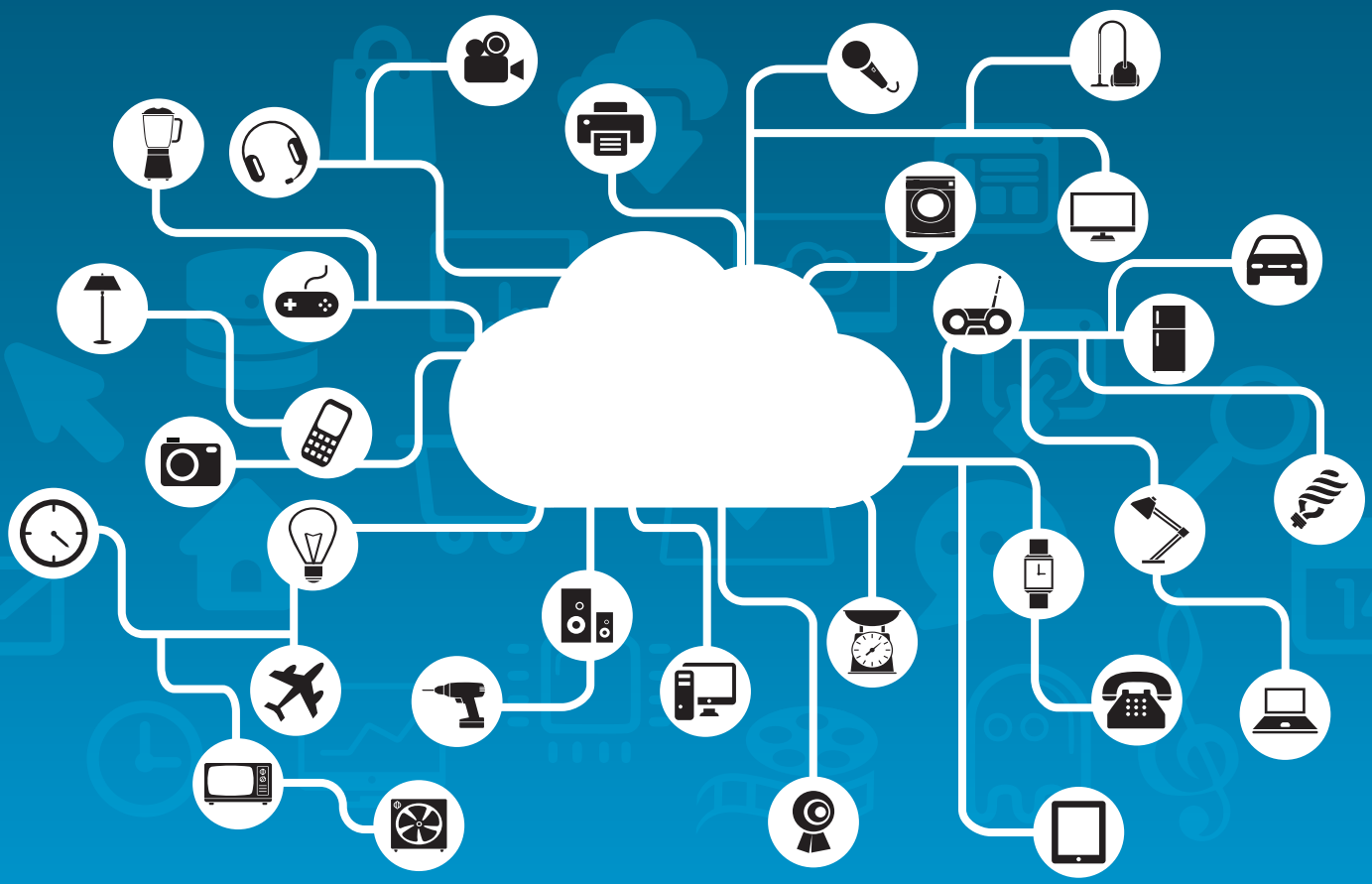
Carta aberta aos líderes de governos do mundo. Pág. 25

# poliTICs

Uma publicação do Instituto Nupef . nº 24 . Outubro | 2016



# A Internet das coisas
## e a segurança do mundo real

## Neutralidade da rede
Um documento informativo da Internet Society sobre política pública. Pág. 16

## O que é a governança de algoritmos? Pág. 9

instituto nupef

# poliTICs

índice nº 24

# Editorial

A Internet, ainda jovem, segue em expansão, diversificando-se, e a crescente introdução de inovações está longe de chegar a um limite. Estas inovações ocorrem tanto em software como em dispositivos e equipamentos, e nas várias formas em que a própria estrutura das redes é organizada e ampliada. Um dos desafios cada vez mais preocupantes envolve o balanço entre essas inovações, as políticas públicas e as implicações para a privacidade, a segurança pessoal e os direitos básicos de acesso à informação. A Internet é o conjunto de seus usuários na ponta – parece trivial dizer isso, mas sem eles e elas a rede de redes não faz sentido e não teria chegado ao que é hoje.

Todos os textos desta edição tratam de um ou mais aspectos desse balanço: os riscos de segurança ampliados com o avanço da chamada Internet das Coisas (IoT); os riscos para todos os envolvidos ao confiar em algoritmos que automatizam atividades e processos; a defesa da neutralidade da rede em sistemas cada vez mais complexos; e o direito essencial a criptografar os dados pessoais.

A chamada interação máquina-a-máquina (ou sensores-a-sensores), conhecida pela sigla M2M, já existia mesmo antes da generalização da Internet e independente desta: sensores que permitem que veículos passem automaticamente por pedágios, prevenção de furtos em lojas e muitos outros. Bruce Schneier alerta que o novo tsunami de inovação na Internet motivado pela generalização da IoT em que bilhões de sensores de todos os tipos estarão conectados e terão algum poder de computação embarcado traz novos desafios para a confidencialidade, integridade e disponibilidade da informação. Veículos podem ser remotamente desativados em movimento, fechaduras podem ser violadas ou bloqueadas, redes elétricas sabotadas, e até assassinatos podem ser cometidos por comando remoto de sistemas médico-hospitalares – resultados possíveis do fato que os dispositivos, equipamentos e sistemas passam a conter computadores embarcados e conectados à Internet.

Virgilio Almeida e Danilo Doneda alertam para riscos similares no uso de algoritmos para automatizar processos que envolvem coleta, armazenagem e manipulação de dados de pessoas e organizações, tanto em serviços de e-governo como em outros e-serviços, e para a necessidade de códigos de conduta para desenvolvedores, operadores e administradores desses sistemas. Fazem assim um chamamento para a necessidade de critérios de governança de algoritmos.

A poliTICs inaugura nesta edição uma parceria entre o Instituto Nupef e a Internet Society, para a publicação periódica em português de documentos relevantes de políticas relacionadas aos direitos na Internet. O primeiro texto é uma revisão detalhada dos conceitos de neutralidade da rede, traduzido e adaptado por Raquel Gatto. Agradecemos a Raquel, coordenadora de desenvolvimento de capítulos e a Raúl Echeberría, vicepresidente de engajamento global da Internet Society.

A defesa do direito básico que tem cada pessoa ou entidade de codificar seus dados está em risco. Governos têm sugerido leis ou regulações para de algum modo impedir ou limitar esse direito. O manifesto do movimento "Secure the Internet" ("mantenha a Internet segura") faz uma forte defesa do direito à criptografia e cita o Relator Especial das Nações Unidas para a Liberdade de Expressão: "a criptografia, o anonimato e os conceitos de segurança a eles relacionados, oferecem a privacidade e segurança necessárias para o exercício do direito à liberdade de opinião e de expressão na era digital."

Boa leitura!

