consentimento seja voluntário ("concedido livremente"): o consentimento sob pressão não é válido. No entanto, na maioria dos casos, a lei atual de proteção à privacidade dos dados provavelmente autorizará as empresas a oferecerem condições de natureza "pegar ou largar". Por isso, em princípio, os publicadores do conteúdo do site estão autorizados a instalar mecanismos de rastreamento que neguem a entrada de visitantes que não autorizarem os seu rastreamento para fins da segmentação comportamental. Entretanto, o mecanismo de rastreamento pode fazer com que tal

---

[8] White House, 'Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (2012) <www.whitehouse.gov/sites/default/files/privacy-final.pdf>, p. 47; p. i.
[9] Ver: Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers' (março de 2012) www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, p. 58 (hereinafter: FTC 2012).
[10] Portaria 2002/58/CE, alterada pela Portaria 2009/136/CE.
[11] Portaria de Proteção de Dados de 1995/46/CE.
[12] Interactive Advertising Bureau United Kingdom, 'Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework, IAB UK Response' (01 de dezembro de 2012) www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf, p 2.
[13] Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising' (WP 171), 22 de junho de 2010.

consentimento seja involuntário, caso as pessoas tenham a necessidade de usar o site. Por exemplo, de acordo com a Autoridade de Proteção de Dados holandesa, a organização pública nacional de radiodifusão não está permitida a usar um mecanismo de rastreamento, visto que a única maneira de acessar certas informações on-line é através do site da emissora.[14] As Autoridades de Proteção dos Dados da UE afirmam que o consentimento deve ser concedido espontaneamente, mas não está claro se a lei atual proíbe os mecanismos de rastreamento em todos os casos.[15]

3 O consentimento informado na prática

A teoria econômica pode auxiliar a análise dos problemas práticos relativos ao consentimento para fins da segmentação comportamental. A partir de uma perspectiva econômica, dar consentimento à segmentação comportamental é equivalente a efetuar uma transação de mercado com uma empresa. Mas essa "transação" é posta em risco por assimetrias de informação. Pesquisas demonstram que muitas pessoas não sabem até que ponto o seu comportamento é monitorado.[16] Portanto, a sua "escolha" em divulgar os dados em troca do uso de um serviço não é considerada uma escolha informada.

Contudo, conforme destacado pela pesquisa econômico-comportamental, mesmo se as empresas solicitassem o consentimento para fins da segmentação comportamental, a assimetria de informação continuaria a ser um problema.[17] É raro as pessoas saberem o que as empresas fazem com os seus dados pessoais, e é difícil prever as consequências do uso de dados no futuro. Se as pessoas não podem avaliar a qualidade dos produtos, as empresas têm poucos incentivos para competir em qualidade. Isto pode levar a produtos de baixa qualidade.[18] Os sites raramente competem em privacidade, conforme ilustrado pelo fato de as

---

[14] Dutch DPA, Letter to the State Secretary of Education, Culture and Science, 31 de janeiro de 2013, www.cbpweb.nl/downloads_med/med_20130205-cookies-npo.pdf.
[15] Article 29 Working Party 2013, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (WP 208) 2 de outubro de 2013. Ver também FTC 2012, p. 52.
[16] Ver e.g. B Ur et al, 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising' (Proceedings of the Eighth Symposium on Usable Privacy and Security ACM, 2012) 4.
[17] Ver A Acquisti and J Grossklags , 'What Can Behavioral Economics Teach Us About Privacy?' in A Acquisti et al (eds), *Digital Privacy: Theory, Technologies and Practices* (London, Auerbach Publications, Taylor and Francis Group 2007).
[18] T Vila, R Greenstadt and D Molnar, 'Why We Can't be Bothered to Read Privacy Policies. Models of Privacy Economics as a Lemons Market' in LJ Camp, and S. Lewis (eds), *Economics of Information Security* (Heidelberg, Springer, 2004).

pessoas serem rastreadas em praticamente todos os sites populares para fins da segmentação comportamental.[19] Parece haver uma situação semelhante no mercado relativa aos aplicativos de *smartphones*.

Quando estimulada pelos fundamentos de controle da privacidade, a lei de proteção à privacidade dos dados visa reduzir a assimetria de informação. Para ilustrar, a legislação da UE exige que as empresas divulguem certas informações aos indivíduos, por exemplo, os fins para os quais os dados pessoais são usados. Os publicadores do conteúdo podem fazer uso de uma política de privacidade de forma a cumprir com os requisitos de transparência da lei de proteção aos dados.

