O Estado da Internet 2020

Manuel da Costa Cabral // ECPMF & OBCT Transeuropa // Alexander Hanff // Geoff Huston // Anna Dorothea Ker // Clara Alves Rodrigues // Darren Thackeray

Maio | 2020

Edição
Pedro Fonseca

Tradução
André Marques
Conclusão das Letras

Paginação
Sara Dias

Fotografias
Capa | Markus Spiske
01 | John Towner
02 | Franck V.
03 | XVIIIZZ
04| Rodolfo Cuadros
06 | Franki Chamaki
07 | Arthur Mazi
09 | Fabio Bracht
10 | TiagoJoaoReis
11 | Portugal Telecom/Altice

Produção
Conclusão das Letras

Patrocínio

Introdução: dos conteúdos às condutas

O fio condutor destes textos sobre o estado da Internet em 2020 são os dados e o seu aproveitamento benéfico ou com fins perniciosos. Apesar das diversas instâncias regulatórias, supranacionais, a sociedade não quer ou não consegue impor um efectivo controlo aos novos desafios penalizadores para o ser humano, nomeadamente em termos de privacidade.

Parece um regresso às origens. A Internet começou como clube restrito de militares e investigadores, passou a serviço público caro e lento, a necessitar de constantes desenvolvimentos físicos e manutenção onerosa. Assegurada esta componente técnica, muito do que ali circula é de empresas com cientistas de dados a exercerem um apertado controlo sobre os cidadãos, escudadas num secretismo quase militar.

Os dados são transmitidos, processados e direccionados para moldar o estado de espírito e melhorar o (conhecimento potencial do) ser humano. Os abusados dados pessoais vivem em plataformas que fomentam "primaveras" de liberdade mas são constantemente roubados e vendidos no mercado negro, limitam a liberdade de expressão e a partilha livre de conteúdos e ideias.

Um exemplo? Em 2019, os serviços online foram "deliberadamente" cortados mais de 200 vezes em 33 países, contabilizou a organização Access Now. Outro? Os processos judiciais de litigância em jurisdições onde os dados são acedidos (não produzidos), com o fenómeno dos SLAPPS sem resolução legislativa à vista.

É uma Inquisição do século XXI, em defesa de excepcionalismos religiosos, políticos (para controlo estatal) ou financeiros, num ambiente pouco ético em que as empresas defendem a isenção do controlo regulatório e fiscal, e os políticos legisladores cedem-lhes esse estatuto esperando retorno.

Os dados são neutros. Os perigos e os benefícios emergem quando são agregados. Se forem mal geridos, vão continuar a servir para fins e objectivos de duvidosa utilidade. Em sentido contrário, podem contribuir realmente para melhorar o ser humano. Cabe a este escolher o caminho.

Pedro Fonseca

“Gangsters digitais”: são o Facebook e a Google um desafio para a democracia?

Clara Alves Rodrigues

Especialista em International Technology Law na Vrije Universiteit Amsterdam. *Texto publicado originalmente no Amsterdam Law Forum, Vol 11, No 3 (2019),*

Este artigo analisa como o Facebook e os modelos de negócios inovadores da Google podem ser uma ameaça para a democracia. A sua concentração económica tornou-os suficientemente poderosos para imporem um determinismo tecnológico: toda a tecnologia que acontece deve acontecer como acontece e não poderia ser de outra forma. Esse determinismo viola activamente o princípio do governo representativo porque concede poder regulatório a empresas privadas não eleitas. Além disso, a autonomia individual dos cidadãos é violada ao exigir consentimento para acordos injustos para os utilizadores que incorporam uma vigilância indiscriminada e o "data mining" [tratamento de dados], capazes de prever e modificar comportamentos. Este artigo visa gerar um debate público sobre os desafios do Facebook e da Google para a democracia.

I. Introdução

Este artigo tem como objectivo analisar se as disrupções que o Facebook e a Google fizeram na lei e na tecnologia estão a afectar os princípios democráticos. Ou seja, avaliar se essas empresas estão a ir contra os princípios básicos do governo representativo e da autogovernança individual. O princípio de um governo representativo respeita o direito igual de todos os cidadãos participarem nas decisões que os governam. O princípio da autogovernança ou autodeterminação relaciona-se com o direito das pessoas a decidirem o seu destino.[1] Um direito não pode existir sem o outro. Os cidadãos não podem participar igualmente numa decisão se não tiverem o direito à escolha. Os cidadãos não têm o direito de escolher se não podem participar igualmente da decisão de quem ou do que os governa.

Nesse sentido, este artigo examinará se essas empresas representam uma ameaça à democracia, observando a lei aplicável e a sua história; analisando a jurisprudência existente e o ambiente económico actual; e elaborando provas empíricas.

Embora possa haver outras empresas de tecnologia que estão a subverter a lei e, consequentemente, os princípios da democracia, este artigo concentra-se no Facebook e na Google devido ao seu modelo de negócios excepcionalmente perigoso. Esse modelo de negócios inovador é o que Shoshana Zuboff[2] chama de "Surveillance Capitalism"[3] ["Capitalismo de Vigilância"] e será examinado mais adiante neste artigo.

A primeira secção deste artigo analisará como a lei hibernou perante as novas tecnologias e como isso contraria o princípio do governo representativo. A hibernação da lei é dupla. Primeiro, este artigo examinará como a lei não se adaptou ao crescimento económico exponencial do Facebook e da Google. Esse crescimento exponencial tem a ver com a estrutura das duas empresas e será analisado à luz da regulamentação aplicável ao direito da concorrência e da sua história. Exemplos relevantes da jurisprudência seguirão a investigação doutrinária e a história legal do direito da concorrência. Tim Wu[4] analisa isso no seu livro "The curse of Bigness". [5] O artigo examinará o perigo dessas empresas e reflectirá sobre como a legislação actual da concorrência se deve adaptar às rupturas que causaram. Em segundo lugar, a hibernação será analisada da perspectiva das tecnologias que a Google e o Facebook criaram per se e como a lei está a ter dificuldades para se adaptar a elas. Essa hibernação tem a ver com "o que" as empresas criaram e "como" estão

a subverter a lei. O Facebook e a Google declararam que a lei não as pode acompanhar como forma de defender o determinismo tecnológico. No seu próximo livro, o professor Fairfield fornecerá uma análise aprofundada de como isso é teórica e empiricamente falso e explicará como a questão do determinismo tecnológico deve ser abordada.[6] Com base nas ideias do professor Fairfield, este artigo abordará a questão da adaptação legal.

A segunda parte deste artigo analisará como o comportamento descontrolado do Facebook e do Google pode representar uma ameaça à autonomia dos indivíduos. Como essas duas empresas quase monopolizaram o mercado dos mecanismos de pesquisa e de media social, elas são as únicas que prestam um serviço essencial no século XXI.[7] A primeira interferência é estabelecida, portanto, na pouca escolha que os cidadãos têm em contratar o Facebook e a Google e a falta de livre arbítrio no que o contrato estipula. A segunda interferência no direito de autonomia ou liberdade do indivíduo é o modelo de negócios inovador que o Facebook e a Google introduziram. Esse modelo de negócios funciona extraindo e analisando os dados dos seus utilizadores para prever o seu comportamento.

Consequentemente, devido às suas correctas previsões, pode modificar o comportamento. A manipulação do comportamento humano é indiscutivel--mente a violação definitiva da autonomia individual, porque leva a pessoa a tomar uma decisão sem conhecimento de nenhuma interferência. Com base nas ideias de Shoshana Zuboff no seu recente livro "Surveillance Capitalism", este artigo estudará a base desse modelo de negócios e as suas implicações.

Com fundamentação nas ideias de Shoshana Zuboff, Tim Wu e Joshua Fairfield, este texto tem como objectivo analisar o modo como a tecnologia foi desenvolvida, bem como a sua legitimidade e perigos. Ao fornecer uma revisão das implicações da tecnologia moderna, deseja proporcionar um futuro mais ponderado que esteja em conformidade com os princípios da democracia e que proteja os direitos e as liberdades dos seus cidadãos.

II. Princípio do governo representativo

II.1. Qual é a preocupação com a concentração económica?

O direito da concorrência deve ser uma verificação do poder privado. Visa garantir que o crescimento económico concentrado não se traduz num poder privado que possa controlar as condições em que o mercado opera e exerça influência política. A Comissão Europeia adoptou uma abordagem mais económica nos últimos anos. Essa abordagem reduziu o número de fusões proibidas.[8] Quando as empresas querem fundir-se, notificam a Comissão para rever e aprovar a transação. No entanto, o mecanismo de referência opera apenas se a fusão atingir os limites de "turnover" [liquidez de activos das empresas] estabelecidos na regulação.[9] Como os serviços são dados gratuitamente no mundo da tecnologia da informação (TI) e os dados pessoais são vistos como uma moeda, isso leva a uma falta de aplicação da lei. Por exemplo, nem a aquisição do Instagram pelo Facebook nem a aquisição da Waze pela Google atingiram os limites de "turnover", pelo que nenhum foi referido à Comissão.[10]

A fusão do WhatsApp com o Facebook também foi autorizada pela Comissão

Europeia. A WhatsApp é uma das aplicações de mensagens mais usadas no mundo. No Reino Unido, por exemplo, é a aplicação de mensagens com mais "downloads" e os seus utilizadores mensais ultrapassam os do Facebook e do Messenger do Facebook.[11] No entanto, a Comissão Europeia argumentou que estavam em mercados diferentes, já que o Facebook tinha anúncios e o WhatsApp não. A Comissão justificou ainda a decisão com a existência de concorrência (como a aplicação Telegram), sobre o facto de os consumidores usarem mais de uma aplicação - o que significa que o efeito de rede ["network effect"] não é um grande obstáculo à entrada ou possibilita uma grande expansão após a fusão. [12]

No entanto, o Facebook afirmou que não havia tecnologia disponível para corresponder aos utilizadores e criar uma plataforma unificada de mensagens. Mais tarde, o Facebook foi multado porque, à época, já havia pessoas a trabalhar em maneiras de juntar o Facebook e o WhatsApp.[13] Isso não deveria ser uma surpresa, dado o lucro substancial a poder ser obtido com a transação. O WhatsApp foi avaliado em 10 milhões de euros e o Facebook comprou-o por 19 mil milhões de euros.[14] Pergunte-se a qualquer criança que tenha jogado o jogo Monopoly e ela entenderia o movimento claro do poder e os riscos de possuir mais do mesmo tipo de propriedade. Inevitavelmente, todos passarão pela sua propriedade, o que facilita o investimento na sua exploração.

Exemplos do passado iluminam a importância do controlo do poder privado. A Era Dourada ["Gilded Age"] - o final do século XIX nos Estados Unidos - foi um período caracterizado tanto por um significativo crescimento económico quanto por uma grande desigualdade de rendimentos. Empresas como a Standard Oil e a US Steel compraram empresas para estabelecerem os seus "trusts" [entidades gestoras] e garantirem os seus monopólios. A ideologia política do "darwinismo social" - ou sobrevivência dos mais aptos - permitiu que os monopólios fizessem o que queriam e justificassem comportamentos anticompetitivos que destruíam qualquer concorrência. Por exemplo, John Pierpont Morgan criou a US Steel pagando ao seu concorrente, Andrew Carnegie, tanto dinheiro que ele se tornou o homem mais rico do mundo. A Standard Oil usou preços predatórios e subornou o governo para aprovar leis para excluir qualquer concorrente potencial.[15] A Era Dourada foi seguida pelo período de "trustbuster" [fim dos "trusts"], iniciado pelo Presidente Roosevelt. Roosevelt entendeu que uma oligarquia era contrária aos princípios básicos da democracia. Como o poder económico se traduzia inevitavelmente em poder político nos Estados Unidos, ele era transferido de representantes eleitos para as empresas.[16]

O direito da concorrência deve ser sobre muito mais do que preços e argumentos económicos. A democracia é um sistema que descentraliza o poder e restringe a autoridade para que os cidadãos tenham poder sobre quem governa o quê. Se um poder económico é excessivamente concentrado em poucas empresas, o bem-estar dos cidadãos fica ao critério privado de algumas.[17] A reduzida escolha num mercado oligárquico significa que os cidadãos não podem optar por não usar os serviços das poucas empresas disponíveis. Consequentemente, o produto não existe pelas necessidades dos consumidores mas imposto pelas demais empresas devido à falta de concorrência. Além disso, para manter o seu domínio, como visto acima, elas visam eliminar a concorrência potencial investindo em barreiras à entrada ou comprando novas empresas.

O Facebook comprou 80 empresas, incluindo o Instagram e o WhatsApp[18]. A Google comprou uma quantidade espantosa de 235 empresas, incluindo YouTube, Double Click, Waze, Motorola Mobility e Deep Mind.[19]

Consequentemente, é criado um ciclo vicioso de falta de concorrência em que as empresas consolidadas compram novas empresas e ganham ainda mais poder de mercado. Para mais, preservam os desejos das grandes empresas em inovação e tecnologia, uma vez que as pequenas empresas ou as startups sabem que a única maneira de obter sucesso é criar um produto que seja adquirido por uma grande empresa. Consequentemente, até as novas empresas agem de acordo com as vontades do Facebook e da Google, e não dos consumidores.[20] Essa concentração é especialmente relevante para a Google e o Facebook porque eles estão no controlo de como e com que finalidade a tecnologia é criada. As implicações desse controlo serão discutidas na próxima secção.

Além disso, a concentração também facilita a organização de objectivos políticos que criam uma pressão política antidemocrática. Notícias afirmam que o Facebook gastou 12,62 milhões de dólares e a Google 21,2 milhões de dólares em lobby junto do governo dos EUA em 2018 para influenciar legisladores e reguladores sobre regras da privacidade e de anti-"trust".[21]

Esses números colocam-os entre os principais gastadores em lobby em Washington. Na Europa, documentos revelados de um processo judicial do criador de aplicações six4Three contra o Facebook mostraram como este ameaçava a Europa de investir noutro local se não recebesse certas garantias em 2013.[22] Embora o RGPD tenha sido aplicado, os documentos revelaram um óptimo relacionamento entre Facebook e Enda Kenny, primeiro-ministro do governo irlandês.