**Bruce Schneier**, especialista em segurança de tecnologias de informação internacionalmente renomado, é fellow do Berkman Center da Universidade Harvard, membro do conselho da Electronic Frontier Foundation (EFF) e membro do conselho assessor do Centro de Informação sobre Privacidade Eletrônica (EPIC), entre muitas outras atividades.

# A Internet das coisas e a segurança do mundo real

Histórias de desastres envolvendo a Internet das Coisas estão na moda[1]. Incluem carros (com ou sem motorista), a rede de energia, barragens e sistemas de ventilação de túneis. Uma especialmente vívida e realista, uma ficção sobre o futuro próximo publicada no mês de junho de 2016 no *New York Magazine* descrevia um ciberataque a Nova York envolvendo ataques de *hackers* a veículos, ao sistema de abastecimento de água, a hospitais, elevadores e à rede elétrica. Nessas histórias, milhares de pessoas morrem. Estabelece-se o caos. Enquanto alguns desses cenários exageram a destruição em massa[2], os riscos individuais são todos reais. E a segurança de computadores e redes tradicional não está preparada para lidar com eles.

A segurança da informação clássica é uma tríade: confidencialidade, integridade e disponibilidade. Em inglês essa tríade é frequentemente referida pela sigla CIA *("confidentiality, integrity, and availability")*, que, convenhamos, cria alguma confusão no contexto da segurança nacional. Mas basicamente as três iniciativas que podem ser feitas com seus dados são furtá-los (confidencialidade), modificá-los (integridade) ou bloqueá-los impedindo que você os use (disponibilidade).

Até agora as ameaças da Internet têm sido largamente sobre confidencialidade. Estas podem ter consequências custosas; uma amostragem estimou que as violações de dados custam uma média de US$ 3,8 milhões cada[3]. Elas podem ser constrangedoras, como o furto de fotos de celebridades do iCloud da Apple em 2014 ou a violação do portal Ashley Madison em 2015. Eles podem ser prejudiciais, como

1. https://motherboard.vice.com/tag/The+Internet+of+Hackable+Things
2. https://www.schneier.com/essays/archives/2005/09/terrorists_dont_do_m.html
3. https://securityintelligence.com/cost-of-a-data-breach-2015

quando o governo da Coreia do Norte furtou dezenas de milhares de documentos internos da Sony ou quando *hackers* roubaram dados de cerca de 83 milhões de contas de clientes do banco JPMorgan Chase, ambos em 2014. Elas podem até mesmo afetar a segurança nacional, como no caso da violação de dados do Escritório de Administração de Pessoal do governo dos EUA, presumivelmente pela China em 2015.

Na Internet das Coisas, as ameaças à integridade e disponibilidade são muito piores que as ameaças à confidencialidade[4]. Uma coisa é se a fechadura inteligente de sua porta permite bisbilhotagem para saber que está em casa. Outra coisa bem diferente é se a fechadura pode ser violada por *hackers* para permitir que um ladrão abra a porta – ou impeça o dono da casa de abrir a porta[5]. Um *hacker* que pode bloquear o controle de seu carro, ou assumir o controle do mesmo, é muito mais perigoso do que aquele que pode escutar suas conversas ou rastrear a localização do seu carro.

Com o advento da Internet das Coisas e de sistemas ciberfísicos em geral, estamos dando à Internet mãos e pés: a capacidade de afetar diretamente o mundo físico[6]. Ataques contra dados e informações agora passam a ser também ataques contra pessoas físicas, aço e concreto.

As ameaças de hoje incluem queda de aviões através de ataques a redes de computadores[7], e desativação remota de veículos, seja quando estão desligados e estacionados ou enquanto eles estão em alta velocidade na estrada[8]. Estamos preocupados com manipulação de contagens em urnas eletrônicas[9], canos de água congelados devido a ataques a termostatos[10], e assassinato remoto através de ataques a sistemas médicos[11]. As possibilidades são quase literalmente infinitas. A Internet das coisas poderá permitir ataques que não podemos sequer imaginar.

Os maiores riscos são provenientes de três coisas: sistemas controlados por software; interconexões entre sistemas; e sistemas automáticos ou autônomos. Vejamos cada um deles:

## > Software de controle

A Internet das coisas é o resultado de existir um computador em todos os dispositivos. Isso nos dá um enorme poder e flexibilidade, mas também traz inseguranças. À medida que mais coisas estão sob controle de *software*, tornam-se vulneráveis a todos os ataques já mencionados contra computadores. Mas devido a que muitas dessas coisas são de baixo custo e de longa

4. https://www.schneier.com/blog/archives/2016/01/integrity_and_a.html
5. https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms
6. https://www.schneier.com/blog/archives/2016/02/the_internet_of_1.html
7. http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft
8. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
9. https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html
10. http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html
11. http://www.informationweek.com/partner-perspectives/bitdefender/hacking-vulnerable-medical-equipment-puts-millions-at-risk/a/d-id/1319873

> Com o advento da Internet das Coisas e de sistemas ciberfísicos em geral, estamos dando à Internet mãos e pés: a capacidade de afetar diretamente o mundo físico. Ataques contra dados e informações agora passam a ser também ataques contra pessoas físicas, aço e concreto...

duração, muitos dos sistemas de atualizações e correções que ocorrem rotineiramente para computadores e *smartphones* não funcionam. Atualmente, a única maneira de corrigir ou atualizar o *software* da maioria dos roteadores domésticos é jogá-los fora e comprar novos. E a segurança obtida com a substituição do seu computador ou telefone celular a cada poucos anos não vai ser viável com seu refrigerador ou o termostato de sua casa: na média, um refrigerador é substituido a cada 15 anos[12], e o termostato provavelmente nunca vai ser trocado. Uma pesquisa recente da Universidade de Princeton encontrou 500 mil dispositivos inseguros na Internet[13]. Esse número está prestes a explodir.

## > Interconexões

À medida que os sistemas são interligados, as vulnerabilidades em um podem levar a ataques contra outros. Já vimos contas do Gmail comprometida através de vulnerabilidades em refrigeradores inteligentes Samsung[14], redes hospitalares comprometidas através de vulnerabilidades em dispositivos médicos[15], e os sistemas da empresa Target invadidos devido a uma vulnerabilidade no seu sistema de ventilação e ar condicionado[16]. Sistemas contêm externalidades que afetam outros sistemas de modos imprevisíveis e potencialmente prejudiciais. O que aparenta ser benigno para os projetistas de um sistema pode tornar-se prejudicial quando ele é combinado com algum outro sistema. Vulnerabilidades em um sistema podem propagar-se a outros sistemas, e o resultado é uma vulnerabilidade que ninguém percebeu e ninguém é responsável pela mitigação. A Internet das coisas vai tornar muito mais corriqueira a ocorrência de vulnerabilidades exploráveis. É matemática simples. Se 100 sistemas estão interagindo, isso significa cinco mil interações e cinco mil vulnerabilidades potenciais resultantes dessas interações. Se 300 sistemas estão interagindo,

12. http://homeguides.sfgate.com/expected-life-refrigerator-88577.html
13. https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things
14. http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html
15. http://www.meddeviceonline.com/doc/medjacking-how-hackers-use-medical-devices-to-launch-cyber-attacks-0001
16. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

isso resulta em 45 mil interações. Mil sistemas: 12,5 milhões de interações. A maioria delas vai ser benigna ou desinteressante, mas algumas serão muito prejudiciais.