No entanto, o problema de assimetria de informação é difícil solucionar devido aos custos de transação para o indivíduo, e novamente, as assimetrias de informação a respeito do significado das políticas de privacidade. Ler as políticas de privacidade levaria muito tempo, já que são geralmente longas, difíceis de ler, e vagas. (Um estudo calculou que as pessoas levariam diversas semanas para ler a política de privacidade de cada site visitado.[20]) Além disso, as políticas de privacidade são demasiadamente difíceis para muitas delas. Portanto, não é surpreendente o fato de quase ninguém ler as políticas de privacidade. Conforme discorre um relatório da Casa Branca, "[s]omente em um mundo imaginário os usuários de fato leem esses avisos e compreendem as suas implicações antes de clicar para dar o seu consentimento."[21] Na prática, a lei de proteção à privacidade dos dados, portanto, não resolve o problema de assimetria de informação.

Para ilustrar o fato, uma loja do Reino Unido conseguiu fazer com que 7500 pessoas lhe vendessem a alma. De acordo com os termos e condições do site, os clientes concediam "a opção intransferível de vender para sempre a sua alma imortal", a menos que recusassem.

---

[19] Hoofnagle, CJ; Good N, 'The web privacy census' (outubro de 2012) <http://law.berkeley.edu/privacycensus.htm>.
[20] AM McDonald and LF Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) *I/S: A Journal of Law and Policy for the Information Society* 540.
[21] White House (Podesta J et al.), 'Big Data: Seizing Opportunities, Preserving Values' (maio de 2014) www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, p. xi.

Caso o fizessem, poderiam salvar a sua alma, e receber um voucher no valor de 5 libras. Mas poucas pessoas recusaram. A empresa depois disse que não exerceria os seus direitos.[22]

A economia comportamental visa aprimorar o poder preditivo da teoria econômica, incluindo percepções a partir de estudos comportamentais e de psicologia. A economia comportamental sugere que as pessoas agem de forma estruturalmente diversa daquela prevista pela teoria da escolha racional econômica. Devido à sua racionalidade limitada, as pessoas geralmente contam com regras básicas, ou com a heurística. Normalmente, esses atalhos mentais funcionam, mas também podem levar a um comportamento que não esteja no melhor interesse das pessoas. Diversas tendências influenciam as escolhas de privacidade, como aquela visando o status quo e a presente.

A tendência que visa o status quo, ou a tendência padrão, descreve a predisposição das pessoas em manter as opções padrão. Elas são menos propensas a dar consentimento sob um regime de adesão que requeira uma ação afirmativa para que o consentimento seja válido, do que sob um regime de exclusão, onde se presume que as pessoas consintam caso não se oponham. [23] Nesta perspectiva, a discussão contínua sobre a adesão/exclusão quanto à segmentação comportamental e outros tipos de marketing direto diz respeito à questão de quem se beneficia com a tendência visando o status quo, a empresa ou o indivíduo.

A tendência presente, ou miopia, sugere que as pessoas costumam escolher a gratificação imediata e desconsiderar os custos ou desvantagens futuros. Por exemplo, muitos acham difícil seguir uma dieta, ou economizar. Se um site conta com um mecanismo de rastreamento, e as pessoas só puderem usar o site se concordarem com o direcionamento comportamental, elas estarão propensas a consentir, ignorando assim os custos de violações de privacidade futuras.

Em suma, a economia comportamental mostra que proteger a privacidade com o instrumento do consentimento informado é bastante problemático. É exagero dizer que as pessoas não leem as políticas de privacidade; se fossem ler, não entenderiam; se entendessem, não

---

[22] Fox News, '7,500 Online Shoppers Unknowingly Sold Their Souls' (15 de abril de 2010) www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/.
[23] Ver Acquisti A and Gross R, 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook' (2006) 4258 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006 (Lecture Notes in Computer Science) 36.

agiriam. Além disso, se todos os concorrentes explorarem a assimetria de informação e as predisposições das pessoas, as empresas têm de fazer o mesmo para permanecer no mercado. As percepções da economia comportamental, assim, sugerem que uma intervenção mais reguladora se justifica na área da segmentação comportamental.