O documento mostra que, devido à sua presidência em 2013, o primeiro-ministro irlandês poderia influenciar as decisões da Directiva Europeia de Dados, que estava a ser discutida à época.[23] Além disso, após a entrada em vigor do RGPD, a preocupação recaiu sobre a autoridade irlandesa de controlo dos dados pessoais. As empresas de Silicon Valley, incluindo o Facebook e a Google, escolheram a Irlanda devido às suas promissoras condições favoráveis. Como o regulador principal deve estar no país em que os países têm a sua autoridade de dados, o comissário de protecção de dados da Irlanda actuava para todos os 28 Estados-Membros.[24] A concentração económica também leva a uma aplicação insuficiente da lei, pois as multas são vistas como uma despesa comercial em vez de um impedimento desse comportamento. Devido ao valor das suas empresas, a Google conseguiu cometer violações de privacidade com o Google Street View, mesmo após vários processos.[25] Outro exemplo mais recente foi a multa recebida pelo Facebook de 5 mil milhões de dólares da Federal Trade Commission dos Estados Unidos pelas violações de privacidade da Cambridge Analytica.[26] Não apenas se tratava de um mês de receitas e menos de um quarto do lucro anual do Facebook, mas também o preço das acções subiu após as notícias confirmarem o valor da multa, que era o esperado pelo Facebook.[27]

Uma solução para isto, como argumentou Wu, é confiar menos na economia e ter um padrão mais rigoroso e amplo em favor da aplicação da lei da concorrência. Por exemplo, estabelecendo uma barreira mais elevada às fusões gigantes ou banindo per

se as fusões que reduzem as empresas concorrentes a menos de quatro.[28] Essa abordagem é uma maneira de garantir a concorrência futura e salvaguardar a inovação, que é extremamente importante no mundo da tecnologia. Ao confiar menos em argumentos económicos, também é mais fácil estabelecer o debate público e até permitir que os cidadãos se queixem e intervenham. As separações também devem ser consideradas. A divisão das empresas pode torná-las mais eficientes, como foi o caso da cisão da Standard Oil. Também pode elevar a qualidade da concorrência em relação às protecções da privacidade.[29]

As multas corporativas parecem geralmente de enorme magnitude mas, quando comparadas aos lucros das principais empresas de tecnologia, são insignificantes. Na prática, essas multas são sentidas mais como um custo dos negócios do que como um impedimento ou uma sanção por comportamento ilegal.[30] Além disso, a Comissão Europeia, ao abordar o comportamento anticoncorrencial, apenas estabeleceu compromissos de comportamento e não soluções estruturais.

Quando a Comissão multou a Google em 4,34 mil milhões de euros por práticas ilegais relacionadas com o seu uso dos dispositivos móveis Android, também exigiu à Google que parasse a conduta ilegal e se abstivesse de comportamentos abusivos semelhantes no futuro.[31] Os compromissos de comportamento são caros, devido à monitorização constante exigida. Eles também são razoavelmente ineficientes quando aplicados a empresas desta magnitude, que possuem estabilidade económica suficiente para suportar confortavelmente as multas impostas em caso de violações. Essa estabilidade financeira leva as grandes empresas de tecnologia a terem uma reduzida consideração pela lei e torna o sistema judicial ineficaz. Remédios estruturais e cisões, por outro lado, são auto-executáveis e, consequentemente, fornecem uma maneira mais eficaz de punir e impedir o mau comportamento de empresas como Google e Facebook.

Um relatório patrocinado pelo governo do Reino Unido publicado em Março [de 2019] recomendava uma acção mais frequente e mais firme para desafiar as fusões.[32] No entanto, em vez de separações, propõe-se um código de conduta e mobilidade de dados como meio para proporcionar uma maior concorrência e inovação. O poder seria disseminado à medida que novos participantes entrassem no mercado com dados e assegurassem que não havia um comportamento abusivo por parte dos gigantes da tecnologia.

Embora ter uma concorrência efectiva seja uma boa maneira de espalhar o poder de mercado, essas empresas ainda teriam concentração económica para arcar com os custos da infracção. Portanto, as separações podem ser um bom primeiro passo para enfrentar as preocupações políticas levantadas pela concentração de poder numa única empresa ou plataforma. O segundo seria a mobilidade de dados para garantir a democracia descentralizando o poder do mercado.

II.2. Quem deve regular a tecnologia?

O Facebook e a Google apresentaram uma história de inevitabilidade tecnológica para descartar a lei e quaisquer tentativas de regulamentação. No entanto, como argumenta Joshua Fairfield, essa é apenas uma história que serve como uma grande campanha de marketing.[33] Consequentemente, existem muitos exemplos de como isto não é

?

Sabia que

A 4G de comunicações móveis só ultrapassou a 2G em 2018, atingindo as 3,4 mil milhões de ligações (44% do total).

A 4G deve liderar “em breve” e ser responsável por 62% das ligações em 2023.

As ligações 5G devem ultrapassar a 2G em 2023 e a 3G dois anos depois.

empiricamente verdade. O mais evidente é o Regulamento Geral para a Proteção de Dados (RGPD). O RGPD entrou em vigor após anos de se ter a privacidade negada e não regulamentada, obrigando o Facebook e a Google a cumpri-lo. Mesmo antes do RGPD, o Tribunal de Justiça da União Europeia (TJUE) decidiu que a Google tinha que admitir solicitações de indivíduos para remover links para páginas da Web acessíveis gratuitamente, resultantes de uma pesquisa pelo seu nome.[34] Outro exemplo é o caso da Licra v. Yahoo, quando houve um leilão online aberto de objetos nazis, o que é proibido em França. O Yahoo alegou que era impossível à empresa garantir que nenhum cidadão francês participasse no leilão.

No entanto, especialistas argumentaram que a maioria dos utilizadores franceses da Internet poderia ser identificada nas bases de dados do DNS ["domain name system" ou sistema de registo de nomes de domínios da Internet]. O Yahoo foi então forçado pelo tribunal a negar o acesso a cidadãos franceses com base nas suas bases de dados do DNS.[35]

Teoricamente, também é impossível afirmar que "a lei está morta" ou que não consegue acompanhar. Como Fairfield argumenta, a lei é a mera regulação do comportamento humano e, portanto, desenvolve-se com ele. A tecnologia também regula inevitavelmente o comportamento humano, determinando o que alguém pode ou não fazer. Consequentemente, a tecnologia nunca é neutra, possui "leis" inerentes que determinam que tipo de comportamento é permitido. Existe uma escolha inerente de valores, direitos e liberdades que são incorporados na tecnologia. Num livro revolucionário, Lawrence Lessig mostrou como o código por trás da tecnologia é lei, pois regula o comportamento humano.[36] [37]

Portanto, os indivíduos responsáveis por programarem o código são aqueles que decidem o que pode e o que não pode ser feito - as nossas liberdades. Consequentemente, a "lei" está a ser criada todos os dias; no entanto, está nas mãos de empresas privadas, a saber, o Facebook e a Google. À medida que a sociedade passa do físico para o digital, as leis precisam de serem feitas através do código subjacente à tecnologia.

O conceito de "cidades inteligentes" ilustra como o mundo físico e digital interagem cada vez mais. Uma "cidade inteligente" procura digitalizar a cidade incorporando sensores em objectos, corpos e lugares. Além disso, recolhe e analisa a informação para explorar diferentes soluções para as questões urbanas e optimizar os seus recursos.[38] Devido ao desenvolvimento e consequente complexidade da tecnologia, é inevitável a criação de parcerias público-privadas para acompanhar o estado da arte em ideias e sistemas. Consequentemente, o governo age mais como um corretor, comprando e organizando os serviços do sector privado.[39] A protecção dos direitos humanos fica assim nas mãos de quem concebeu a cidade inteligente. Por exemplo, o direito à privacidade só pode ser concedido aos cidadãos das Cidades Inteligentes se for incorporado na tecnologia que a governa, produzindo uma privacidade por design.

A abordagem tecnológica para uma cidade inteligente pode ser completamente diferente. Toronto fez uma parceria com a empresa-mãe da Google, a Alphabet. Na proposta do projecto, existia uma garantia explícita para salvaguardar o direito à privacidade, mas o projecto permaneceu secreto. No entanto, um consultor do projecto afastou-se devido à falta de transparência e às dúvidas sobre como

prosseguiria.[40] Por outro lado, há o caso de Barcelona em que a prioridade está a ser dada à transparência. A transparência convida a uma cultura de partilha de informações e a um debate público onde governo, cidadãos e entidades privadas estão todos envolvidos no processo da tomada de decisão. O debate público promoveu a inovação, garantindo o respeito pelos direitos humanos.[41]
Como regular a tecnologia é uma pergunta difícil, mas inevitável. As leis existentes são difíceis de aplicar devido aos seus modelos de negócios disruptivos que fornecem serviços gratuitos e dificultam definir mercados. Novas leis também são difíceis de conceber devido às implicações desconhecidas.

Consequentemente, a melhor resposta sobre como regular a tecnologia é através da comunicação. É necessário informar os cidadãos e envolvê-los no debate público. Numa democracia, o Estado não deve ter o único poder de decidir sobre o uso da tecnologia. No entanto, a tecnologia também não deve estar nas mãos de poucas empresas de tecnologia e de lucros corporativos, como na Europa.

As inovações em tecnologia não significam que estamos no caminho certo. Da mesma forma que continuar a conduzir um veículo por novas estradas não significa que se esteja no caminho certo, especialmente quando nem sequer se decidiu para onde se quer ir. Deve-se parar, decidir para onde ir e pedir instruções. A tecnologia é uma ferramenta social e a única maneira de assegurar que ela é usada para o bem-estar dos cidadãos é envolver todos no processo da tomada de decisão em torno da tecnologia.

Dessa forma, deve haver regulação para garantir que isso não é deixado apenas nas mãos do Facebook e da Google.

III. Autonomia dos indivíduos

III.1. A capacidade de escolha

Facebook e Google são quase indispensáveis no século XXI. As questões da sua indispensabilidade aliadas à concentração económica já foram abordadas na primeira parte deste artigo. Nesta parte, será abordada de uma micro-perspectiva, do ponto de vista do "utilizador" de tais vantagens.

As tecnologias da informação e da comunicação estão agora mais difundidas que a electricidade.[42] Elas são uma necessidade na vida quotidiana e na participação social. O Facebook possui 76,3% do mercado de media social na Europa e a Google possui uma participação impressionante de 93,85% no mercado dos motores de busca na Europa. Essa posição dominante e a falta de concorrência real tornam quase impossível evitar essas duas empresas no nosso dia a dia.

Consequentemente, é justo dizer que qualquer acordo com os "termos de serviço" ou "política de privacidade" é forçado, devido à falta de opções. O receio do consentimento forçado é salvaguardado na Directiva 93/13/CEE do Conselho, de 5 de Abril de 1993, sobre as cláusulas abusivas nos contratos celebrados com os consumidores. A directiva estipula que o "acordo do utilizador" ou a "política de privacidade" não podem ser sujeitos a negociação individual e podem ser considerados ilícitos, dependendo da natureza dos bens, serviços e contexto.[43] Esta directiva tornou-se obsoleta no mundo digital porque os serviços digitais causam disrupção ao serem gratuitos. Portanto, Clickwraps, acordos com os quais um utilizador precisa de concordar com as condições para usar o produto ou serviço, foram confirmados pelos

tribunais. No entanto, uma prática injusta justificada por um acordo sem escolha é um ataque à autonomia individual. Para mais, para proteger a autonomia individual, esses termos precisam de ser fortemente regulamentados e a sua legalidade regularmente comparada de acordo com o RGPD.

Existe um certo receio de que, ao impor leis sobre a tecnologia e torná-la menos "gratuita", isso sufocará a inovação e fará mais mal do que bem à sociedade.
No entanto, na prática, o que acontece na ausência do Estado? Se removêssemos qualquer controlo, por exemplo abolindo a constituição, estaríamos mais ou menos livres? Teríamos mais ou menos direitos? É fácil entender, sob essa perspectiva, como discutiríamos o último ponto. Se não houvesse um texto legal a estabelecer os nossos direitos e liberdades e a aplicá-los, eles não existiriam. Consequentemente, estaríamos à mercê dos mais fortes e poderosos, seja o Estado, uma entidade privada ou um indivíduo autoritário.
Existem constituições e regulamentos para garantir e salvaguardar esses direitos, não para serem capturados. Portanto, pode-se argumentar que a liberdade se baseia num tipo específico de controlo através da reflexão.[44] Assim, quando o Facebook e a Google advogam pela liberdade da lei, eles estão a defender a liberdade de a explorar. Sem a possibilidade de optar pelas práticas de "data mining" e de vigilância, que serão discutidas mais à frente, os utilizadores não têm escolha a não ser consentir num contrato abusivo com o Facebook e a Google.

III.2. A capacidade de tomar uma decisão

Aqui é onde Facebook e Google divergem completamente de outras empresas de tecnologia. O seu modelo de negócios é algo completamente novo que Shoshana Zuboff nomeou como "Capitalismo de Vigilância".[45] É importante observar que o primeiro passo crucial é dar um nome. Como Fairfield argumentou, a mudança começa num idioma e em comunidades, somente depois pode haver regras e aplicação nos tribunais. Para resolver um problema, precisamos de nomeá-lo e defini-lo. Essa definição é o primeiro passo crucial para iniciar uma discussão e tentar encontrar soluções. Só então podemos regular.