## > Autonomia

Nossos sistemas de computação são cada vez mais autônomos. Eles compram e vendem ações, ligam ou desligam o aquecedor, regulam o fluxo de eletricidade através da rede e – no caso de veículos sem motorista – pilotam automaticamente viaturas a seus destinos. A autonomia é interessante por várias razões, mas de uma perspectiva de segurança ela significa que os ataques podem ter efeito imediato, automático e amplo. Quanto mais nós removemos os seres humanos do controle, ataques mais rápidos podem ocorrer e mais perdemos a capacidade de usar dispositivos inteligentes que nos ajudariam a perceber falhas antes que seja tarde demais.

Estamos construindo sistemas que são cada vez mais poderoso e cada vez mais úteis. O efeito secundário decorrente é que eles são cada vez mais perigosos. Uma única vulnerabilidade forçou a Chrysler a chamar para reparos 1,4 milhões de veículos em 2015[17]. Estamos acostumados a computadores sendo atacados em massa – basta lembrar das infecções por vírus em grande escala a partir da última década - mas não estamos preparados para a possibilidade de isso ocorrer em todas as coisas ao nosso redor.

Os governos estão começando a preocupar-se. No ano passado, tanto o diretor da Inteligência Nacional (DNI) dos EUA James Clapper[18] e o diretor da NSA Mike Rogers[19] testemunharam perante o Congresso, alertando para essas ameaças. Ambos acreditam que somos vulneráveis.

A Avaliação de Ameaças Mundiais feita pelo DNI em 2015 coloca o desafio desta forma: "A maior parte da discussão pública sobre as ameaças cibernéticas concentrou-se na confidencialidade e oferta da informação; a espionagem cibernética enfraquece a confidencialidade, ao passo que os ataques de negação de serviço e as ações de destruição de dados enfraquecem a oferta de produtos e serviços. No futuro, no entanto, poderemos ver também mais operações cibernéticas para alterar ou manipular informação eletrônica, a fim de comprometer a sua integridade (ou seja, precisão e confiabilidade) em vez de apagá-la ou bloqueá-la. A tomada de decisões governamentais, de executivos, investidores ou outros será prejudicada se eles não puderem confiar nas informações que estão recebendo"[20].

A edição de 2016 da Avaliação do DNI constatou: "As operações cibernéticas futuras

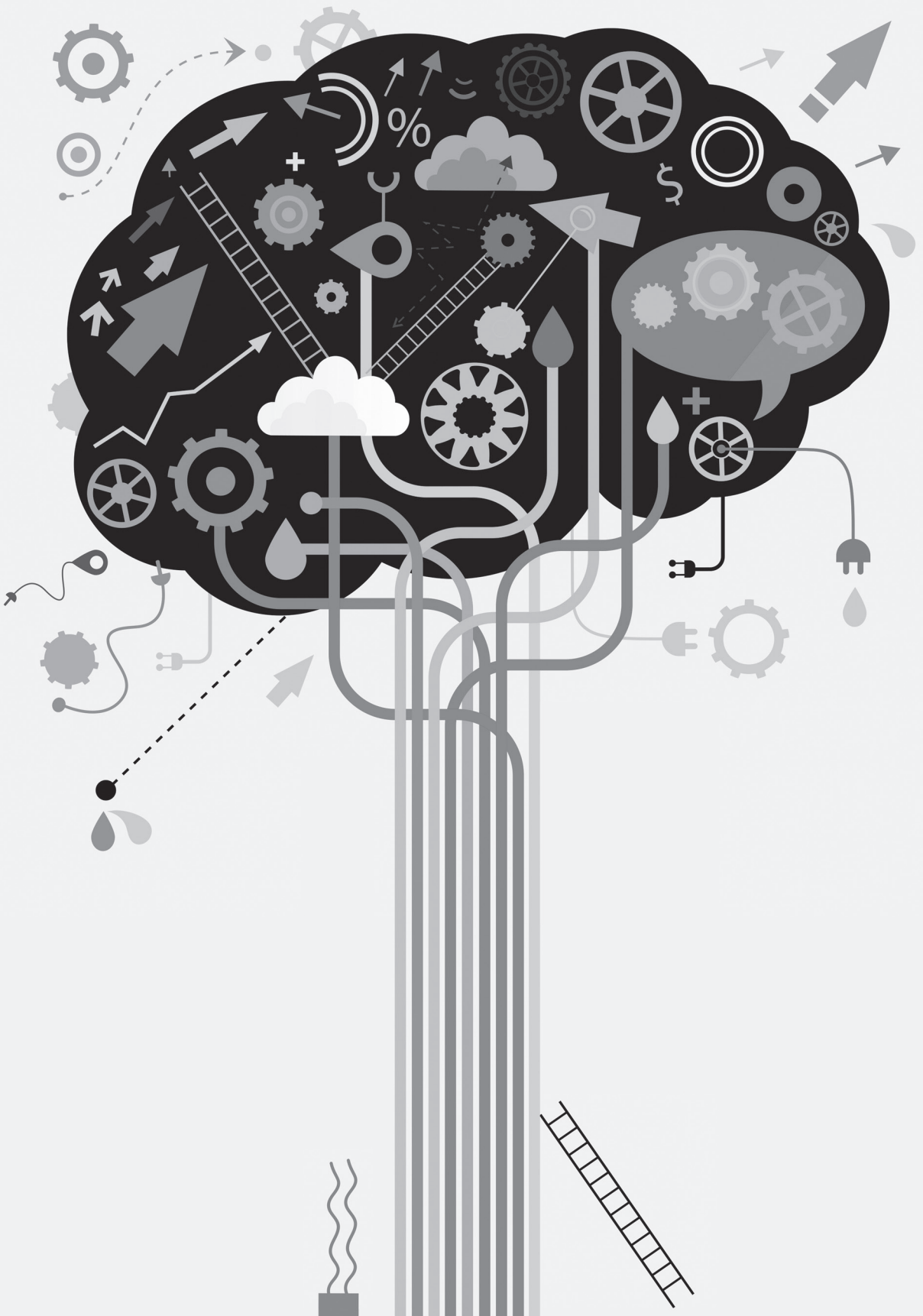
17. https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/
18. http://www.scmagazine.com/intelligence-committee-hosts-cybersecurity-hearing/article/438202
19. http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it
20. http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

quase certamente darão uma ênfase maior nas ações de manipulação ou alteração de dados para comprometer sua integridade… que poderão afetar a tomada de decisões, reduzir a confiança em sistemas ou causar efeitos físicos adversos. A adoção mais ampla de dispositivos de Internet das coisas e inteligência artificial – em ambientes como sistemas de saúde e serviços públicos – só irá agravar esses efeitos potenciais"[21].

Especialistas em segurança estão trabalhando em tecnologias que podem mitigar grande parte desses riscos, mas muitas soluções não poderão ser implantadas sem o envolvimento dos governos. Isso não é algo que o mercado pode resolver. Tal como no caso da privacidade dos dados, os riscos e as soluções são técnicos demais para a compreensão da maioria das pessoas e organizações; empresas podem procurar esconder de seus clientes, seus usuários e o público a insegurança de seus próprios sistemas; as interconexões podem tornar impossível relacionar os violadores de dados com os danos resultantes; e os interesses das empresas muitas vezes não coincidem com os interesses do público[22].

Os governos precisam desempenhar um papel maior: estabeler normas, fiscalizar a conformidade, estimular a implementação de soluções em empresas e redes. E, nos EUA, mesmo que o Plano de Ação Nacional de Cibersegurança do governo federal tenha alguns pontos corretos, está longe de ser suficiente, até porque muitos de nós desconfiam de qualquer solução liderada pelo governo. A próxima pessoa a ocupar a presidência dos EUA será provavelmente forçada a lidar com um desastre na Internet em grande escala que poderá inclusive matar muita gente. Espero que ele ou ela responda com suficiente reconhecimento sobre o que o governo pode fazer e que a indústria não pode, como com a vontade política de fazer isso acontecer.