4 Proteção individual ao invés de empoderamento

Algumas leis de proteção à privacidade dos dados contêm regulamentos que poderiam proteger os interesses de privacidade - também depois de as pessoas consentirem o processamento. Por exemplo, de acordo com as Diretrizes OCDE de Proteção à Privacidade, os dados pessoais devem ser protegidos por controles de segurança adequados. [24] Os regulamentadores da UE e dos EUA também enfatizam a necessidade de as empresas protegerem os dados que possuem.[25]

E a lei de proteção à privacidade dos dados da UE tem um regime mais rigoroso para as "categorias especiais de dados", como os dados que revelam a raça, as opiniões políticas, a saúde ou a vida sexual. [26] Em diversos países da União Europeia, o uso das categorias especiais de dados pessoais para marketing direto é proibido; em outros países, só é permitido com o consentimento explícito dos indivíduos.[27] Algumas empresas direcionam a publicidade com base em categorias como "artrite", "estado geral de saúde cardiovascular", [28] ou "consumidores portadores de necessidades especiais/deficientes." [29] Essas empresas processam categorias especiais de dados. Uma aplicação rigorosa dos regulamentos existentes relativos a categorias específicas de dados pode reduzir problemas de privacidade, tais como os efeitos inibidores.

Uma vez que os riscos de privacidade envolvidos no uso de dados de saúde para fins da segmentação comportamental parecem superar os possíveis benefícios para a sociedade ao permitir tais práticas, deve-se considerar a proibição do uso de todos os dados relativos à

[24] Princípio do Controle de Segurança (n°11), Diretrizes da OCDE que regem a proteção da privacidade e os fluxos transfronteiriços de dados pessoais.
[25] FTC 2012, p. 24-26. Ver também o artigo 17 da Portaria de Proteção de Dados da UE.
[26] Artigo 8 da Portaria de Proteção de Dados.
[27] Há exceções, mas não são relevantes para a segmentação comportamental.
[28] Yahoo Privacy, 'All Standard Categories' http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/asc/details.html.
[29] Rocket Fuel, 'Health Related Segments' http://rocketfuel.com/downloads/Rocket%20Fuel%20Health%20Segments.pdf.

saúde para fins da segmentação comportamental, seja mediante consentimento explícito do indivíduo ou não. Os regulamentos sobre as categorias especiais de dados poderiam ser interpretados levando em consideração o contexto da sua coleta. Por exemplo, o rastreamento de visitas a sites contendo informações médicas deve, sem dúvida, ser visto como o processamento de "categorias especiais de dados", visto que a empresa pode inferir dados sobre a saúde a partir de tais informações de rastreamento.

Na medida em que a aplicação rigorosa dos princípios mais protetores da lei de proteção à privacidade dos dados possa de alguma forma mitigar os problemas de privacidade, são necessários regulamentos complementares relativos a este assunto. Vimos que os requisitos de consentimento informado, mesmo que sejam exigidos os sistemas de adesão, não serão eficazes para estimular a privacidade enquanto as empresas estiverem autorizadas a oferecer condições de natureza "pegar ou largar".

5 Ampliando o debate

É hora de ampliar o debate da privacidade além do consentimento informado. Visando à transparência, o consentimento não será suficiente para garantir um nível razoável de privacidade. O direito do consumidor ilustra como o empoderamento e os regulamentos de proteção à privacidade podem ser usados como ferramentas complementares. Em muitos casos, o direito do consumidor exige que as empresas divulguem informações aos consumidores (calorias, custos de entrega...). Tais requisitos de transparência têm como objetivo empoderar os consumidores a tomarem decisões de acordo com as suas preferências. Outros regulamentos relativos ao direito do consumidor visam proteger os consumidores. Por exemplo, alguns ingredientes alimentares não podem ser utilizados, e há normas mínimas de segurança para diversos produtos.