Google e Facebook usam a experiência humana como matéria-prima gratuita que é transformada em dados comportamentais e vendida. Eles lucram com a experiência dos utilizadores, daí o nome de capitalismo da vigilância.[46] Ao recolher, processar e analisar os dados dos utilizadores, eles podem prever e vender dados comportamentais (Big Data) aos anunciantes. O capitalismo da vigilância trouxe três rupturas principais. A primeira tem a ver com o capitalismo. No capitalismo, os argumentos são de que, devido às incertezas do mercado, é melhor deixá-lo sozinho. Se os actores do mercado agirem livremente, com predomínio pelo interesse e pela incerteza, o mercado irá autoregular-se.[47] Podemos, portanto, ver uma evidente mudança de paradigma. Como o Facebook e a Google têm acesso a dados informativos sobre os seus utilizadores, isto deixou de ser um predomínio da incerteza e da ignorância. Portanto, eles podem agir independentemente das forças invisíveis do mercado.[48]

Em vez de o tentar convencer a comprar algo ou executar uma acção específica como um anúncio comum, ele manipula-o para o fazer. Manipular significa que o controla a seu favor, o que Zuboff chama de "poder instrumentário", moldar o comportamento humano para os fins dos

outros.[49] A compreensão teórica desse conceito seria suficiente para compreender a violação definitiva da autonomia pessoal. O utilizador não apenas enfrenta uma escolha da invasão, como os acordos injustos com o utilizador, mas também nem sequer reconhece que isto está a acontecer em primeiro lugar. Envenena a experiência interior para formar a vontade.[50]

Há provas que mostram como o capitalismo de vigilância pode prejudicar a autonomia de uma pessoa e atacar a democracia. O Cambridge Analytical Scandal revelou como os dados de milhões de utilizadores do Facebook foram recolhidos e usados numa campanha política.[51] Ao recolher milhões de perfis no Facebook, é possível identificar os eleitores mais persuasivos e os problemas com os quais se preocupam para lhes enviar a mensagem certa na hora certa. Por exemplo, foi enviada propaganda dirigida à comunidade afro-americana com a referência de Clinton à juventude afro-americana de"super predadores".[52] A Google também aceitou conscientemente propaganda que alegava falsamente poder resolver os problemas dos empréstimos durante a crise de 2011.[53]

A segunda disrupção é a indiferença radical para com os consumidores. Os dados dos utilizadores serviram como matéria-prima para ser analisada e vendida. Como os utilizadores são apenas os meios, não o fim, não há incentivo para tentar melhorar as suas plataformas ou melhorar a privacidade dos serviços para agradar aos consumidores. A terceira disrupção é a qualidade do produto. O que é relevante é que seja usado por todos, não que seja o melhor. Como o interesse é fazer com que o maior número de pessoas use o serviço, ele incentiva a criação de novos falsos, uma das maiores ameaças à liberdade de expressão. O capitalismo de vigilância, portanto, forma uma ruptura não apenas porque manipula a autonomia individual mas também porque é indiferente às necessidades e aos melhores interesses dos cidadãos e da sociedade.

Perante a falta de concorrência no mercado da tecnologia, é praticamente impossível não ser alvo de vigilância indiscriminada e "data mining" dos dados na esfera digital. A Google controla fabricantes de equipamentos originais, como smartphones, tablets, produtos conectados, automóveis e até equipamentos domésticos. Os dados recolhidos são então vendidos e comprados no mundo do monopólio da tecnologia. Por exemplo, a Google pagou alegadamente à Apple 9 mil milhões de dólares em 2018 e 12 mil milhões em 2019 para ser o mecanismo de pesquisa por defeito do [browser] Safari.[54]

A Google negoceia com operadores de telecomunicações, fabricantes de equipamentos originais e de sistemas operativos e também leiloa [a informação de] utilizadores dos seus produtos a empresas como o Baidu, um motor de pesquisa chinês de propriedade estatal.[55] Esses comportamentos asseguram ainda mais os monopólios de tecnologia, já que é difícil entrar no mercado sem comprar grandes quantidades de dados.

Os novos negócios têm de obter acesso ao mercado online criando aplicações de terceiros distribuídos pelas lojas de aplicações online da Google, da Apple e da Microsoft.[56] Essa é uma clara desvantagem por comparação com as aplicações pré-instaladas, pois milhões de utilizadores usam as aplicações padrão e pré-instaladas. A Comissão Europeia já multou a Google uma vez por exigir que os

fabricantes pré-instalassem a sua aplicação de busca e o browser do Google como condição para licenciar a loja de aplicações da Google.[57] Para assegurar uma concorrência justa, esse pacote conjunto precisa de ser combatido continuamente.

Adicionalmente, os filtros usados no Facebook e no Google criam um ambiente isolado que interfere com a nossa liberdade de expressão. Como mencionado acima, o interesse está no uso das plataformas. Portanto, o único objectivo é maximizar o envolvimento.[58] Isso é melhor criado com material inflamatório e até notícias falsas que criam reacções instantâneas. Quando esses dois efeitos são combinados e complementados, ocultam os utilizadores de outras informações e interferem com a sua liberdade de expressão e capacidade de formar opiniões.

A nossa autonomia foi manchada por acordos injustos com os utilizadores que não nos deixam escolha, esvaziando a palavra "consentimento". Esses contratos devem ser fortemente regulados para garantir que não comprometem a privacidade dos utilizadores e cumprem o RGPD. Desenvolvimentos importantes aconteceram na Alemanha. Uma decisão judicial proibiu o Facebook de combinar os dados dos utilizadores nas suas plataformas sociais e recolher dados de sites de terceiros sem o seu consentimento.[59] Além disso, o tribunal esclareceu que o processamento de dados não pode ser uma condição prévia para o uso do Facebook, para que seja genuinamente voluntário. Foi considerado anticompetitivo por estar a usar a sua posição dominante para estabelecer termos comerciais que se aproveitavam dos consumidores.[60]

Com deveres estritos que garantem direitos sobre os dados, pode haver uma mitigação geral dos riscos e danos que o Big Data representa para a democracia. Ao limitar o objectivo dos dados recolhidos, implementar a comunicação entre advogados de direitos humanos e cientistas de dados (e outros especialistas técnicos relevantes no campo específico) e, eventualmente, considerar um uso "opt-in opt-out" dos dados.[61] As soluções estão disponíveis e é preciso haver uma discussão vívida e aberta para seleccionar as melhores.

IV. Conclusão

A tecnologia do Facebook e da Google estão a desafiar a democracia. A capitalização da experiência humana leva a rupturas significativas que precisam de ser tratadas com cuidado. Como Harari explica, a propriedade sempre trouxe desigualdade. À medida que os humanos se tornam proprietários das coisas, são formadas hierarquias. Consequentemente, apenas uma pequena parte da população tem riqueza e poder.[62] A revolução industrial interrompeu isso devido à crescente dependência das massas. Assim, os governos, liberal e comunista, concentraram-se em investir na saúde, educação e bem-estar dos seus cidadãos, para garantirem trabalhadores e soldados saudáveis. No entanto, o capitalismo da vigilância providenciou uma nova ruptura. Como a prosperidade não depende mais das massas, o capitalismo da vigilância torna a sociedade cada vez mais desigual, concentrando novamente poder e riqueza nas mãos de uma pequena elite. Como mostrado acima, os cidadãos são obrigados a obter uma forma estragada de consentimento do poder para entidades privadas não-eleitas. Esse controlo não consentido dá origem ao Big Other - um

poder soberano que age independentemente do governo e do dinamismo da democracia de mercado.[63]

O capitalismo da vigilância é o ataque mais explícito à nossa autonomia. O debate público deve ser de elevada prioridade. Primeiro, para quebrar o ciclo de desinformação que Facebook e Google estão a espalhar na sociedade e, segundo, para suscitar o debate público como um meio de abordar a questão. O público deve ser informado para começar a exigir uma luta contra essa opressão e injustiça. A sociedade precisa questionar essas actividades e os seus perigos para a democracia.

Deve-se indagar se esse tipo de propaganda é legal, considerando a precisão e a manipulação que implica. Parece estranho ter havido uma enorme preocupação com o marketing subliminar, algo que nem se comprovou que funcionasse, levando a proibições em países como a Grã-Bretanha e a Austrália.[64] No entanto, agora permitimos anúncios direccionados que podem formar e substituir a nossa própria vontade e chegam ao ponto de atrapalhar eleições democráticas.

Após regulamentar esses anúncios manipuladores, o foco deve mudar para os acordos injustos com os utilizadores e as políticas de privacidade que exigem o consentimento forçado dos utilizadores. A conformidade com o RGPD e a análise do conteúdo potencial de exploração precisam de ser avaliadas continuamente para salvaguardar a nossa autonomia. Para entender as questões relevantes e encontrar as suas soluções, é necessária uma visão geral de todas as áreas do Direito, conforme demonstrado pela nova jurisprudência alemã.

Depois de proteger a vontade e a autonomia dos utilizadores, é preciso mudar o controlo sobre quem tem poder sobre a tecnologia. O Facebook e a Google são quase essenciais no século XXI e, portanto, não podem ser o controlo exclusivo sobre plataformas que agora são vistas como um espaço público.[65] Já era evidente que a lei podia acompanhar a tecnologia. Agora, a sociedade precisa de saber como. Mais uma vez, é preciso haver um debate público sobre como a tecnologia pode ser melhor usada, salvaguardando a autonomia dos utilizadores. É precisa uma mudança sobre quem está no controlo. Caso contrário, como mostrado, a Google e o Facebook terão a liberdade de continuar a explorar os utilizadores como quiserem.

Finalmente, a concentração económica tem de ser gerida. Como Zuboff afirma no seu livro, abordar as questões de concorrência não significa necessariamente abordar as questões da privacidade e do capitalismo da vigilância. Uma ruptura do Facebook e da Google significa apenas mais empresas no negócio do capitalismo da vigilância. No entanto, foi demonstrado que é certamente mais fácil controlar as empresas se elas forem menores, primeiro, porque é difícil fazer escolhas políticas específicas e atingir metas políticas se houver muitas vontades para concordar em vez de apenas uma[66]. Em segundo, porque a concentração económica facilita o pagamento de multas, elas podem ser facilmente vistas como despesas comerciais e não como uma prática dissuasora. Essa indiferença é evidente; por exemplo, a Google teve vários casos de violação de privacidade no Google Street View, em que pagou as multas e continuou a fazer exactamente o mesmo.[67] As cisões podem ser o primeiro passo para recuperar o controlo e fazer cumprir a lei.

Em conclusão, é preciso haver um debate público. A sociedade, não a Google e o

Facebook, precisa de recuperar o controlo. Precisamos de encontrar a resposta sobre como e quem deve regular essas empresas tecnológicas[68]. Somente com um debate público aberto e informado, a lei e a jurisprudência podem encontrar soluções para os desafios que Facebook e Google colocam à democracia.

?
Sabia que

Em 2023, a Europa ocidental terá 370 milhões de utilizadores da Internet (87% da população), crescendo dos 345 milhões de 2018. E 365 milhões vão usar dispositivos móveis.

Haverá 4 mil milhões de equipamentos online, mais 1,6 mil milhões do que em 2018, e os 169 milhões de "hotspots" Wi-Fi públicos devem aumentar para 628 milhões, com o Wi-Fi6 presente em 11% deles.

Cisco

1 Unrepresented Nations & Peoples Organisation, "Self Determination" (acedido em 03.06.2019).

2 Shoshana Zuboff entrou para a Harvard Business School em 1981 e é Charles Edward Wilson Professor Emerita na Harvard Business School. Em 2014 e 2015 foi Faculty Associate no Berkman Center for Internet and Society da Harvard Law School. A sua carreira tem sido devotada ao estudo da ascensão do digital, as suas consequências individuais, organizacionais e sociais e da sua relação com a história e futuro do capitalismo.

3 S. Zuboff, The Age of Surveillance Capitalism, London: Profile Books Ltd, 2019.

4 Tim Wu é professor da Columbia Law School e autor de artigos de opinião para o The New York Times. É mais conhecido pelo seu trabalho na teoria da Net Neutrality. É autor dos livros The Master Switch, The Attention Merchants ou The Curse of Bigness, bem como do artigo Network Neutrality, Broadband Discrimination e de outros . Em 2013 foi nomeado um dos America's 100 Most Influential Lawyers e em 2017 para a American Academy of Arts and Sciences.

5 T. Wu, The Curse of Bigness, Columbia Global Reports, 2018.

6 Joshua Fairfield é um especialista em direito e tecnologia reconhecido internacionalmente, especializado em propriedade digital, contrato electrónico, privacidade em Big Data e comunidades virtuais. Foi orador numa palestra em Master of International Technology Law sobre "Can Law Keep Up With Technology?", após a qual deu acesso ao seu livro não publicado no Google Docs. O livro centra-se na necessidade do desenvolvimento de uma nova linguagem para lidar com questões de tecnologia e cooperação humana. Muitas pessoas de diferentes origens e áreas de especialização têm acesso ao livro e podem comentar sobre o mesmo, retratando o espírito de debate público e cooperação que o livro exige.

7 S. Zuboff, The Age of Surveillance Capitalism, London: Profile Books Ltd, 2019.

8 Wu 2018, supra note 5.

9 Council Regulation (E.C.) No 139/2004 of 20 January 2004 on the Control of Concentrations Between Undertakings (the E.C. Merger Regulation).

10 A. Italianer, "Competition Merger Brief", European Commission, 2015-1.

11 B. Bucher, "WhatsApp Has Grown its User Base by 20% in the U.K.", Messenger People, 2019 (acedido em 03.06.2019).

12 Italianer 2015, supra note 9.

13 Case No. M. 8228 (Facebook/WhatsApp), Merger Procedure, 17.5.2017.

14 Italianer 2015, supra note 9.

15 Wu 2018, supra note 5, p. 59.

16 Wu 2018, supra note 5, p. 55.

17 R. Pitofsky,"The Political Content of Antitrust", University of Pennsylvania Law Review 1979-127 (acedido em 16.07.2019).

18 "List of mergers and acquisitions by Facebook", Wikipedia (acedido em 16.07.2019).

19 List of Google's Acquisitions, Crunchbase (acedido em 16.07.2019).

20 M. Vestager, "Shaping Competition Policy in the era of Digitalisation: Welcoming Speech", European Commission, 17.01.2019 (acedido em 16.07.2019).

21 P. Dave, "Google, Facebook spend big on U.S lobbying amid policy battles", Reuters, 23.01.2019 (acedido em 16.07.2019).