21. http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf
22. https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html



**Danilo Doneda**, professor de direito civil da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ).

**Virgílio A.F. Almeida**, professor do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG), Brasil, e atualmente professor visitante da Universidade de Harvard.

# O que é a governança de algoritmos?[1]

Os algoritmos são basicamente um conjunto de instruções para realizar uma tarefa, produzindo um resultado final a partir de algum ponto de partida. Atualmente, os algoritmos embarcados em sistemas e dispositivos eletrônicos são incumbidos cada vez mais de decisões, avaliações e análises que têm impactos concretos em nossas vidas.

A vocação que os algoritmos têm para penetrar em diversos âmbitos do nosso cotidiano já é vista como um fato da vida. Eles realizam tarefas que dificilmente pensaríamos em cumprir sem que houvesse um ser humano diante delas. À medida que aumentam a sofisticação e a utilidade dos algoritmos, mais eles se mostram "autônomos", chegando a dar a impressão de que existe alguma "máquina pensante" em alguns dos raciocínios misteriosos que remontam aos primórdios da era da informática. De fato, o termo "algoritmo" costuma ser usado ou mencionado como sinônimo para computador, máquina, código, *software* e por aí vai.

A disponibilidade de um poder computacional e de conjuntos de dados que não param de crescer permite que os algoritmos realizem tarefas de uma magnitude e complexidade insuportável para os padrões humanos. Já mal se pode prever ou explicar seus resultados, nem mesmo por parte de quem os escreve.

Ao mesmo tempo, por mais valiosos que sejam os seus resultados, os algoritmos são capazes de tirar os seres humanos do circuito de seus vários processos decisórios – o que pode ser um risco! Assim é que, para estimular a sua integração em alguns processos sociais

1. Os autores agradecem a Yasodara Córdova por suas valiosas contribuições e sugestões.

e econômicos onde eles podem ser valiosos, talvez seja o caso de elaborarmos instrumentos que permitam algum tipo de governança para os algoritmos. Com isso, talvez possamos evitar uma gama de influências negativas sobre o equilíbrio de poderes em favor daqueles capazes de exercer poder real quanto ao seu uso, maximizando ademais os benefícios que eles podem trazer e reduzindo o seu potencial de riscos. Um exemplo de tal mudança no equilíbrio de poderes é dado por Frank Pasquale ao mencionar que alguns planos de saúde se negaram a aceitar uma mulher que consumia antidepressivos para facilitar o sono. O registro histórico de uso de tais medicamentos, que poderiam até ajudá-la se mantidos rigorosamente com propósitos medicinais, foi apresentado contra ela com base em premissas sobre o uso dessas drogas.[2]

## :: PROBLEMAS E OUTRAS QUESTÕES QUE PODEM ADVIR DOS ALGORITMOS

A complexidade do trabalho dos algoritmos aumenta com o uso cada vez maior das técnicas de aprendizagem automática. Com elas, o algoritmo é capaz de reorganizar seu funcionamento interno com base nos dados que está analisando. Conforme já descreveu Pedro Domingos, os algoritmos de aprendizagem automática são "os algoritmos que fazem outros algoritmos... para que nós não precisemos fazê-los."[3] Em geral, não é tarefa fácil para o cientista que trabalha com dados ou para quem escreve algoritmos descrever os passos que um algoritmo deu para produzir um determinado resultado, nem que seja apenas em termos abstratos.

Portanto, os algoritmos acrescentam um elemento novo à cadeia de informação – sua opacidade – que costuma estar associada à dificuldade de decodificar o seu resultado. Os seres humanos vão ficando cada vez menos capazes de compreender, explicar ou prever o funcionamento interno, os vieses e os eventuais problemas dos algoritmos. Vem aumentando a preocupação diante de situações em que nos fiamos nos algoritmos para a tomada de decisões importantes, até mesmo fundamentais, que afetam nossas vidas ao ponto de muitos trabalhos acadêmicos e campanhas públicas estarem clamando por uma transparência cada vez maior dos algoritmos e sua respectiva responsabilização pelo que fazem.[4]

Ao mesmo tempo, existem justificativas

2. F. Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015
3. P. Domingos, The Master Algorithm, Basic Books, 2015.
4. Electronic Privacy Information Center, Algorithmic Transparency: End Secret Profiling," Epic.org, 2015; https://epic.org/algorithmic-transparency.

não técnicas para a sua opacidade. Algumas dessas justificativas se baseiam em questões relativas à concorrência. Um algoritmo aberto pode colocar a empresa por ele responsável em desvantagem diante da concorrência. Outras se baseiam na propriedade intelectual: há países onde a lei protege o sigilo comercial ou a propriedade intelectual das empresas. Outra razão para não se abrir determinados algoritmos é a possibilidade de algumas pessoas, uma vez cientes das suas características, darem um jeito de "enganar" o algoritmo.[5] Portanto, a opacidade dos algoritmos é uma tendência sustentada por elementos de natureza tanto técnica quanto não técnica.

Mas a opacidade não tem conseguido barrar a ampla adoção dos algoritmos em vários domínios. De fato, eles já não são vistos apenas como o truque que faz funcionar os mecanismos de busca ou como algo que ajuda o e-comércio a arrebanhar as preferências dos clientes. Eles são, sim, componentes essenciais dos veículos autoconduzidos, dos sistemas de previsão de crimes e dos exames para diagnosticar várias doenças, juntamente com uma lista que também não para de crescer com tantas novas aplicações de bastante importância. Algumas dessas aplicações, a propósito, têm impactos diretos sobre a sociedade, como o uso para dar aos dados algum sentido que leve ao desenvolvimento e à ação humanitária, ou o apoio para chegar-se ao diagnóstico médico correto, ou mesmo ao dar mais racionalidade a decisões judiciais.[6]

Os algoritmos surgiram para realizar uma quantidade infindável de tarefas, não só por conta do seu próprio desenvolvimento quanto pela ocorrência de condições que transformaram todo o ambiente em que se situam. Decerto "o algoritmo não é um algoritmo pelo fato de executar (as instruções dadas); ele é um algoritmo pois funciona a partir de um conjunto heterogêneo de atores, que a ele transmitem a exata ação que pressupomos estar sendo por ele realizada."[7]

Esse ambiente contém elementos de grande relevância para a governança dos algoritmos. A bem da verdade, sua governança pode mesmo se basear em ferramentas que atuem não apenas no próprio algoritmo como também sobre elementos do seu ambiente. Dentre tais elementos, os conjuntos de dados talvez sejam os mais fundamentais. Os algoritmos se tornaram muito mais úteis enquanto função

5. T. Gillespie, "The Relevance of Algorithms," Media Technologies: Essays on Communication, Materiality, and Society, T. Gillespie, P. Boczkowski, and K. Foot, eds., MIT Press, 2014, pp. 167–194.
6. http://www.unglobalpulse.org
7. L. Introna, "Algorithms, Governance, and Governmentality: On Governing Academic Writing," Science, Technology, & Human Values, 3 June 2015; doi:10.1177/0162243915587360.

da disponibilidade de dados, que é relevante para seu funcionamento interno. Conforme destacou Tarleton Gillespie, "os algoritmos são inertes, máquinas sem sentido, enquanto não estiverem ligados a bases de dados sobre as quais venham a funcionar."[8]

Os conjuntos de dados são formados a partir de dados coletados em ritmos cada vez mais acelerados, à medida que nossas atividades vão deixando rastros (pensemos nas nossas atividades na Internet) ou vão sendo, quase sempre, monitoradas. Isso leva à oferta de muito mais dados relevantes. E essa questão é absolutamente central à ideia do *"big data"*, o paradigma para dados que costumam "alimentar" algoritmos, com características usualmente chamadas de 3 V's: volume (há mais dados disponíveis), variedade (a partir de uma gama muito maior de fontes) e velocidade (em ritmo crescente, até mesmo em tempo real).[9]