Alguns sugerem que os formuladores de políticas devem dar mais atenção ao uso de dados, e menos ao consentimento informado visando a coleta de dados.[30] Entretanto, concentrar-se principalmente no uso de dados impõe riscos consideráveis. Contesto fortemente a ideia de a coleta de dados manter-se, em grande parte, não regulamentada. Muitos problemas de

[30] Ver, por exemplo, o Conselho de Consultores da Presidência em Ciência e Tecnologia, ""Big Data and Privacy: A Technological Perspective," 2014, e Craig Mundie, "Privacy Pragmatism: Focus on Data Use, Not Data Collection," Relações Internacionais.

privacidade, como os efeitos inibidores, já ocorrem por causa da coleta de dados. Além disso, na Europa, seria difícil conciliar um regime que não regulamente a coleta de dados com a jurisprudência dos direitos fundamentais e os tratados.[31]

O que os formuladores de políticas devem fazer sobre as condições de natureza "pegar ou largar". como os mecanismos de rastreamento? A lei pode proibir mecanismos de rastreamento em determinadas circunstâncias. Por exemplo, as empresas de serviço público de radiodifusão muitas vezes recebem financiamento público, e têm um papel essencial prestando informações às pessoas. Mas se as pessoas temerem o monitoramento do seu comportamento, podem desistir de usar os meios de comunicação de serviço público. Portanto, os formuladores de políticas devem proibir as empresas de serviço público de radiodifusão de instalar mecanismos de rastreamento nos seus sites. Os formuladores de políticas também poderiam ir além e proibir todo o rastreamento de terceiros para fins da segmentação comportamental nos meios de comunicação de difusão pública.

Em termos gerais, é questionável a pertinência de os sites de órgãos estaduais permitirem o rastreamento de terceiros para fins da segmentação comportamental - mesmo com o consentimento das pessoas. Na prática, os sites do setor público podem usar *widgets* de terceiros, tais como botões de mídia social; os publicadores de conteúdo do site podem não perceber que tais *widgets* podem expor os visitantes a um rastreamento de privacidade invasivo. No entanto, não está claro o motivo pelo qual o setor público deva facilitar o rastreamento do comportamento das pessoas para fins comerciais. Portanto, os formuladores de políticas devem considerar a proibição de todo rastreamento para fins da segmentação comportamental em sites públicos.

Os formuladores de políticas podem acrescentar proibições às suas agendas para regulamentar a segmentação comportamental. Mas seria difícil definir as proibições de forma que não sejam super ou subinclusivas. As perguntas difíceis são colocadas diante dos pesquisadores e formuladores de políticas. Deve-se manter um equilíbrio cuidadoso entre o paternalismo indevido e a proteção às pessoas. A proteção jurídica da privacidade continuará sendo um processo de aprendizagem. Caso sejam adotados novos regulamentos, o seu efeito prático

[31] Ver, por exemplo: Tribunal Europeu dos Direitos Humanos, S. e Marper v, Reino Unido, n° 30562/04 e 30566/04.04 de dezembro de 2008, par. 67; Tribunal de Justiça da União Europeia, C-293/12 e C-594/12, Digital Rights Ireland Ltd, 8 de abril de 2014, par.29.

teria de ser avaliado. Os problemas com os requisitos atuais de consentimento informado demonstram que a regulamentação, que parece boa no papel, não é capaz de proteger efetivamente a privacidade na prática.

6 Protegendo a privacidade com o uso da tecnologia

A distinção entre os regulamentos de empoderamento e proteção nos termos da lei poderia também estimular discussões sobre ferramentas técnicas de proteção à privacidade. Empoderar os usuários é uma meta importante. Por exemplo, a tecnologia pode ajudar a promover a transparência significativa em matéria de processamento de dados e criação de perfis. E são necessários mecanismos de fácil utilização para dar, suspender ou retirar o consentimento. No entanto, em algumas circunstâncias, as pessoas podem obter mais benefícios da proteção contra os riscos, do que serem confrontadas com questões de transparência e escolhas. Exemplos de abordagens técnicas mais protetoras incluem serviços que automaticamente protegem as informações pessoais, metadados ou comunicações, independentemente da iniciativa do usuário.

7 Conclusão

Em conclusão, não há uma solução definitiva para aprimorar a proteção da privacidade na área de segmentação comportamental. Embora a regulamentação atual muitas vezes enfatize o empoderamento individual sem muita reflexão sobre as questões práticas, poder-se-ia usar uma abordagem combinada para proteger e empoderar as pessoas. Para aprimorar a proteção da privacidade, a lei atual de proteção à privacidade dos dados deve ser mais rigorosamente aplicada. Mas o potencial limitado do consentimento informado deve ser levado em consideração como uma medida de proteção da privacidade. Por isso, os formuladores de políticas devem dar mais atenção aos regulamentos que protegem as pessoas, e menos aos que as empoderam.