22 J. Edwards, "This is not a threat: Facebook denies it would have pulled investment from Europe and Canada if demands were not met", Business Insider, 04.03.2019 (acedido em 16.07.2019).

23 C. Cadwalladr, "Revealed: Facebook's global lobbying against data privacy laws", The Guardian, 02.03.2019 (acedido em 16.07.2019).

24 N. Vinocur, "Millions of Americans rely on Europe's tough new privacy rules to safeguard their data, but the law's chief enforcer – Ireland – is in bed with the companies it regulates", 24.04.2019 (acedido em 16.07.2019).

25 S. Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilisation", Journal of Information and Technology, 2015-30.

26 J. Wong, "Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports", The Guardian, 12.07.2019.

27 J. Swartz, "Facebook stock hits highest price in nearly a year after reports of $5 billion FTC fine", MarketWatch, 14.07.2019 (acedido em 16.07.2019).

28 Wu 2018, supra note 5, p. 129.

29 Wu 2018, supra note 5, p. 133.

30 S. Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilisation", Journal of Information and Technology, 2015-30, p. 75-89.

31 European Commission, "Antitrust: Commission Fined Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine", Press release, 18.07.2018 (acedido em 03.06.2019).

32 Digital Competition Expert Panel, "Unlocking digital competition", Crown copyright, March 2019.

33 Fairfield, supra note 6.

34 Case C-131/12, Google Spain and Google, 2014.

35 C. Duh, "Yahoo! Inc. LICRA", Berkeley Technology Law Journal, 2002-1, p. 359-378.

36 Lester Lawrence Lessig III é um académico americano, advogado e activista político. É Roy L. Furman Professor of Law na Harvard Law School e antigo director do Edmond J. Safra Center for Ethics na Harvard University.

37 L. Lessig, Code Version 2.0, New York: Basic Books 2006, p. 4.

38 IBM Institute of Business Value, "A Vision of Smarter Cities", 2009.

39 R. Kitchin, P. Cardullo & C. Di Feliciantonio, "Citizenship, Justice and the Right to the Smart City", The Programmable City Working Paper 2018-41.

40 S. Fussell, "The City of the Future is a Data-Collection Machine", The Atlantic, 21.11.2018 (acedido em 03.06.2019).

41 M. Dean, "A digital right to the city: who defines democracy in smart cities?"(acedido em 03.06.2019).

42 S. Zuboff 2019, supra note 4, p.4

43 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (acedido em 03.06.2019).

44 Lessig 2006, supra note 24.

45 Zuboff, 2019, supra note 4.

46 J. Naughton, "The goal is to automate use: Welcome to the age of surveillance capitalism", The Guardian, 20.01.2019 (acedido em 17.07.2019).

47 L. Yueh, The Greatest Economists: How Their Ideas Can Help Us Today, Penguin Random House, 2018, p.11.

48 S. Zuboff 2019, supra note 4, p.497.

49 Idem, p.13.

50 Idem, p.521.

51 H. Savies, "Ted Cruz using firm that harvested data on millions of unwitting Facebook users", The Guardian, 2015 (acedido em 03.06.2019).

52 M. Lee, "Surveillance Capitalism, Cambridge Analytica, and Data Security", 29.05.2018 (acedido em 03.06.2019).

53 Zuboff 2019, supra note 4.

54 L. Segarra, "Google to pay Apple $12 Billion to Remain Safari's Default Search Engine in 2019: Report", Fortune, 20.09.2018 (acedido a 16.07.2019).

55 R. Lee, "Telecom and Tech Gian Conflict of Interest and Competition Violations: Part 2", The Epoch Times, 01.02.2019 (acedido em 16.07.2019).

56 R. Lee, "Telecom and Tech Gian Conflict of Interest and Competition Violations: Part 2", The Epoch Times, 01.02.2019 (acedido em 16.07.2019).

57 European Commission, "Antitrust: Commission Fined Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine", Press release, 18.07.2018 (acedido em 03.06.2019).

58 C. Doctorow,"Regulating Big Tech makes them stronger, so they need competition instead", The Economist, 06.06.2019 (acedido em 03.06.2019).

59 N. Lomas, "German antitrust office limits Facebook's data gathering", TechCrunch, 07.02.2019 (acedido em 03.06.2019).

60 Ibid.

61 G. Sarfaty, "Can big data revolutionise international human rights law", Penny Law: Legal Scholarship Repository, 2018.

62 Y. N. Harari, 21 Lessons for the 21st Century, Jonathan Cape, 2018.

63 Zuboff, 2015, supra note 19.

64 S. Dwilson, 'Laws on Subliminal Marketing', Chron (acedido em 03.06.2019).

65 Zuboff 2019, supra note 4, pp. 521.

66 Pitofsky, supra note 16.

67 Zuboff 2019, supra note 4.

68 Idem, p. 521.

?

Sabia que

Estão mais de 5.000 satélites a orbitar a Terra e 775 são usados para telecomunicações. 2017 teve o número mais elevado de lançamentos, com 453 satélites, um aumento perante os 382 de 2018.

O problema com a privacidade

Anna Dorothea Ker

Presos numa sociedade de vigilância global, perdemos de vista o que privacidade quer realmente significar. Para reclamar o seu valor, temos de reconsiderar o que queremos proteger.

Um Conceito em fluxo

Privacidade – com o passar do tempo, esta palavra aparece no nosso vocabulário colectivo em intervalos cada vez mais próximos. Estamos inundados com "privacidade": nas notícias, nos anúncios, na retórica das empresas tecnológicas. Mas com o seu crescente uso vem uma torrente de confusão. Está na altura de dar um passo atrás e questionar: do que estão exactamente líderes políticos, jornalistas e empresas a referir-se quando falam de privacidade? E porque interessa isto?

Em 1975, a filósofa judicial Judith Jarvis Thomson observou que "a coisa mais impressionante sobre o direito à privacidade é que ninguém parece ter uma ideia clara do que é". Apesar do mundo parecer muito diferente hoje, esta declaração permanece verdadeira. Ao longo das últimas décadas, uma expansão de programas de segurança nacional e uma adopção tecnológica generalizada mudaram as noções societais de privacidade, definindo o panorama para as estruturas globais de vigilância que se entranharam na infra-estrutura da Internet. Neste ambiente, é crucial que pensemos e falemos claramente relativamente à privacidade, porque o modo como pensamos hoje dirá como será consagrado na nossa legislação, políticas, livros e tecnologias de amanhã.

Percepções do passado

Um breve olhar na história da privacidade no Norte Global revela a lenta evolução do termo ao longo dos séculos. No tempo dos gregos antigos, a diferenciação de Aristóteles entre as esferas da *polis* (pública/política) e *oikos* (privada/doméstica) estabeleceu o quadro de referência para o que poderia ser considerado o primeiro sinal de privacidade: a privacidade do corpo e do lar. O conceito era uma força orientadora integral na arquitetura - para os ricos, pelo menos – ao longo da Idade Média, e foi galvanizada durante a Renascença, quando os lares separados para as famílias se tornaram comuns em toda a Europa.

A segunda linha da privacidade – privacidade da informação ou privacidade dos dados - envolve informações pessoais, incluindo a correspondência, registos médicos e informações financeiras. Essa forma de privacidade começou a desenvolver-se muito mais tarde. Os Estados Unidos aprovaram o *Post Office Act* em 1710, que impedia os trabalhadores postais de lerem a correspondência das pessoas, mas não foi até à Era Dourada [final do século XIX] que a privacidade foi reconhecida como um direito. Em 1890, o juiz da Supremo Tribunal de Justiça, Louis Brandeis, e o advogado Samuel Warren publicaram o seu artigo de referência *The Right to Privacy* na *Harvard Law Review*, argumentando que, embora a privacidade não estivesse explicitamente consagrada na Constituição, o "direito a ser deixado em paz" era inerente à lei comum.

O impulso social pela privacidade que se seguiu foi uma resposta ao surgimento de uma tecnologia emergente (a câmara fotográfica, na época) - um fenómeno que ocorreria repetidamente nas décadas seguintes. Não foi até à II Guerra Mundial que a privacidade foi consagrada como um direito humano internacional. A Assembleia Geral das Nações Unidas adoptou o Artigo 12º na Declaração

Universal dos Direitos Humanos (UDHR) em 1948:
Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.

Sete anos mais tarde, a Convenção Europeia dos Direitos Humanos (ECHR) foi ratificada, incluindo o Artigo 8º:

Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

No entanto, o direito à privacidade na ECHR está sujeita a certas restrições "de acordo com a lei" e "necessárias numa sociedade democrática". A ampla interpretação destes qualificadores pelo governo dos EUA, em particular, percorreu um longo caminho para enfraquecer a privacidade como um direito e uma liberdade civil.

Um momento essencial na evolução da privacidade ocorreu em 1967, quando Alan Westin, professor de direito público e governo da Universidade de Columbia, colocou o conceito como uma questão de acesso e controlo. No seu trabalho seminal, "Privacy and Freedom", Westin enquadrou a privacidade como "a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outras pessoas".

Essa definição estabeleceu a referência para um entendimento comum da privacidade informacional - que levou Westin à vanguarda do então emergente campo da lei da privacidade. Nas décadas seguintes, no entanto, a noção de privacidade-como-controlo passou a ser distorcida por duas poderosas vagas sociais: o aparato da segurança nacional e os imperativos corporativos das empresas de tecnologia.

Contexto actual

Em 1985, o sociólogo Gary T. Marx escreveu que "numa sociedade em que todos se sentem [como] alvo de investigação, a confiança... é prejudicada. De facto, as actuais tecnologias de vigilância podem estar a criar um clima de suspeita do qual não há escapatória". Nas décadas seguintes, as rotas de fuga metafóricas na nossa sociedade global da informação ficaram bloqueadas. O início dos anos 2000 marcou um ponto de viragem para a "vendetta" da segurança nacional contra a privacidade e o pioneirismo da indústria tecnológica da economia de vigilância - forças que abalaram profundamente o entendimento mais profundo dessa noção.

Um momento crucial na nossa consideração global da diluição da privacidade ocorreu em 2013, quando Edward Snowden revelou a extensão da operação "dragnet" de vigilância sistemática com o PRISM pela NSA, muitos aspectos dos quais tinham sido fortalecidos em resposta aos ataques terroristas do 11 de Setembro de 2001. No acto de equilíbrio do governo entre as disposições antiterrorismo e as liberdades civis, medidas de segurança nacional melhoradas degradaram severamente o direito à privacidade dos cidadãos. Isso foi evidenciado na aprovação pelo Congresso da *USA Patriot Act* (2001), que muito aumentou os poderes da espionagem doméstica. [Ler o guia para a vigilância do governo dos EUA do The Privacy Issue.] Outro golpe na privacidade dos cidadãos dos EUA ocorreu em 2008 com a aprovação do *Foreign Intelligence Surveillance Amendment Act* (FISA), que permitiu a

monitorização efectiva por "dragnet" de todas as chamadas e emails que envolviam um destinatário nos EUA. Justificando essas medidas sob a bandeira da segurança, que foi posicionado como um fim para proteger a liberdade, o governo dos EUA fez da privacidade o inimigo da liberdade. Infelizmente, os EUA não são o único regime ocidental a fazê-lo. [Para uma compreensão mais detalhada, ler o artigo "United States of Surveillance"].

Juntando-se aos governos nos esforços da vigilância – embora com propósitos diferentes - está a indústria global de tecnologia, liderada por Silicon Valley. Em 1890, foram os novos avanços na tecnologia fotográfica que levaram o juiz Brandeis a despertar a consciência pública sobre a privacidade. Mais de um século depois, a tecnologia emergente ainda é a força motriz que traz o debate sobre a privacidade de volta à arena pública. Desta vez, é o exponencial poder computacional, combinado com a proliferação de dados, que desencadeou ameaças à privacidade. Roger McNamee, investidor em tecnologia e ex-consultor do Facebook, explica o ponto de viragem: "até por volta de 2000, o sector de tecnologia não tinha tido suficiente poder de processamento, memória, armazenamento ou largura de banda de rede para desenvolver produtos que pudessem ser profundamente integrados nas nossas vidas".

No entanto, em vez de ser só a tecnologia, é a maneira pela qual esse poder de processamento foi cooptado pelas empresas de tecnologia para "reivindicar unilateralmente a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais", e esse é o problema, explica a Professora Emérita em Harvard Shoshana Zuboff. O fenómeno, a que ela chama de "capitalismo de vigilância", surgiu em 2002, quando os engenheiros da Google desenvolveram um sofisticado novo sistema para a publicidade altamente segmentada.

Com esse sistema, todos os pedaços de dados que geramos - não apenas enquanto navegamos online, mas à medida que percorremos as cidades e nos retiramos para as nossas próprias casas - são captados por inúmeras formas de "trackers", desde *cookies* a GPS e sensores em dispositivos IoT [de Internet das Coisas]. Em seguida, são combinados e vendidos aos anunciantes no mercado da publicidade comportamental. Graças à grande quantidade de dados que mantêm sobre os utilizadores da Internet, os vendedores do espaço de publicidade online - principalmente Google e Facebook - permitem aos anunciantes atingirem audiências muito específicas, que são categorizadas não apenas pelos dados demográficos (sexo, idade, localização), mas também pelos traços de carácter. A ideia subjacente é que, quanto mais dados forem recolhidos sobre as pessoas, mais fácil será prever - e, portanto, influenciar - o que elas farão em seguida. Assim, qualquer detalhe mundano das nossas vidas – por outras palavras, o tecido da nossa experiência pessoal e privada – tornaram-se a mercadoria mais lucrativa da Era da Informação, sem o nosso conhecimento, consentimento ou capacidade de optar por não participar. [Para mais informação, consulte o guia da indústria "adtech"].

A vigilância pela *Big Tech* é o pano de fundo de uma série de desenvolvimentos-chave na privacidade que se desenrolaram em 2018. No início do ano, rebentou o escândalo da Cambridge Analytica, revelando que a empresa britânica de "data mining" tinha recolhido os dados de milhões de utilizadores do Facebook para uso em publicidade política - que o

?