Se os conjuntos de dados forem usados como partes centrais das tarefas a serem realizadas por algoritmos, é importante enfatizar a necessidade de verificar se estão sendo usados dentro da lei e da ética. Em suma, cabe assegurar que os dados sejam legítimos e corretos, que estejam atualizados e não apresentem nenhum viés. Por exemplo, a mineração de dados e outros métodos usados para refinar os conjuntos de dados podem acabar resultando em discriminação. Além disso, a seleção, a classificação, a correlação e outras técnicas costumam repetir vieses ambientais, pois são capazes de imitar as condições sociais e pessoais. Isso nem é uma grande novidade, pois a discriminação estatística (a formação de estereótipos a partir do comportamento "médio" de um grupo discriminado) já é questionada há quatro décadas, mas trata-se de um problema que os algoritmos vêm sempre destacando.[10]

Já foram identificados na literatura alguns riscos que o uso dos algoritmos pode trazer, tais como manipulação, viés, censura, discriminação social, violações da privacidade e dos direitos proprietários, abuso do poder de mercado, efeitos sobre as capacidades cognitivas e uma crescente heteronomia. É preciso considerar um processo de governança para os algoritmos com vistas a tratar desses riscos.

## :: COMO EXERCER A GOVERNANÇA DOS ALGORITMOS

Já foram identificados na literatura alguns riscos que o uso dos algoritmos pode trazer, tais

8. T. Gillespie, op.cit.
9. H. Fang and A. Moro, "Theories of Statistical Discrimination and Affirmative Action: A Survey," NBER working paper no. 15860, Nat'l Bureau of Economic Research, 2010; www.nber.org/papers/w15860.
10. F. Saurwein, N. Just, and M. Latzer, "Governance of Algorithms: Options and Limitations," Social Science Research Network, vol. 17, no. 6, 2015, pp. 35–49.

como manipulação, viés, censura, discriminação social, violações da privacidade e dos direitos proprietários, abuso do poder de mercado, efeitos sobre as capacidades cognitivas e uma crescente heteronomia. É preciso considerar um processo de governança para os algoritmos com vistas a tratar desses riscos.

A governança dos algoritmos pode variar desde os pontos de vista estritamente jurídico e regulatório até uma postura puramente técnica. Ela costuma priorizar a responsabilização, a transparência e as garantias técnicas. A escolha da abordagem de governança pode basear-se em fatores tais como a natureza do algoritmo, o contexto em que ele existe ou uma análise de risco.[11]

Quando se opta por uma abordagem de governança, esta deve buscar geralmente uma redução dos problemas causados pelos algoritmos. Ela deveria tentar preservar a sua eficácia e reduzir os resultados indesejáveis.

Algumas ferramentas de governança não agem sobre o algoritmo mas sim sobre os dados que eles precisam para funcionar. Isso se aplica a algumas das ferramentas que já estão presentes na legislação de proteção de dados que, em alguns países, incluem medidas relativas à transparência e à razoabilidade, aplicáveis diretamente aos algoritmos e às plataformas que dão suporte ao seu funcionamento. Por exemplo, a premissa que as decisões automatizadas devem basear-se em critérios transparentes costuma estar presente em algumas leis de proteção de dados. O mesmo ocorre com o direito de solicitar revisão humana para as decisões tomadas automaticamente.

O uso de algoritmos para regular conjuntos de dados está no cerne da maioria dos arcabouços jurídicos para a proteção dos dados, o que também exige que esses conjuntos de dados sejam legítimos e corretos, cumprindo vários requisitos para atender a esses critérios. Um bom exemplo seria o consentimento para o uso de dados pessoais em várias ocasiões, uma vez que a propriedade é outra das questões que assomam, e identificar conjuntos de dados específicos – de maneira a permitir consentimento para tratamento e uso de dados, seja para uso pessoal ou simplesmente originado por um cidadão – também deveria ser assunto para regulação.

A necessidade de uma prestação de contas e da transparência dos algoritmos costuma ser mencionada como outra abordagem possível. A transparência, como já mencionamos, não é natural a muitos dos algoritmos que estão em uso, por razões técnicas e não técnicas, de forma

11. European Data Protection Supervisor, Towards a New Digital Ethics: Data, Dignity, and Technology, opinion 4/2015, EDPS, 11 Sept. 2015; https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf.

que precisamos de instrumentos de governança para estimular a adoção de certos níveis de transparência, ou de algoritmos abertos.

A prestação de contas, que está ligada à noção de responsabilidade, justeza e processo devido no uso dos algoritmos, também é fundamental e invoca outra questão que deverá ser enfrentada com o uso generalizado de algoritmos: quem fica responsável pelo seu uso? Em quais situações o criador de um algoritmo será responsabilizado e em quais o será uma empresa ou órgão governamental que empregue esse algoritmo?

As garantias técnicas são outro recurso fundamental, de maneira a estabelecer opções para o projeto de algoritmos quanto à mineração e análise de dados com considerações que busquem evitar preconceito, desigualdade ou quaisquer outros resultados tendenciosos. Nesse âmbito, os engenheiros e pesquisadores estão desenvolvendo técnicas para assegurar que os algoritmos e a sua implementação atendam aos padrões de concepção, desempenho e mesmo responsabilização. Num momento seguinte, existem técnicas de auditoria que podem ser úteis para determinar se o algoritmo adere às normas técnicas exigidas.

Uma ferramenta intimamente ligada à auto-regulação é o desenvolvimento de princípios ligados ao uso ético de dados pessoais – o que vem sendo mencionado às vezes como ética do *"big data"*. Mesmo sendo uma variação da abordagem da auto-regulação, alguns órgãos governamentais têm mencionado que talvez esses princípios devam ser desenvolvidos como parte de um novo arcabouço regulatório.[12]

Outro elemento importante é que os algoritmos estão sempre atuando sob as condições do momento, enfrentando situações novas e inéditas que exigem respostas, o que requer o constante acompanhamento dos seus resultados para avaliação. Essa questão é ainda mais importante no caso das técnicas de aprendizado automático.

A implantação de instrumentos de governança para os algoritmos pode ocorrer em vários níveis. Descrevemos aqui uma pequena gama, levando em conta que alguns só seriam considerados se o risco que apresentassem fosse substancial e concreto. Os processos de governança de algoritmos podem variar desde soluções orientadas para o mercado até mecanismos governamentais.

Um conjunto de órgãos de supervisão é necessário para estruturar e implementar a

12. F. Saurwein et al, op.cit.

governança dos algoritmos sobre uma variedade de instrumentos. Fica evidente que não existe uma solução única para todos os casos.

As empresas particulares devem abordar o uso de algoritmos dentro de padrões estabelecidos (se os seus clientes estiverem numa posição tal que possam evitar o uso de algoritmos arriscados embutidos em seus softwares, serviços e produtos), contanto que haja transparência e responsabilização em níveis adequados.

Para que funcione sistematicamente, essa abordagem da iniciativa privada deve ser parte da organização interna das empresas, onde elas definem os padrões que refletem o interesse público e estabelecem um processo de revisão e um órgão interno para garantir a integridade e conformidade com valores de interesse público quando usarem algoritmos.

Essa abordagem também pode basear-se em processos de auto-regulação no âmbito da indústria como um todo onde, por exemplo, padrões coletivos e valores de interesse público são definidos para um setor específico – conforme acontece quando a indústria automobilística define padrões de qualidade e segurança para software embarcado nos automóveis. Um órgão de supervisão específico para a indústria, capaz de assumir a forma de comitês multissetoriais, teria a incumbência de exigir de quem os cria as informações relativas aos algoritmos.

E, por fim, um órgão de supervisão governamental encarregado da regulação dos algoritmos é mais uma possibilidade para o futuro, priorizando requisitos tais como o nível de transparência ou de qualidade de serviço em termos de erros, risco de morte ou lesões causadas por algoritmos ou por software, juntamente com violações de segurança e outros assuntos pertinentes.

> A prestação de contas, que está ligada à noção de responsabilidade, justeza e processo devido no uso dos algoritmos, também é fundamental e invoca outra questão que deverá ser enfrentada com o uso generalizado de algoritmos: quem fica responsável pelo seu uso?

Texto traduzido e adaptado para esta publicação por **Raquel Gatto**, coordenadora de desenvolvimento de capítulos da Internet Society nas Américas.

# Neutralidade da rede
## Um documento informativo
## da Internet Society sobre política pública[1]

*A neutralidade da rede é um tema complexo e controverso e parte importante de uma Internet livre e aberta. Permitir o acesso, a possibilidade de escolha e a transparência das ofertas de Internet garante aos utilizadores beneficiar de pleno acesso aos serviços, aplicações e conteúdos disponíveis na Internet.*

### :: INTRODUÇÃO

A Internet tornou-se uma ferramenta indispensável para utilizadores por todo o mundo e um facilitador fundamental da inovação e do crescimento econômico. É pouco provável que a procura por ligações à Internet com maior largura de banda diminua. Mesmo agora, alguns operadores de rede têm de usar técnicas de gestão de congestionamentos e de modelagem de tráfego para manter as suas redes funcionando sem problemas.

Como resultado, alguns analistas temem que os operadores de rede sejam tecnicamente capazes de usar práticas de gestão de tráfego para dar tratamento preferencial a determinados fluxos de dados. Outros receiam que práticas destinadas a aumentar as receitas possam

1. Publicado originalmente em http://www.internetsociety.org/policybriefs/networkneutrality

bloquear conteúdos considerados como concorrentes ou dar vantagens injustas à certos conteúdos sobre outros. Os analistas consideram estas práticas problemáticas, especialmente quando discriminam intencionalmente determinados tipos de fornecimento de conteúdos em detrimento dos utilizadores finais. Esta situação gerou maior preocupação pública no sentido de que este tipo de prática coloca em perigo os princípios de abertura e transparência da Internet.

Nos debates sobre política pública e regulamentação, o termo "neutralidade da rede" é frequentemente utilizado como um rótulo amplo. No entanto, este termo pode ter diferentes significados segundo o ponto de vista de quem o utiliza. Por exemplo, as discussões sobre a neutralidade da rede abordam muitas vezes preocupações relacionadas com a liberdade de expressão, a concorrência de serviços e a possibilidade de escolha dos utilizadores, o seu impacto na inovação, práticas de gestão de tráfego não discriminatório, fixação de preços e modelos de negócio.

A partir deste diálogo da neutralidade da rede, alguns acreditam que é necessário implementar políticas e medidas regulamentares para preservar uma Internet aberta e para garantir que esta continue a ser um motor para a inovação, a liberdade de expressão e o crescimento econômico. A Internet Society acredita que concentrar a atenção no resultado das práticas de gestão de rede, e não nas medidas técnicas ou políticas empregadas para obter esse resultado, permitirá a flexibilidade necessária nas operações de rede.

## :: CONSIDERAÇÕES FUNDAMENTAIS

Um elemento-chave da arquitetura da Internet é que os dados dos usuários são transmitidos em datagramas padronizados de informações sem ter em conta o seu conteúdo, os emissores ou destinatários. Esta abordagem não discriminatória face ao tráfego de Internet é uma premissa central do funcionamento da rede, permitindo que os dados trafeguem sem impedimento quanto à natureza dos mesmos. Basicamente, esta abordagem de interligação aberta é um dos pilares que sustenta a Internet e que permitiu o seu êxito.

No entanto, na prática, os datagramas são por vezes tratados de forma diferente para fazer frente ao congestionamento da rede, às restrições de recursos, aos acordos comerciais e a outras considerações práticas relativas ao funcionamento da rede. Algumas operadoras de redes argumentam que os atuais recursos de largura de banda e infraestrutura estão congestionados e que para solucionar o problema e oferecer uma boa qualidade de serviço aos clientes é necessária uma intervenção significativa sobre a gestão do tráfego nas redes.

Estas práticas de gestão de redes motivam o debate sobre se constituem ou não uma forma de tratamento justa e imparcial dos dados que viajam através da Internet. Também se questiona até que

> Um elemento-chave da arquitetura da Internet é que os dados dos usuários são transmitidos em datagramas padronizados de informações sem ter em conta o seu conteúdo, os emissores ou destinatários. Esta abordagem não discriminatória face ao tráfego de Internet é uma premissa central do funcionamento da rede, permitindo que os dados trafeguem sem impedimento quanto à natureza dos mesmos.

ponto as atividades de gestão de redes constituem práticas discriminatórias que potencialmente restrinjam o acesso a conteúdos e limitem a liberdade de expressão dos utilizadores da Internet.

Do ponto de vista operacional da rede, muitas das preocupações relacionadas com a neutralidade da rede são o resultado de uma questão fundamental sobre a própria concepção da Internet: a abordagem do "melhor esforço" para mover dados através das redes. Esta abordagem significa que se aplicam os melhores esforços do sistema para entrega de todos os dados ao seu destino em função da disponibilidade dos recursos da rede. Contudo, esta abordagem não oferece um tratamento preferencial a um fluxo de dados sobre outro. Pelo contrário, esforça-se para tratar todos os dados de uma forma neutra e sem discriminação.

No entanto, nas operações do dia-a-dia, as operadoras de rede administram o tráfego de dados através de diferentes redes, ao mesmo tempo que dão resposta a eventos envolvendo segurança, falhas e congestionamentos imprevistos. Ainda que as práticas de gestão de dados sejam necessárias para o funcionamento normal da Internet, existe a preocupação de que quaisquer manipulações do fluxo de dados de rede possam tratar certos dados e conteúdos de maneira prejudicial – o que pode implicar em práticas de gestão de dados que conduzam potencialmente a práticas comerciais anticoncorrenciais ou a outras consequências socialmente nocivas.

## :: OBSTÁCULOS

Como se observa, existem diferenças de opinião sobre quais práticas de gestão de rede constituem atividades de rotina e são aceitáveis, e quais são excessivas e podem resultar em discriminação prejudicial, tanto para os usuários como para os fornecedores de conteúdos. Abaixo são descritos cinco desafios específicos geralmente discutidos nos diálogos sobre a neutralidade da rede:

**1. Bloquear e filtrar:** Bloquear ou filtrar conteúdos é uma prática segundo a qual se nega acesso aos utilizadores finais a certos conteúdos online em função de determinados controles regulamentares ou objetivos de negócio dos provedores de serviços Internet, ou dos operadores de infraestrutura de rede, para favorecer os seus próprios conteúdos. Alguns consideram que a filtragem seletiva dos conteúdos de Internet vai contra os princípios de acesso livre e gratuito, especialmente quando favorece os serviços de um provedor. Outros veem o bloqueio e filtragem como métodos necessários para proteger crianças e adolescentes contra conteúdos censuráveis, ou para limitar a proliferação de conteúdos ilegais online.