Sabia que

De uma análise ao assunto de 9.673 emails, os números mais eficazes para usar são:

4 5 8 10 11

Montague Street Media

denunciante Christopher Wylie afirmou influenciar o Brexit e a vitória de Trump nas eleições de 2016. Em Maio, o Regulamento Geral para a Proteção de Dados (RGPD) entrou em vigor na Europa e, um mês depois, o *California Consumer Privacy Act* (CCPA) foi assinado como lei. Ambas as leis foram concebidas para dar aos utilizadores da Internet mais controlo sobre como os seus dados pessoais são armazenados, e ambos são passos importantes para a protecção legal da privacidade - ainda assim, estudos mostram que, um ano depois, a maneira como pensamos e cuidamos da nossa privacidade não mudou muito - e as estruturas da economia de vigilância certamente também não.

O problema, segundo a associação de direitos civis *European Digital Rights* (EDRi), é que, muito antes da aprovação dessas leis, a evolução da indústria tecnológica – os seus produtos, serviços e modelo de negócios - prejudicou a capacidade dos utilizadores de "controlarem significativamente os seus dados pessoais por meio de escolhas informadas". De políticas de privacidade pouco claras, longas e totalmente enganosas a avisos de *cookies* que alegam apenas "optimizar a experiência do utilizador", o ónus colocado sobre os indivíduos é muito alto. De facto, explica o EDRi, as pessoas ficaram "tão sobrecarregadas com pedidos de consentimento para o uso dos seus dados que a escolha informada se tornou ilusória". No entanto, como o uso da Internet é essencial para a nossa vida quotidiana, não podemos realmente optar por não participar - um obstáculo que mina a noção de privacidade-como-controlo.

Então, porque é tudo isto importante? Os desenvolvimentos tecnológicos e a recolha de dados só vão aumentar exponencialmente. Duas décadas após o nascimento do capitalismo de vigilância e do enfraquecimento da privacidade pelas medidas de segurança nacional, estamos apenas a despertar para a nova realidade que surgiu à nossa volta. À medida que descobrimos coletivamente como lidar com isso, encontramo-nos num ponto crítico, no qual os valores que priorizamos hoje informarão as políticas, leis, livros e tecnologias de amanhã e, finalmente, o tipo de sociedade que queremos para viver. Nada menos que os pilares democráticos fundamentais da autonomia individual e dos direitos de decisão estão em jogo.

Futuros "frameworks"

Para a privacidade ter um futuro na Era da Informação, devemos deixar de tomar o seu significado como garantido e começar a ser específico sobre o que queremos proteger. Isso exigirá uma reformulação do que entendemos ser a privacidade - uma que esclareça os muitos direitos e responsabilidades interconectados que ela incorpora. Uma forma é começar a considerar a privacidade além do seu valor como um direito individual. "O objectivo deve ser entendido como manter a liberdade individual e colectiva, e a justificação não apenas como o de apoiar o autodesenvolvimento individual e próspero, mas também formas democráticas de governança", explicou Deirdre Mulligan, directora da Faculdade do Centro de Direito e Tecnologia de Berkeley. "Isto requer que a privacidade sirva como uma verificação do acréscimo de poder pelo estado e pelas grandes corporações alimentadas por uma vigilância persistente e ampla". Perceber a privacidade como um controlo do poder impregna o próprio conceito de poder e revela o quanto é importante para o bom funcionamento das sociedades livres e abertas.

O jornalista e engenheiro de software Jon Evans baseia-se na ideia de privacidade como uma liberdade colectiva, escrevendo na TechCrunch: "Privacidade é como votar. A privacidade de um indivíduo, como o voto de um indivíduo, geralmente é em grande parte irrelevante para qualquer pessoa além dela própria... mas a acumulação da privacidade individual ou a falta dela, como a acumulação de votos individuais, tem enormes consequências". Evans considera a recolha de dados que forma a base da sociedade de vigilância actual como um "enorme problema de segurança pública" - com três implicações principais.

Primeiro, argumenta, a ausência de privacidade tem um efeito assustador no pensamento e divergência individual. Segundo, se a privacidade é mercantilizada - como exigem os defensores da propriedade de dados - ela torna-se uma questão de classe, entrincheirando ainda mais o desequilíbrio de poder entre aqueles com maiores e menores meios. Terceiro, a acumulação de dados pessoais continuará a manipular a opinião e o comportamento do público - como foi o caso nas eleições presidenciais de 2016 nos EUA. Entendida dessa maneira, a necessidade de intervenção governamental para actualizar e reforçar as proteções à privacidade torna-se inegável. Se defendermos a privacidade como bens comuns, conclui Evans, "não podemos começar a pensar nela como um activo individual a ser vendido aos capitalistas da vigilância. Ela, e nós, somos mais importantes do que isso".

Um outro elemento da reformulação da privacidade vem de Sarah Igo, Professora Associada de História da Universidade Vanderbilt e autora de "The Known Citizen - A History of Modern Privacy in America". Igo argumenta que o futuro da privacidade se baseia na renegociação das coisas pelas quais estamos dispostos a desistir - começando pela conveniência:

Muitas das invasões de privacidade que experimentamos agora, desde perfis sociais até rastreamento comercial, apelaram aos consumidores sob a bandeira da conveniência. Isso era verdade desde os dias das primeiras agências de crédito no século XIX. As informações pessoais trocadas por facilidade e eficiência pareciam uma pechincha razoável, até necessária, em casos individuais. Mas o que não ficou claro inicialmente foram os efeitos acumulados dessa pechincha em vários domínios da sociedade e sob condições tecnológicas que corroeram continuamente as barreiras entre os detentores de dados.

Esta mudança tornou os que lucram com a recolha de dados pessoais cada vez mais poderosos. Também os tornou menos suscetíveis à regulamentação e a controlos legais razoáveis. Reverter as incursões mais preocupantes na privacidade exigirá vontade e acção políticas sustentadas. Mas também exigirá que examinemos com muito cuidado o quanto queremos elevar o valor da conveniência sobre o valor que antes era considerado "privacidade" - uma sensação de discrição e controlo sobre os próprios detalhes biográficos, movimentos físicos, relacionamentos íntimos e desejos pessoais.

Estes detalhes, movimentos, relacionamentos e desejos são incorporados num conceito que Maciej Cegłowski denominou "ambient privacy", que define como "o entendimento de que há valor em manter as nossas interacções quotidianas fora do alcance da monitorização, e que os pequenos detalhes das nossas vidas diárias devem passar despercebidos. O que fazemos em casa, no trabalho... na escola ou no nosso tempo de lazer não pertence a um registo

permanente". Segundo Cegłowski, a privacidade ambiental não é propriedade de indivíduos, mas do mundo ao nosso redor. No entanto, como a lei postula a privacidade como um direito individual, ela não pode responder adequadamente à questão maior em jogo. Cegłowski alerta para os perigos da inação:

A privacidade ambiental desempenha um papel importante na vida cívica. Quando toda a discussão ocorre sob o olhar do software, num meio com fins lucrativos, trabalhando para moldar o comportamento dos participantes, pode não ser possível criar o consenso e o senso partilhado da realidade, que é um pré-requisito para a auto-governação. Se isso for verdade, o afastamento da privacidade ambiental será uma mudança irreversível, porque removerá a nossa capacidade de funcionar como uma democracia.

Como podem essas diferentes interpretações de privacidade ser reconciliadas, para trazer uma clareza construtiva às conversas que temos sobre o seu futuro? Talvez a resposta seja revelada quando nos concentramos menos na palavra "privacidade" em si e mais nos valores que queremos que ela proteja. Entendemos privacidade como liberdade, liberdade civil, autonomia, controlo? Privacidade *versus* conveniência, segurança nacional, vigilância? Questionar os significados específicos das palavras que usamos quando falamos de privacidade - incluindo os conceitos acima referidos - ajudará indivíduos, governos e empresas a falar e a agir sobre o assunto da privacidade com um impacto tangível.

Nesta base, fazem-se as seguintes recomendações:

1. Os governos devem liderar o comando de um entendimento mais aprofundado das ligações entre privacidade e democracia, tanto as abertas (por exemplo, como corretores de dados como a Cambridge Analytica influenciaram o processo democrático nos EUA e no Reino Unido em 2016, e podem fazê-lo novamente em 2020) como as mais subtis (por exemplo, o efeito que a erosão da privacidade tem sobre o discurso, dissidência, protesto e outros pilares de uma sociedade livre). Crescentes recursos devem ser aplicados em investigação e políticas para fortalecer as instituições e disposições do governo democrático, desenvolvendo quadros de referência adaptáveis para proteger os variados e em evolução valores que atribuímos à privacidade.

2. As empresas também devem assumir a responsabilidade de definir novas normas para a indústria, centradas nas necessidades dos seus clientes como seres humanos, não como utilizadores. Isso pode começar com uma re-avaliação dos termos e condições da empresa e das políticas de privacidade, tanto em termos de conteúdo (por exemplo, "são a forma como recolhemos dados realmente necessárias? Quais as alternativas menos invasivas?") como de forma (por exemplo, "Isto está escrito de forma transparente e directa? As pessoas têm informações suficientes para darem o seu consentimento informado ou revogá-lo facilmente?") Sintonizar - e responder - aos desejos e prioridades dos clientes será fundamental para a empresa estar à prova do futuro quando a privacidade se torna uma prioridade crescente para os consumidores.

3. Os indivíduos devem exercer o seu poder de consumidor reflectindo sobre a privacidade e o que isso significa para eles, além de lutarem pela protecção desses valores. Podem-se iniciar conversas sobre privacidade com amigos, colegas e

comunidades, participando de um consumo consciente da tecnologia - fazendo escolhas informadas sobre os produtos e serviços que trazemos para as nossas vidas. As pessoas que vivem em democracias podem falar com representantes locais e requerer que tomem medidas para melhorar os direitos colectivos para a privacidade. Essas ações aparentemente pequenas e quotidianas, impulsionadas pela clareza de pensamento e intenção, têm o poder de restituir valor aos inumeráveis significados da privacidade - esclarecendo e consolidando o papel da privacidade no presente e no futuro.

?

Sabia que

Entre 2016 e 2018 a largura de banda internacional nas redes globais mais do que duplicou para os 963 Tbps. A cidade com mais capacidade para comunicações internacionais é **Frankfurt (Alemanha), com 86,2 Tbps.**
Seguem-se:

Londres (Reino Unido)	61,8 Tbps
Amesterdão (Holanda)	55,6 Tbps
Paris (França)	54,5 Tbps
Singapura	37 Tbps
Hong Kong (China)	25,3 Tbps
Miami (EUA)	25,1 Tbps
Estocolmo (Suécia)	23,2 Tbps
Marselha (França)	21,9 Tbps
Nova Iorque (EUA)	21.3 Tbps

TeleGeography

Como é que o Facebook sabe tanto sobre mim?

Anna Dorothea Ker

1. Que dados recolhe o Facebook de mim – e como?

O Facebook recolhe o máximo de informações possível sobre os utilizadores - de informações de contacto e localização física a informações muito sensíveis, como as opiniões políticas e o "status" financeiro.

Ao inscrever-se numa conta do Facebook, tem de enviar o seu nome real, sexo, data de nascimento e endereço de e-mail ou número do telemóvel. Em 2019, muita dessa informação de pelo menos 267 milhões de utilizadores foi acedida ilegalmente.

Os utilizadores também são incentivados a acrescentar uma ampla gama de informações pessoais adicionais, do relacionamento pessoal à escola e à cidade actual. Enquanto se navega no site para se envolver com os amigos, comunidades e organizações que segue, o Facebook mantém um registo das actividades do seu comportamento. Isso inclui tudo o que partilha, adiciona, gosta e clica, além de fotos nas quais é marcado e ligações que faz. Esta informação está disponível para visualização em "Your Interests". O Facebook acompanha todas as ligações com amigos (incluindo as pessoas de que você não é amigo) e todos os anúncios que vê e em que clica.

O Facebook também recolhe dados de localização gravando cada endereço IP que você usa quando se liga ao site, solicitando que partilhe a sua localização no *browser* e no telefone e dificultando a sua saída ("opt out"). Essas informações combinadas são usadas para veicular anúncios específicos de locais e documentar os seus movimentos físicos, para que os anunciantes possam rastrear a ligação entre anúncios digitais e compras no mundo real. Em 2018, o Facebook comercializou activamente a Onavo, uma aplicação "spyware" que foi comercializada como sendo uma VPN [rede privada virtual]. A Onavo podia aceder aos dados do telemóvel das pessoas que a instalaram, sendo depois retransmitida para o Facebook. A empresa registou vários pedidos de patentes nos EUA para a tecnologia que permitia prever a sua localização futura, analisando os seus dados de localização anteriores e os dos seus amigos. Embora não seja incomum que as empresas de tecnologia registem patentes para tecnologias que acabam por nunca usar, esta demonstra o interesse do Facebook em desenvolver recursos de processamento para esse tipo muito lucrativo e altamente intrusivo de informação pessoal.

2. O Facebook usa dados de outras fontes para criar o meu perfil?

O Facebook usa ferramentas de rastreamento, listas de contactos e uma complexa rede de aplicações de terceiros ["third-party"] para recolher informações sobre os seus utilizadores e mesmo não utilizadores.

A rede de aplicações de entidades fora do Facebook é um dos principais canais para a recolha de dados. Quando se escolhe a opção "Facebook login" que muitos sites oferecem, isso permite ao site ou à aplicação aceder a informações sobre o utilizador. Exactamente o quê e quanto difere de empresa para empresa, variando do nome e género às listas de amigos. Estas listas são agregadas como "social graph" [mapa digital da personalidade online, dos amigos mais próximos no Facebook e do que é partilhado com eles] e foi o que permitiu à Cambridge Analytica reunir dados sobre tantas pessoas. Na sequência desse escândalo, o Facebook fez

alterações para que as empresas não possam recolher dados sobre os amigos dos utilizadores sem a sua permissão expressa.

Pontos de recolha de dados menos óbvios incluem "plug-ins" sociais que funcionam como rastreadores e são incorporados em sites que não pertencem ao Facebook, como os botões "Like" e "Share" que se vêem pela Web. O Facebook Analytics e os anúncios do Facebook são algumas das outras formas de como a empresa recolhe informações sobre os utilizadores de outros sites e aplicações.

O Facebook também permite que as empresas enviem listas de contactos dos seus utilizadores que desejam segmentar com publicidade. Isso permite às empresas combinarem os utilizadores do Facebook com as suas próprias bases de dados de endereços de e-mail, listas de contactos compradas a intermediários de dados e informações públicas disponíveis, como registos de eleitores [nos EUA], e usem todas essas informações para atingir as desejadas audiências. Pode ver quais as empresas que o seguem clicando em "Settings > Ads > Advertisers and Businesses" (Definições > Anúncios > Anunciantes e empresas).

Entre 2013 e 2018, o Facebook teve o Partner Categories, um programa de licenciamento de dados para melhorar a precisão dos recursos de publicidade direccionada da empresa, usando informações sobre as ações offline de indivíduos. Desde a Datalogix, em 2012, o Facebook começou a licenciar entidades "third-party" de comercialização de dados (incluindo Acxiom, Epsilon, Experian, Oracle Data Cloud, TransUnion e WPP nos EUA) para agregar grandes quantidades de informações sobre os seus utilizadores - principalmente de natureza financeira.

Isso incluiu transações com cartão de crédito, saldos de contas, programas de fidelização e rendimentos. O Facebook pode nunca ter partilhado os seus próprios dados com essas entidades. No entanto, também nunca explicou como o programa Partner Categories realmente funcionava, argumentando que não tinham obrigação de o fazer porque não eram eles que recolhiam as informações. Após esse programa ser criticado em 2018, o Facebook encerrou-o.

3. Pode o Facebook seguir-me se eu não tiver uma conta?

O Facebook pode vigiar as pessoas sem uma conta usando diversas técnicas, desde o "upload" de contactos até a rastreadores noutros sites.

Mesmo se não se tiver uma conta no Facebook, a empresa poderá segui-lo online de duas maneiras principais. O método principal ocorre quando amigos que estão no Facebook optam por enviar os seus contactos pessoais para a rede social para ver quem podem conhecer. Essas informações são combinadas para criar os chamados "shadow profiles" [perfis-sombra] sobre utilizadores que não são do Facebook, que são usados para gerar recomendações de amigos no caso de um novo utilizador se inscrever. Outra maneira que o Facebook pode dizer se duas pessoas se conhecem é vasculhar os metadados das fotos à procura de registos horários e da localização geográfica. Nalguns casos, o Facebook pode comparar a poeira e os riscos das lentes nas câmaras que tiraram as fotos.

Enquanto se navega na Web, muitos sites usam ferramentas de analítica e rastreamento como o Facebook Pixel e outras APIs [de "application programming interface"] sociais para seguir os

?

Sabia que

A Alphabet (Google) lucrou 98 mil milhões de dólares no ano passado. Revelou também, pela primeira vez, que o YouTube atingiu os 15 mil milhões de dólares em publicidade (36% de crescimento relativamente a 2018), tem três mil milhões de assinaturas nos canais pagos Music e Premium, e cresceu no negócio da cloud 53% para os 10 mil milhões de dólares.

Alphabet

visitantes. Essas informações são devolvidas ao Facebook e usadas para redirecionar anúncios, que o seguem pela Web, entre outros propósitos. As ferramentas de rastreamento do Facebook foram encontradas em 30% dos principais 10 mil sites - incluindo sites pornográficos, como revelou um estudo de 2018.

4. O Facebook vende os meus dados?

Mark Zuckerberg testemunhou que o Facebook não vende directamente os dados do utilizador. Mas os dados são como a empresa ganha dinheiro - vendendo aos anunciantes o acesso ao utilizador como consumidor.

O Facebook mantém que não vende dados sobre os seus utilizadores. Estes dados são o activo mais valioso do Facebook; portanto, é do interesse da empresa manter a propriedade dos mesmos. Em vez disso, a empresa vende o acesso aos utilizadores para que as empresas possam alcançar as audiências que querem através da publicidade altamente segmentada. Uma das maneiras como o Facebook faz isso é com uma longa lista de características pessoais, "categorias de interesse" ou "atributos únicos" - desde raça, sexo e estado civil ao nível de rendimentos. Num estudo de 2016, o ProPublica recolheu 52 mil desses atributos exclusivos, submetidos pelos utilizadores - incluindo alguns obscuros, como "Fingir Escrever em Situações Embaraçosas". O Facebook permite que os anunciantes escolham uma seleção personalizada desses atributos para exibirem anúncios para os tipos específicos de pessoas que desejam segmentar. Por exemplo, um novo ginásio de luxo em Nova Iorque pode solicitar ao Facebook que mostre os seus anúncios a mulheres entre os 25 e os 35 anos que moram em Manhattan, ganham mais de 60 mil dólares por ano e estão interessadas em "fitness pessoal", "roupas desportivas" e "vida saudável".

Além do lucro que o Facebook obtém com a venda do acesso aos dados do utilizador, a empresa possui um histórico de partilha de dados de forma intrusiva e não consensual. Uma investigação em 2018 do The New York Times revelou os "acordos especiais" que o Facebook estabeleceu com as empresas de Big Tech entre 2010 e 2018 à procura de um forte crescimento. Isso incluía permitir que o Netflix e o Spotify lessem as mensagens privadas de um utilizador do Facebook, permitir que o Bing da Microsoft visse quase todos os amigos de um utilizador do Facebook sem consentimento, permitir à Amazon captar as informações de contacto do utilizador através dos seus amigos no Facebook e permitir que o Yahoo visse textos de amigos no Facebook - apesar de declarar publicamente que tinha parado com essa prática em 2014.

5. O Facebook ouve as minhas conversas?

O Facebook negou repetidamente ouvir as conversas dos seus utilizadores através de microfones. Mas uma variedade de outras pistas de onde recolhe informações - e a maneira como combina essas informações para exibir anúncios - é ainda mais invasiva.

Você já viu um anúncio no Facebook ou no Instagram sobre um produto que nunca procurou, nunca mencionou num email ou escreveu de qualquer outra forma no seu telefone - mas mencionou recentemente a um amigo? Quando aqueles ténis de nicho de que falou próximo do telemóvel aparecem num anúncio no dia seguinte, é demasiado estranho para ser uma coincidência. Provavelmente não é o seu microfone que está a ouvir. O Facebook negou repetidamente isso – num artigo no

seu blogue em 2016 e perante o Congresso dos EUA.

Confie-se ou não em Mark Zuckerberg, as razões técnicas que limitam a espionagem por microfone pelo Facebook são convincentes - pode não valer a pena. Como o engenheiro do Facebook, Antonio Garcia Martinez, explicou na revista Wired, "a vigilância constante por áudio produziria cerca de 33 vezes mais dados por dia do que o Facebook actualmente consome. Tal espionagem seria eminentemente detectável, gerando quantidades visíveis de dados no seu smartphone quando o Facebook manteria uma ligação sempre activa para Zuckerberg". Um estudo de 2018 realizado por investigadores da Northeastern University apoia isso - não encontraram provas de que as aplicações do Facebook activassem o microfone sem permissão expressa, nem que ficheiros de áudio fossem transmitidos a partir de telemóveis.

Em 2018, o Facebook lançou um dispositivo de "smart video" chamado Portal, que permite aos clientes efectuar chamadas pela Internet. Sabemos que o Facebook analisa os dados de utilização do Portal, como a duração e frequência das chamadas, para dar anúncios segmentados aos utilizadores. Embora o Facebook afirme que tem uma postura centrada na privacidade com o produto, também se sabe que usam gravações transcritas para treinar a inteligência artificial que alimenta o Portal. Não há provas de que o Portal também esteja a registar as conversas e a transmiti-las para seres humanos, como os dispositivos Alexa da Amazon foram apanhados a fazer, mas os utilizadores preocupados com a privacidade serão cautelosos.

O Facebook está relutante em enfrentar o problema, devido ao risco de a empresa ser obrigada a explicar a real infra-estrutura que suporta o seu complexo sistema de publicidade comportamental - que é sem dúvida mais invasivo do que simplesmente escutar pelos microfones do telemóvel. Os perfis claramente definidos que permitem ao Facebook veicular publicidade altamente específica são criados por meio de uma combinação de todos os dados que recolhem na Internet. Estes dados são recolhidos, agregados e analisados com tanta eficácia para nos servir conteúdo e anúncios que parece que o Facebook nos escuta.

6. Como posso parar o Facebook de me seguir e reclamar o controlo sobre os meus dados?

Além de eliminar [as aplicações do] Facebook e das suas subsidiárias Instagram e WhatsApp, existem várias etapas que se podem executar - na própria plataforma e em medidas externas - para recuperar pelo menos um certo grau de controlo sobre os seus dados.

Apagar o Facebook

A solução mais eficaz é, claro, apagar todas as suas contas nos serviços detidos pelo Facebook - isso significa também o Instagram e o WhatsApp. Se estiver pronto para mergulhar na sua privacidade, não se esqueça de antes copiar os seus dados do Facebook. (Settings > Your Facebook Information, ou Definições > A Sua Informação). No entanto, se mantiver a(s) sua(s) conta(s) do Facebook, existem algumas medidas defensivas que pode tomar.

Limite as informações que o Facebook sabe sobre si:

- Veja que dados o Facebook e os anunciantes têm e bloqueie o acesso: Settings>Ads>Ad Settings (Definições > Anúncios > Definições de anúncios).

- Bloqueie o acesso do Facebook ao seu microfone e localização.

- Faça um Privacy Checkup no Facebook para saber que informação pode remover.

- Reveja todas as aplicações "third-party" ligadas à sua conta do Facebook e remova o seu acesso.

- Apague a informação que partilhou anteriormente com o Facebook: dados pessoais (número de telefone, data de nascimento, preferências de personalidade), textos antigas, fotos etc.

- Desmarque-se e aos seus amigos das fotos para evitar o treino das ferramentas de reconhecimento facial em evolução do Facebook.

Limite as informações que os parceiros e rastreadores do Facebook sabem sobre si:

- Pare de usar a opção "fazer login com o Facebook" em todos os sites e aplicações que o permitem e mude para um gerador de passwords que crie uma única e segura para cada site.

- Instale uma extensão no browser bloqueadora de rastreadores, como o Privacy Badger, para impedir o rastreamento pelo Facebook Pixel e pelo botão "Like" do Facebook.

Use uma VPN com uma ferramenta integrada de rastreamento. Descubra o recurso Anti-Tracker da IVPN.

Consulte o guia da indústria "adtech" que contém recomendações e estratégias simples de auto-defesa digital.

?

Sabia que

Em 2023 os utilizadores da Internet devem crescer para 5,3 mil milhões e para 5,7 mil milhões de utilizadores de telemóveis.

Cisco

Privacidade ou vigilância por design: questões fundamentais num mundo ligado através da IoT

Alexander Hanff

Co-fundador da Think Privacy AB. *Texto publicado originalmente na revista Third.digital, reproduzido sob autorização.*

Apesar das obrigações legais já com uma década, os dispositivos IoT falham progressivamente no que diz respeito à Ética de Dados, com cada vez mais dispositivos a recolher vastas quantidades de dados para fins alheios à sua necessidade de operar.

Há um mundo de que muitos não estão cientes de que existe, nem do impacto que este tem no nosso dia a dia. A Internet of Things (IoT ou Internet das Coisas) não é um novo ecossistema, tendo já algumas décadas, mas à medida que nos esforçamos para tornar as nossas tecnologias "burras" em inteligentes, enfrentamos novos riscos que ameaçam a nossa própria existência como seres autónomos.

Nos últimos anos, temos visto uma moda crescente em conectar tudo à IoT e da perspetiva do consumidor, tal é bastante cómodo; ser capaz de monitorizar a casa quando se está fora numa viagem de negócios ou conseguir que os eletrodomésticos encomendem as compras automaticamente quando a despensa está vazia, pode parecer uma situação em que todos saem a ganhar.

Mas o que muitas pessoas não compreendem é que com este acréscimo de comodidade, vem também uma verdadeira ameaça aos seus direitos fundamentais. À medida que os fabricantes que vendem estes dispositivos, juntamente com os fornecedores de serviços que os apoiam, se esforçam para recolher cada vez mais dados para fins que nada têm a ver com a sua necessidade de operar, mas, sim com o capitalismo da vigilância. O que queremos dizer com capitalismo de vigilância é que esta vigilância digital do nosso comportamento, das nossas interações, das nossas preferências e das nossas opiniões está a ser transformada numa arma "contra nós com eficiência militar"[1]?

Através do uso de sensores, microfones e câmaras, as nossas casas tornaram-se fonte para uma indústria multimilionária, centrada em torno da análise do *Big Data*, uma indústria assente em dados extraídos de forma clandestina, sem custos, sob o disfarce de "inteligente".

À medida que as nossas vidas se tornam mais complexas, num mundo aparentemente apanhado num fluxo constante de mudanças rápidas, a comodidade torna-se numa oferta atrativa, especialmente quando o preço por esta comodidade é visto de maneira tão competitiva ou mesmo gratuita.

Como funciona o capitalismo de vigilância: o lado negro por detrás da conveniência

A verdade é que estes produtos e serviços não são concebidos para melhorar as nossas vidas, mas sim para recolher o máximo possível do "excedente comportamental"[2], ou seja, informação que pode ser extraída através do uso de tecnologias que podem ser utilizadas para outros fins. No caso do capitalismo

de vigilância, isto significa normalmente que estes dados irão ser utilizados para construir perfis que permitam a manipulação do comportamento através da análise psicológica. Esta manipulação poderá ser feita para nos persuadir a comprar um produto específico ou um serviço (publicidade comportamental), ou poderá mesmo ser usada de outras formas, como influenciar a forma como votaríamos numa eleição política.