**2. Vias rápidas da Internet:** A expressão vias rápidas da Internet se refere à prática de dar tratamento preferencial de rede a determinados fluxos de dados com base em acordos comerciais entre operadores de Internet. Por exemplo, conteúdos de vídeo específicos podem ser fornecidos com maior rapidez através de uma rede mediante acordos comerciais entre as operadoras de rede. Há quem veja nestes acordos uma prática discriminatória inaceitável, dando tratamento preferencial a alguns dados na rede e potencialmente degradando o desempenho de outros. No entanto, outros veem as "vias rápidas" como uma maneira eficaz de entregar conteúdos aos usuários com uma melhor qualidade de serviço.

**3. Estrangulamento:** O termo estrangulamento se refere a certas práticas comerciais que reduzem as taxas de transferência dos conteúdos entregues aos usuários finais. O estrangulamento pode incluir técnicas como limitar especificamente as velocidade de envio ou transferência dos usuários para certos tipos de fluxos de dados, como no caso das práticas de gestão de tráfego entre pares *(peer-to-peer)*. Alguns veem o estrangulamento como um meio necessário para evitar o congestionamento e melhorar o desempenho da rede. Outros consideram que estas práticas são controversas, especialmente quando não são divulgadas claramente ou quando os operadores discriminam injustamente determinados fluxos de dados.

**4. Serviços de taxa zero** *(zero-rating)***:** O termo descreve uma prática comercial mediante a qual determinados conteúdos são entregues ao usuário final a um custo consideravelmente reduzido, ou até mesmo de forma gratuita. Neste cenário, o provedor de serviços de Internet normalmente subsidia o custo do acesso à Internet em troca de vantagens de mercado tangíveis ou intangíveis. Estas vantagens de mercado podem traduzir-se em aumento da base de assinantes, direitos de acesso preferencial para o fornecimento de serviços de Internet, ou a possibilidade de lucrar com os dados recolhidos dos assinantes dos serviços. Há um debate sobre se estes serviços discriminam os fluxos de dados

que não foram fornecidos sob um serviço de taxa zero. Da mesma forma, não está claro se o fato de fornecer apenas um subconjunto do acesso pleno à Internet no âmbito de um serviço de taxa zero a quem de outra forma não teria acesso à Internet é melhor ou pior do que o dano potencial resultante de um acesso limitado à Internet. Este debate é particularmente importante nos países em desenvolvimento, onde foram levantadas preocupações sobre as potenciais desvantagens e consequências involuntárias dos serviços de taxa zero.

**5. Concorrência no mercado:** A existência de uma concorrência saudável no mercado é um tema frequente nas discussões sobre neutralidade da rede. Nos mercados onde as opções de serviços de Internet a preços acessíveis são limitadas, os usuários estão potencialmente mais vulneráveis a restrições de acesso aos conteúdos disponíveis ou à redução do desempenho da rede. Para os provedores de serviços de Internet, a concorrência no mercado é útil ao oferecer aos consumidores a possibilidade de escolha e estímulo à inovação entre os fornecedores de serviços. Além disso, a promoção da concorrência no fornecimento de acesso à Internet permite que os usuários possam escolher entre diferentes serviços e experiências online.

## :: PRINCÍPIOS DE ORIENTAÇÃO

> Com incidência das práticas nos resultados de gestão de redes, a abordagem regulamentar e das políticas deve reger-se pelo princípio geral de abertura, bem como por características que promovam o acesso, a possibilidade de escolha e a transparência. Esses valores fundamentais são representados pelos seguintes princípios orientadores gerais: o acesso a serviços de Internet, aplicações, sites e conteúdos aprimora a experiência do usuário e o potencial da Internet para impulsionar a inovação, a criatividade e o desenvolvimento econômico. As práticas que limitem ou bloqueiem o acesso a conteúdos da Internet constituem uma preocupação primordial.

> Que os usuários escolham e controlem as suas atividades online, incluindo os seus fornecedores, serviços e aplicações – reconhecendo as limitações legais e técnicas – é importante para uma interligação aberta. Para alguns usuários, a seleção de fornecedores e serviços online é limitada, tornando-os particularmente vulneráveis a práticas de gestão de rede potencialmente discriminatórias.

> A transparência das decisões sobre os fluxos de dados é importante para um acesso justo e imparcial aos recursos da Internet. O acesso transparente a informações precisas sobre a largura de banda e as políticas de gestão de rede permite aos utilizadores tomar decisões informadas sobre os seus serviços de Internet.

Em termos mais específicos, estes princípios

orientadores gerais traduzem-se no seguinte:

> Ofertas de serviços competitivos e transparentes que permitam ao usuário tomar decisões informadas ao escolher um fornecedor e um nível de serviço. Isto inclui a divulgação de informações, tanto públicas como contratuais, acerca das velocidades médias que os operadores de rede realmente oferecem no serviço de Internet aos seus clientes, durante os períodos normais e de pico, bem como as limitações que aplicam quanto ao volume de dados.

> Acesso livre a uma variedade de serviços, aplicações e conteúdos oferecidos de forma não discriminatória.

> Práticas razoáveis de gestão de rede que não afetem a concorrência nem sejam prejudiciais. A clarificação dos limites das práticas razoáveis de gestão de rede seria benéfica.

> Informações compreensíveis e acessíveis às quais está sujeito um assinante, sobre as limitações dos serviços, bem como as restrições relativas à rede e ao tráfego.

> Monitorização regulamentar da prestação de serviços de Internet para assegurar que não ocorra uma degradação da qualidade. A avaliação da qualidade deve se basear em medições e normas entendidas de maneira generalizada, incluindo as medições em grande escala do desempenho da banda larga (LMAP) e métricas de desempenho para IP (IPPM) dos grupos de trabalho do *Internet Engineering Task Force (IETF)*.

> Iniciativas educativas para informar os utilizadores sobre o que implicam as práticas de gestão de rede e como escolher ofertas de serviços que satisfaçam às suas necessidades.

É importante notar que nenhum dos princípios acima exclui a possibilidade de usar práticas

É importante notar que nenhum dos princípios acima exclui a possibilidade de usar práticas razoáveis de gestão de rede. Há uma clara necessidade de gerir as redes para manter um bom funcionamento da Internet e fornecer aos utilizadores serviços inovadores e de alta qualidade.

razoáveis de gestão de rede. Há uma clara necessidade de gerir as redes para manter um bom funcionamento da Internet e fornecer aos utilizadores serviços inovadores e de alta qualidade. Na verdade, as abordagens regulamentares que afetam a sustentabilidade da Internet aberta global devem ter em conta a realidade técnica de como funcionam e são geridas as redes.

Mais importante ainda, um ambiente de acesso à Internet caracterizado pela possibilidade de escolha e transparência permite aos utilizadores controlar a sua experiência de Internet e capacitando-os para se beneficiarem e participarem nela plenamente.

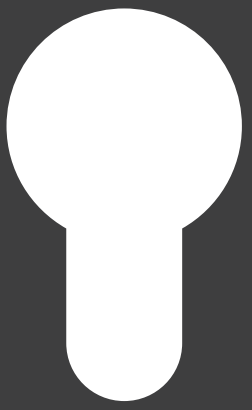
## Recursos adicionais

A *Internet Society* publicou uma série de documentos e conteúdos adicionais relacionados com este tema. Estes estão disponíveis para acesso gratuito no portal da *Internet Society*.

*"Open Inter-networking - Getting the fundamentals right: access, choice, and transparency"*, 21 de fevereiro de 2010, http://www.internetsociety.org/open-inter-networking-getting-fundamentals-right-access-choice-and-transparency

*"Network neutrality - let those packets flow"*, 30 de março de 2015, https://www.internetsociety.org/blog/asia-pacific-bureau/2015/03/network-neutrality-%E2%80%93-let-those-packets-flow

*"Zero rating: enabling or restricting Internet access?"* 24 de setembro de 2014, http://www.internetsociety.org/blog/asia-pacific-bureau/2014/09/zero-rating-enabling-or-restricting-internet-access



# Carta aberta

## aos líderes de governos do mundo

*Esta carta é uma iniciativa da organização não-governamental Access Now, que atua em defesa dos direitos digitais ao redor do mundo, e desde janeiro de 2016 está sendo enviada para líderes de diversos países que discutem legislações ou outras medidas que podem minar o uso da criptografia. Além de fundamentais para a comunicação segura na rede, a criptografia e o anonimato permitem a privacidade necessária para a liberdade de expressão e opinião na era digital, como ressaltou o Relator Especial da ONU para a Liberdade de Expressão, David Kaye. A carta conta com o apoio de mais de 150 organizações ao redor do mundo e já foi enviada para governos de países como Estados Unidos, Reino Unido, Austrália, França e aos membros da União Europeia. Ela segue aberta para adesão em https://www.SecureTheInternet.org*

Exortamos as senhoras e senhores a proteger a segurança de seus cidadãos, sua economia e seu governo, apoiando o desenvolvimento e a utilização de ferramentas e tecnologias de comunicações seguras, rejeitando políticas que possam impedir ou prejudicar o uso de criptografia forte e instigando outros líderes a fazerem o mesmo.

Ferramentas, tecnologias e serviços de criptografia são essenciais para proteger nossa infraestrutura digital de comunicações pessoais contra danos e defendê-la de acessos não autorizados. A capacidade de se desenvolver e utilizar criptografia livremente consiste na pedra fundamental para a economia global de hoje. O crescimento econômico na era digital é alimentado pela capacidade de confiar e autenticar nossas interações e de se comunicar e realizar negócios com segurança, dentro e através das fronteiras.

Alguns dos técnicos e especialistas em criptografia mais notáveis do mundo explicaram recentemente que leis ou políticas que minam a criptografia podem "forçar um retrocesso nas melhores práticas implementadas para tornar a Internet mais segura", "aumentar substancialmente a complexidade do sistema" e os custos associados e "criar alvos concentrados que podem atrair atores maliciosos"1. A ausência de criptografia facilita o acesso a dados pessoais sensíveis, incluindo informações financeiras e de identidade, por parte de criminosos e outros agentes maliciosos. Uma vez obtidos, esses dados sensíveis podem ser vendidos, expostos publicamente ou utilizados para chantagear ou constranger as vítimas. Além disso, dispositivos ou equipamentos com criptografia frágil são os principais alvos de criminosos.

O Relator Especial das Nações Unidas para a Liberdade de Expressão apontou que "a criptografia, o anonimato e os conceitos de segurança a eles relacionados, oferecem a privacidade e segurança necessárias para o exercício do direito à liberdade de opinião e de expressão na era digital". Ao avançarmos para conectar o próximo bilhão de usuários, restrições à criptografia em qualquer país provavelmente terão um impacto global. Ferramentas e tecnologias de criptografia ou anonimização permitem que advogados, jornalistas, denunciantes e organizadores comuniquem-se livremente através das fronteiras e trabalhem para melhorar suas comunidades. Elas também garantem aos usuários a integridade de seus dados e autentica indivíduos, empresas e governos.

Encorajamos o apoio à proteção e segurança dos usuários através do fortalecimento da integridade das comunicações e sistemas. Todos os governos devem rejeitar leis, políticas ou outros mandatos ou práticas, incluindo acordos secretos com empresas, que limitem o acesso ou prejudiquem a criptografia e outras ferramentas e tecnologias seguras de comunicação. Os usuários devem ter a opção de usar – e as empresas a opção de fornecer – a criptografia mais forte disponível, incluindo a criptografia fim-a-fim (end-to-end), sem medo de que os governos

obrigarão o acesso ao conteúdo, metadados ou chaves de criptografia sem o devido processo e o respeito aos direitos humanos. Assim:

> Governos não devem, de nenhuma maneira, banir ou limitar o acesso do usuário à criptografia ou proibir a aplicação ou uso de criptografia por grau ou tipo;

> Governos não devem tornar obrigatória a concepção ou implementação de backdoors ou vulnerabilidades em ferramentas, tecnologias ou serviços;

> Governos não devem exigir que ferramentas, tecnologias ou serviços sejam concebidos ou desenvolvidos para permitir o acesso de terceiros a chaves de criptografia ou a dados não criptografados;

> Governos não devem tentar enfraquecer ou minar os padrões de criptografia ou influenciar intencionalmente o estabelecimento de padrões de criptografia, exceto para promover um nível mais elevado de segurança da informação. Nenhum governo deve ordenar que algoritmos, padrões, ferramentas ou tecnologias de criptografia sejam inseguros; e

> Governos não devem, seja por acordos privados ou públicos, obrigar ou pressionar qualquer entidade para exercer qualquer atividade que seja incompatível com os princípios acima.

A existência de criptografia forte, assim como de ferramentas e sistemas seguros que se apoiem nela, são fundamentais para aprimorar a segurança no ciberespaço, fomentar a economia digital e proteger os usuários. Nossa capacidade de potencializar o uso da Internet para o crescimento global e prosperidade e como ferramenta para organizadores e ativistas requer a capacidade e o direito de se comunicar de forma privada e segura através de redes confiáveis.

Estamos ansiosos para trabalhar juntos em direção a um futuro mais seguro.

poliTICs 24

EDITOR **CARLOS A. AFONSO** • COORDENAÇÃO TÉCNICA **PAULO DUARTE** • TRADUÇÕES **RICARDO SILVEIRA** • REVISÃO **THIAGO NOVAES** • PROJETO GRÁFICO **MONTE DESIGN** • CAPA, DIAGRAMAÇÃO & IMAGENS **PAULO DUARTE** • VERSÃO ONLINE **LIQUID VISION**



Esta é uma publicação do Instituto Nupef - **https://nupef.org.br**
As versões digitais de todas as edições da revista estão disponíveis em **https://politics.org.br**
Entre em contato conosco por e-mail: **politics@nupef.org.br**

**APOIO:** FORDFOUNDATION nic.br



A tiragem das edições da poliTICs é pequena. Se você quiser receber gratuitamente a edição impressa, envie um email para politics@nupef.org.br com seu nome, endereço completo - incluindo o CEP - e a sua área de atuação.

A poliTICs procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro).

Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuizo ao conteúdo, aderência ao SI. Para mais informação: http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp

Os originais foram compostos com OpenOffice 4.X e GNU/Linux

**ISSN: 1984-8803**

instituto nupef

Todas as edições da poliTICs estão disponíveis em

https://politics.org.br

https://nupef.org.br
https://rets.org.br
https://tiwa.org.br

**O Instituto Nupef é uma organização sem fins de lucro, dedicada à reflexão, análise, produção de conhecimento e formação, principalmente centradas em questões relacionadas às Tecnologias da Informação e Comunicação (TICs) e suas relações políticas com os direitos humanos, a democracia, o desenvolvimento sustentável e a justiça social.**

**Além de realizar cursos, eventos, desenvolver pesquisas e estudos de caso, o Nupef edita a poliTICs, a Rets (Revista do Terceiro Setor) e mantém o projeto Tiwa – provedor de serviços internet voltado exclusivamente para instituições sem fins lucrativos – resultado de um trabalho iniciado há 21 anos, com a criação do Alternex (o primeiro provedor de serviços internet aberto ao público no Brasil). O Tiwa é um provedor comprometido prioritariamente com a privacidade e a segurança dos dados das entidades associadas; com a garantia de sua liberdade de expressão; com o uso de software livre e de plataformas abertas.**

instituto nupef

**https://nupef.org.br**
**https://politics.org.br**
**https://rets.org.br**
**https://tiwa.org.br**