Há inúmeros exemplos de produtos que foram usados desta maneira. A "My Friend Cayla"[3], uma boneca inteligente que pedia informação pessoal às crianças e que era capaz de ter conversas básicas com os seus donos, foi retirada das lojas por todo o mundo após se ter descoberto que a tecnologia dentro da boneca gravava as conversas e as enviava de volta para os servidores da empresa para análise. Ao longo do Verão de 2019, houve vários escândalos associados aos "Smart Assistants" (assistentes inteligentes), envolvendo todos os dispositivos convencionais da Google, Amazon, Microsoft e da Apple, quando se descobriu que as gravações das interações com estes dispositivos estavam a ser enviadas de volta aos seus centros de dados e ouvidos pelo seu "staff"[4].

Para piorar a situação, foi descoberto que estas gravações incluíam um número significativo de "falsos positivos", em que os dispositivos tinham gravado eventos que não era suposto terem sido considerados como interações por estes (como casais a discutir, actividades sexuais[5], etc.).

Em várias ocasiões, os dispositivos que compramos para acrescentar à nossa "casa inteligente" estão cada vez mais concebidos para deixar de funcionar, caso decidamos que não queremos que estes gravem informação sobre as nossas vidas diárias, mesmo que essa informação não seja necessária para o dispositivo funcionar. Por exemplo, um conhecido fabricante de colunas "inteligentes" lançou uma actualização de *software* nos seus dispositivos IoT conectados, em que caso o proprietário se recusasse a aceitar as políticas de recolha de dados, o dispositivo parava simplesmente de funcionar[6]. Estes dados não eram necessários para o dispositivo funcionar, aliás, antes de o *software* ter sido actualizado remotamente, as colunas funcionavam perfeitamente. Isto foi simplesmente o caso de pôr os clientes na situação desagradável de "dá-nos os teus dados ou estragamos o teu caro dispositivo". Em qualquer outra situação, tal seria considerado chantagem ou extorsão e visto como um acto criminoso, porém no mundo da IoT, isto está a tornar-se rapidamente no procedimento típico.

Ao abrigo da legislação europeia como o Regulamento Geral para a Proteção de Dados (RGPD) e a Diretiva de Privacidade e Comunicações Eletrónicas, este comportamento é considerado ilegal. Por exemplo, nos termos do RGPD, o consentimento não é considerado válido se "a prestação de um serviço depender do consentimento, apesar de este não ser necessário para o desempenho"[7] e a directiva Relativa à Privacidade e às Comunicações Eletrónicas (e-Privacy) requer que seja solicitado o consentimento para qualquer armazenamento ou acesso a quaisquer informações já armazenadas no dispositivo do utilizador

final, que não sejam consideradas como "estritamente necessárias" para o desempenho do serviço solicitado[8].Como tal, no caso da já referida coluna inteligente, pode argumentar-se que obrigar clientes a consentir em actividades de processamento de dados desta natureza, sob a ameaça de desativação das suas colunas, não cumpre os requisitos de nenhuma das leis. Contudo, a falta de reforço de ambas as leis (até recentemente) levou a uma série de abusos.

Para além disso, o RGPD requer que todos os produtos e serviços que envolvam o processamento de dados pessoais devam implementar os princípios da "Privacidade por *Design*" (daí o título deste artigo). Porém, a prática comum é a da "Vigilância pela Concepção", de forma a absorver todo o excedente comportamental. Claro que as empresas por detrás de todos estes produtos juram levar a sério a privacidade e explicam as suas práticas apenas nas profundezas das suas políticas de privacidade, que são tão inacessíveis ao "consumidor comum" que se tornam inúteis.

No ensaio "The Cost of Reading Privacy Policies"[9], Aleecia McDonald e Lorie Faith Cranor salientaram que "o custo de oportunidade nacional do tempo de leitura de políticas está na ordem dos 781 mil milhões de dólares" se cada utilizador da Internet nos EUA lesse as políticas de privacidade associada aos serviços que estes usam - o que é efetivamente considerada uma estimativa prudente. Apesar do ensaio já ter mais de uma década e os requerimentos ao abrigo do RGPD serem que tais avisos estejam numa linguagem simples e compreensiva, pouco mudou na prática[10] com as várias políticas de privacidade a ainda consistirem num muro de texto em linguagem jurídica que poucos entenderiam e muitos menos leriam.

O caso Withings

Num recente caso-teste apresentado pelo autor, juntamente com o regulador francês de privacidade e proteção de dados Comission Nationale de l'Informatique et des Libertés (CNIL), contra um fabricante de balanças "inteligentes", este modelo foi entretanto contestado.

Neste caso particular, após adquirir a balança inteligente Withings Body+ foi descoberto que, de maneira a usar efectivamente as funções dos aparelhos para rastrear os vários atributos relacionados como o peso, o IMC [índice de massa corporal], entre outros, é necessário instalar uma aplicação chamada Health Mate no smartphone.

Na altura, pareceu uma situação razoável, pois era possível monitorizar, receber gráficos e tabelas interessantes para mostrar progresso (ou a falta deste) ao longo do tempo. Os problemas não se manifestaram até ao ponto em que, de forma a instalar a aplicação Health Mate, ter de se concordar com a "política de privacidade" da Withings. Ao ler a política de privacidade, torna-se rapidamente evidente que a Withings quer a sua parte do excedente comportamental para propósitos de "marketing, publicidade e recomendações"[11]

e a não ser que se dê o consentimento de tal instalação de actividades da aplicação não se pode completar [a sua activação], o que torna estas balanças "inteligentes" (e nada baratas) Body+ estúpidas de novo - indo, assim, contra o propósito para o qual foi adquirida.

Não há informação relacionada com este assunto no momento da venda, no embalamento ou mesmo na caixa. A primeira vez que se sabe do assunto é na instalação da aplicação e mesmo aí só se se for um "nerd" dedicado à privacidade e disposto a ler o texto, ao invés de apenas clicar no tão apelativo botão "Aceitar".

Provavelmente, o que muitos não entendem é que estas balanças Body+ Scales, assim como a Alexa da Amazon, a cama EightSleep, a Smart TV da Samsung, o rastreador de fitness Fitbit e os milhares de outros dispositivos IoT interconectados são todos considerados "dispositivos terminais" sob a Directiva e-Privacy na UE. Além disso, todos estão sob a jurisdição do requerimento específico para obtenção de consentimento ou do armazenamento de informação nestes "dispositivos terminais".

Além disso, desde a introdução do RGPD (de onde a Directiva e-Privacy vai buscar a definição de consentimento), esse consentimento tem que ser dado livremente, tem que ser estritamente necessário para o funcionamento do dispositivo ou para o fornecimento do serviço pedido e o acesso ao serviço não pode ser retirado, caso não se dê o consentimento para o processamento do excedente comportamental.

Este artigo não poderia sair numa altura mais oportuna, pois o Tribunal de Justiça da União Europeia [TJUE] publicou a 1 de Outubro de 2019 a decisão do Caso c-673/17(Planet 49)[12], reiterando os requerimentos de consentimento nestas circunstâncias – abrindo portas a um *tsunami* de queixas judiciais contra empresas que operavam, até agora, num vácuo regulatório pois, apesar de já existir a lei, esta raramente foi executada na última década. No caso contra a Withings, o autor apresentou uma queixa que abrangia vários assuntos abordados neste artigo. No que diz respeito aos requerimentos de consentimento para concordar com a política de privacidade da Withings, de maneira a completar a instalação da aplicação Health Mate e, portanto, a aceder a todas as ferramentas publicitadas com as balanças Body+, tem se discutido que tudo acima referido não cumpre os requerimentos de consentimento válido ao abrigo do RGPD.

A Withings argumenta, obviamente, que a empresa envia os dados para a sua *cloud* com o objetivo de fornecer gráficos e análises ao utilizador (que é uma maneira bastante conveniente para obter dados para outros propósitos, tais como as suas actividades relacionadas com marketing). Porém, o autor salienta que esses dados podem ser processados na aplicação no próprio smartphone, seguindo assim os princípios da "Privacidade by Design", como é exigido pelo RGPD.

?

Sabia que

A empresa de comércio electrónico Amazon é o maior anunciante publicitário. Em 2019, investiu 11 mil milhões de dólares (2% do mercado global de publicidade). O aumento de 3,8 mil milhões de dólares relativamente ao ano anterior foi de 34% quando as vendas só aumentaram 20% para 280,5 mil milhões de dólares.

Campaign

Outras questões como o facto de os dados relacionados com a saúde serem considerados uma categoria de dados especial e, daí, exigirem uma abordagem mais rigorosa para os processar do que a outros tipos de dados pessoais, foram também incluídas na queixa.

Antes do julgamento do TJUE quanto ao Planet 49, houve um pequeno sinal de decisão favorável, reforçando os direitos fundamentais que foram dados pelo direito europeu, mas dada a nova jurisprudência, está-se esperançoso que a CNIL irá efectivamente reforçar o RGPD e a Diretiva e-Privacy neste caso particular.

A necessidade de proteger a privacidade de maneira a proteger a humanidade

O autor não é de maneira nenhuma um caso isolado. Há uma estimativa de sete mil milhões de dispositivos IoT actualmente implementados no mundo, um número que se estima vá triplicar nos próximos cinco anos e ultrapassar os 21 mil milhões[13]. Enquanto muitos destes dispositivos até agora têm sido instalados para fins industriais, a razão para o crescimento explosivo previsto nos próximos cinco anos deve-se à emergência e aceitação aceleradas de dispositivos de consumo inteligentes pessoais e ao desenvolvimento de ambientes e cidades inteligentes. Tudo isto ampliará o processamento do excedente comportamental e os riscos dos nossos direitos fundamentais.

Muitos podem questionar porque pode alguém ficar preocupado com estas actividades de processamento, que removem as tarefas mundanas do dia-a-dia e se não há nada a esconder, não há nada a temer...

A realidade é muito diferente, tal como se viu com o escândalo da Cambridge Analytica, estes dados podem ser usados como armas - Tim Cook não estava a ser alarmista. A nossa democracia está, de facto, em risco de manipulação do eleitorado baseada nos seus perfis comportamental e psicográfico.

Mas é ainda mais sério do que apenas a nossa democracia. O risco do capitalismo de vigilância cria e estende-se para o núcleo da nossa espécie – o eu. Se através da observação constante e o processamento do excedente comportamental nos estamos a tornar cada vez mais um objecto de manipulação, então o impacto na autonomia, autodeterminação e agência é profundo.

Se as próprias decisões que estamos a tomar no nosso dia-a-dia estão a ser manipulada através de operações psicológicas ("psyops") concebidas para obter uma reacção emocional, em vez de racional, perdemos as liberdades que nos definem como espécie.

Conceitos como a liberdade de expressão, liberdade de associação, opinião, pensamento e qualquer outro tipo de liberdade a que nos agarramos com tanta força e protegemos como um direito fundamental do Homem, deixam de existir.

Como a psicologia nos ensinou, quando as pessoas se apercebem que estão a ser observadas, mudam o seu comportamento (conhecido como o "Efeito Hawthorne") e este torna-se artificial. Isto nunca foi mais claro do que com a emergência do sistema do crédito social, agora instalado na China, onde através da constante monitorização de toda a gente, o governo chinês procura controlar o comportamento de toda a população.

E se perdermos todas estas liberdades, o que quer isto dizer para as futuras gerações e para o futuro da raça humana e sociedade? Se perdermos a liberdade de pensamento, expressão e associação devido à constante manipulação do comportamento através de psicográficos e vigilância, o que quer isto dizer para a futura inovação num mundo onde só se pensa no que se é incentivado e só se experimenta aquilo que as corporações globais querem que se experimente?

Mas o que é que podemos fazer sobre isso?

Felizmente, o ambiente legislativo está a começar a recuperar o atraso. Há um movimento global com objetivo de chegar a mais leis de proteção da privacidade, como o RGPD na UE.

Como indivíduos, é preciso que prestemos mais atenção aos dispositivos, aos produtos e aos serviços que se usa e é simplesmente preciso parar de clicar em "Aceitar" para aceder a estes dispositivos, produtos e serviços.

Jamais se iria sugerir que nos devíamos todos excluir do mundo digital, assim de repente. Mas apenas que estejamos meramente mais vigilantes e que tomemos os passos adequados de forma a responsabilizar quem procura explorar os nossos direitos.

Não custa nada apresentar uma queixa ao Regulador na UE por isso, quando se deparar com um serviço ou produto que requeira um consentimento para processar os seus dados de uma maneira que não é necessária para o funcionamento do próprio produto ou serviço, apresente uma queixa.

Lembre-se, se alguma coisa é grátis, o mais provável é que você seja o produto. A única forma de poder dar a volta a isto e mitigar os riscos resumidos neste artigo é tomar uma posição, exercer os nossos direitos e garantir que as nossas futuras gerações terão as mesmas oportunidades e liberdades que tínhamos antes da emergência do capitalismo de vigilância.

Pois, ao falharmos em não agir agora, o futuro já está perdido.

1 "Tim Cook: personal data being 'weaponised'"

2 Shoshana Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power"

3 "Connected toys violate European consumer law"

4 "Yep, human workers are listening to recordings from Google Assistant, too"

5 "Amazon staff 'listen to users having sex' on Alexa recordings, report claims"

6 "Rejecting Sonos' private data slurp basically bricks bloke's boombox"

7 "General Data Protection Regulation (Recital 43)"

8 "Directive on privacy and electronic communications (Article 5(3))"

9 "I/S: A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review"

10 "Most EU cookie 'consent' notices are meaningless or manipulative, study finds"

11 "Privacy Policy for Withings Products and Services"

12 Processo C-673/17: Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV contra Planet49 GmbH.

13 "How Many IoT Devices Are There?"

Sabia que

Em 2018, contavam-se 10 mil milhões de dispositivos da Internet of Things (IoT). Este ano, esse valor deve crescer para 30 mil milhões a 50 mil milhões e chegar aos 74 mil milhões em 2025. E 33 milhões de dispositivos IoT são activados por comandos vocais.

Policy Horizons Canada, Bernard Marr

Os dados não dormem

A cada minuto, uma avalanche de bits circula pelos cabos de telecomunicações de e para os centros de dados, onde são processados, guardados e expedidos para os utilizadores.

De mensagens em equipamentos móveis a páginas da Web, o enorme fluxo tem vindo a crescer e não dá sinais de estagnar ou diminuir. O termo Big Data faz todo o sentido neste enorme mundo de conjuntos gigantescos de dados.

Desde 2013, a Domo tem revelado o conjunto "Data Never Sleeps", uma série de infografias com as quantidades de dados que circulam a cada 60 segundos na Internet. Para contextualizar estes fluxos, cada dia tem 1.440 minutos.

No ano passado, em termos globais, o motor de busca **Google** processou 4,497 milhões de pesquisas por minuto – mais do dobro dos 2 milhões de há sete anos.

Nesse espaço de tempo, colocaram-se 511,2 mil mensagens no **Twitter** (foram apenas 100 mil em 2013) e, em média, o **Facebook** registou um milhão de utilizadores a ligarem-se à sua rede social.

O **Netflix** emitiu 694.444 horas de conteúdos por minuto, enquanto o **YouTube** registou 4,5 milhões de vídeos por minuto em 2019. Sete anos antes, recebia uma média de 48 horas de novos vídeos a cada 60 seguntos.

O **Instagram** atingiu as 55.140 novas fotos partilhadas, quando eram apenas 3.600 em 2013. São enviadas mais de 18 mil milhões de mensagens de texto mas os emails chegam aos 188 milhões por minuto.

2013

EVERY MINUTE of the DAY

THE MOBILE WEB RECEIVES 217 NEW USERS.

YOUTUBE USERS UPLOAD 48 HOURS OF NEW VIDEO.

EMAIL USERS SEND 204,166,667 MESSAGES.

GOOGLE RECEIVES OVER 2,000,000 SEARCH QUERIES.

FACEBOOK USERS SHARE 684,478 PIECES OF CONTENT.

WORDPRESS USERS PUBLISH 347 NEW BLOG POSTS.

571 NEW WEBSITES ARE CREATED.

CONSUMERS SPEND $272,070 ON WEB SHOPPING.

FOURSQUARE USERS PERFORM 2,083 CHECK-INS.

TWITTER USERS SEND OVER 100,000 TWEETS.

FLICKR USERS ADD 3,125 NEW PHOTOS.

INSTAGRAM USERS SHARE 3,600 NEW PHOTOS.

TUMBLR BLOG OWNERS PUBLISH 27,778 NEW POSTS.

BRANDS & ORGANIZATIONS ON FACEBOOK RECEIVE 34,722 "LIKES."

APPLE RECEIVES ABOUT 47,000 APP DOWNLOADS.

WITH NO SIGNS OF SLOWING, THE DATA KEEPS GROWING

These are just some of the more common ways that Internet users add to the big data pool. In truth, depending on the niche of business you're in, there are virtually countless other sources of relevant data to pay attention to. Consider the following:

The global Internet population grew 6.59 percent from 2010 to 2011 and now represents 2.1 BILLION PEOPLE.

These users are real, and they are out there leaving data trails everywhere they go. The team at Domo can help you make sense of this seemingly insurmountable heap of data, with solutions that help executives and managers bring all of their critical information together in one intuitive interface, and then use that insight to transform the way they run their business. To learn more, visit www.domo.com.

DOMO

SOURCES: HTTP://NEWS.INVESTORS.COM/, ROYAL.PINGDOM.COM, BLOG.GROVO.COM, BLOG.HUBSPOT.COM, SIMPLYZESTY.COM, PCWORLD.COM, BIZTECHMAGAZINE.COM, DIGBY.COM

2014

EVERY MINUTE OF THE DAY

PINTEREST USERS PIN 3,472 images.

YOUTUBE USERS UPLOAD 72 HRS. OF NEW VIDEO.

EMAIL USERS SEND 204,000,000 MESSAGES.

Google RECEIVES OVER 4,000,000 SEARCH QUERIES.

VINE USERS SHARE 8,333 VIDEOS.

FACEBOOK USERS SHARE 2,460,000 PIECES OF CONTENT.

SKYPE USERS CONNECT FOR 23,300 HOURS.

TINDER USERS SWIPE 416,667 TIMES.

YELP USERS POST 26,380 REVIEWS.

WHATSAPP — USERS SHARE — 347,222 PHOTOS.

APPLE USERS DOWNLOAD 48,000 apps.

TWITTER USERS TWEET 277,000 TIMES.

PANDORA USERS LISTEN TO 61,141 HOURS OF music.

AMAZON MAKES $83,000 IN ONLINE SALES.

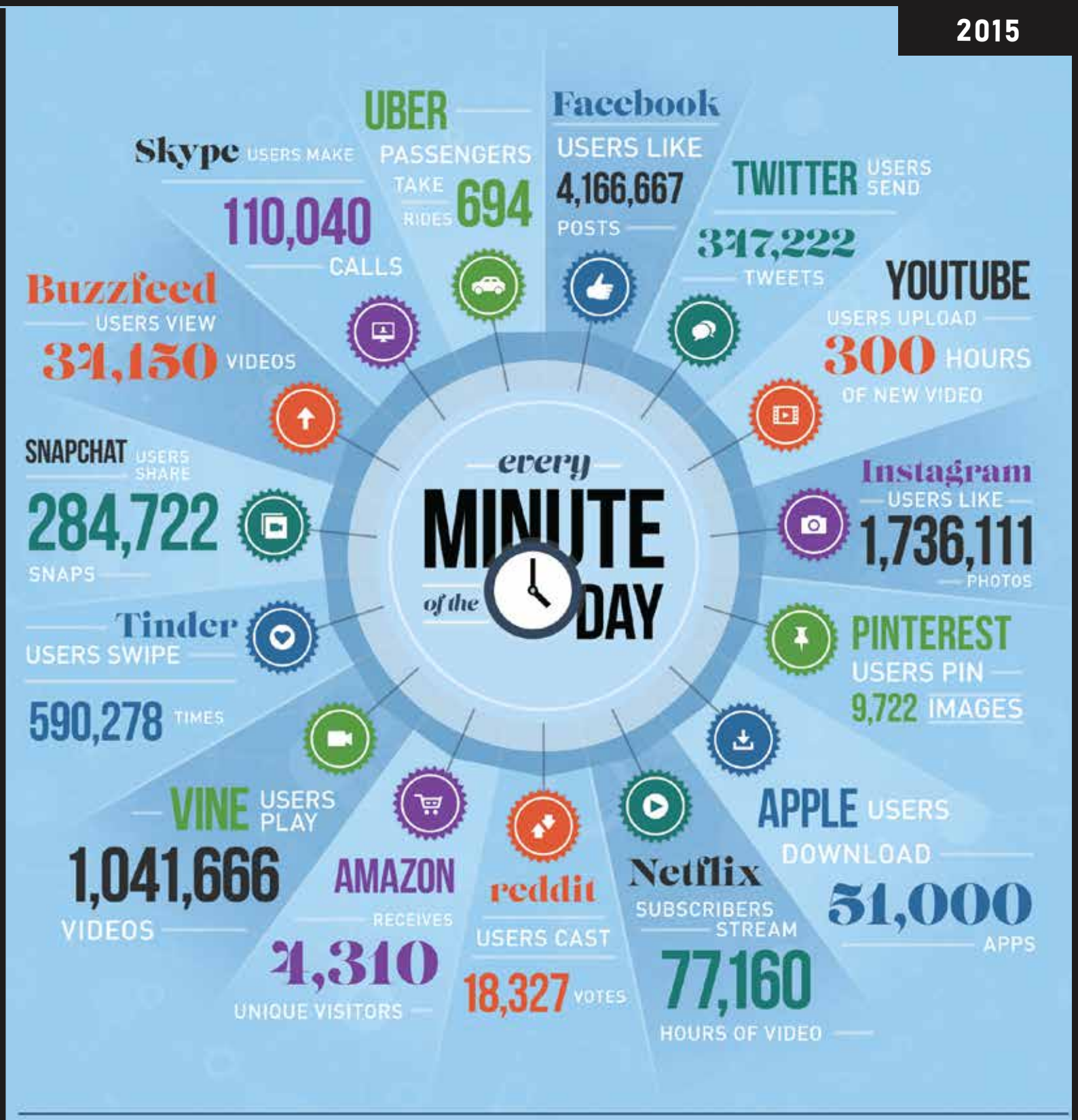
INSTAGRAM USERS » POST 216,000 NEW PHOTOS.

THE GLOBAL INTERNET POPULATION GREW 14.3% FROM 2011 - 2013 AND NOW REPRESENTS **2.4 BILLION PEOPLE.**

With each click, share and like, the world's data pool is expanding faster than we can comprehend. Businesses today are paying attention to scores of data sources to make crucial decisions about the future. The team at Domo can help your business make sense of this endless stream of data by providing executives with all their critical information in one intuitive platform. Domo delivers the insights you need to transform the way you run your business. Learn more at www.domo.com.

DOMO

SOURCES:
BITS.BLOGS.NYTIMES.COM, INTEL.COM, APPLE.COM, TIME.COM, DAILYMAIL.CO.UK, SKYPE.COM, STATISTICBRAIN.COM



THE GLOBAL INTERNET POPULATION GREW **18.5%** FROM 2013–2015 AND NOW REPRESENTS **3.2 BILLION PEOPLE.**

With each click, share and like, the world's data pool is expanding faster than we can comprehend. Businesses today are paying attention to scores of data sources to make crucial decisions about the future. The team at Domo can help your business make sense of this endless stream of data by providing executives with all their critical information in one intuitive platform. Domo delivers the insights you need to transform the way you run your business. **Learn more at www.domo.com.**

DOMO

SOURCES:

FACEBOOK, TWITTER, YOUTUBE, INSTAGRAM, PINTEREST, APPLE, NETFLIX, REDDIT, AMAZON, TINDER, BUZZFEED, STATISTA, INTERNET LIVE STATS, STATISTICBRAIN.COM

2016 every MINUTE of the DAY

PRESENTED BY DOMO

BUZZFEED USERS VIEW **159,380** PIECES OF CONTENT

SNAPCHAT USERS WATCH **6,944,444** VIDEOS

Netflix SUBSCRIBERS STREAM **86,805** HOURS OF VIDEO

GOOGLE TRANSLATES **69,500,000** WORDS

Americans USE **18,264,840** MEGABYTES OF WIRELESS DATA

YOUTUBE USERS SHARE **400** HOURS OF NEW VIDEO

Instagram USERS LIKE **2,430,555** POSTS

FACEBOOK MESSENGER USERS SHARE **216,302** PHOTOS

SIRI ANSWERS **99,206** REQUESTS

Amazon MAKES **$222,283** IN SALES

Tinder USERS SWIPE **972,222** TIMES

3,567,850 TEXT MESSAGES ARE SENT IN THE **U.S.**

Giphy SERVES **569,217** GIFS

TWITTER USERS SEND **9,678** EMOJI-FILLED TWEETS

Dropbox USERS UPLOAD **833,333** NEW FILES

THE WEATHER CHANNEL RECEIVES **13,888,889** FORECAST REQUESTS

GLOBAL INTERNET POPULATION GROWTH 2012–2016
(IN BILLIONS)

Data has become the new enterprise currency. The ability to collect, analyze, and leverage it effectively will distinguish the best from the rest. Domo helps you stay ahead by bringing your data and people together in the cloud, where everyone in your organization can easily access the information they need to make faster, better-informed decisions and optimize business performance.

Learn more at www.domo.com

DOMO

SOURCES: SNAPCHAT, NETFLIX, GOOGLE, INSTAGRAM, TINDER, THE WEATHER COMPANY, DROPBOX, GITHUB, GIPHY, YOUTUBE, BUZZFEED, AMAZON, CTIA, MARY MEEKER'S 2016 INTERNET TRENDS REPORT, USA TODAY, GLOBAL WEB INDEX

2017

2017 every MINUTE of the DAY

PRESENTED BY DOMO

THE WEATHER CHANNEL
RECEIVES 18,055,555.56 FORECAST REQUESTS

GIPHY
SERVES 694,444 GIFS

NETFLIX
USERS STREAM 69,444 HRS OF VIDEO

SNAPCHAT
USERS SHARE 527,760 PHOTOS

LINKEDIN
GAINS 120+ NEW PROFESSIONALS

AMAZON
MAKES $258,751.90 IN SALES

YOUTUBE
USERS WATCH 4,146,600 VIDEOS

TUMBLR
USERS PUBLISH 74,220 POSTS

TWITTER
USERS SEND 456,000 TWEETS

103,447,520 SPAM EMAILS SENT

15,220,700 TEXTS SENT

WIKIPEDIA
USERS PUBLISH 600 NEW PAGE EDITS

SKYPE
USERS MAKE 154,200 CALLS

GOOGLE
CONDUCTS 3,607,080 SEARCHES

INSTAGRAM
USERS POST 46,740 PHOTOS

BUZZFEED
USERS VIEW 50,925.92 VIDEOS

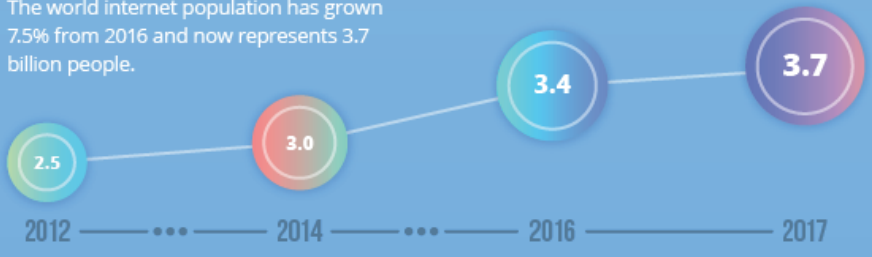
VENMO
PROCESSES $51,892 PEER-TO-PEER TRANSACTIONS

UBER
RIDERS TAKE 45,787.54 TRIPS

SPOTIFY
ADDS 13 NEW SONGS

AMERICANS
USE 2,657,700 GB OF INTERNET DATA

The world internet population has grown 7.5% from 2016 and now represents 3.7 billion people.



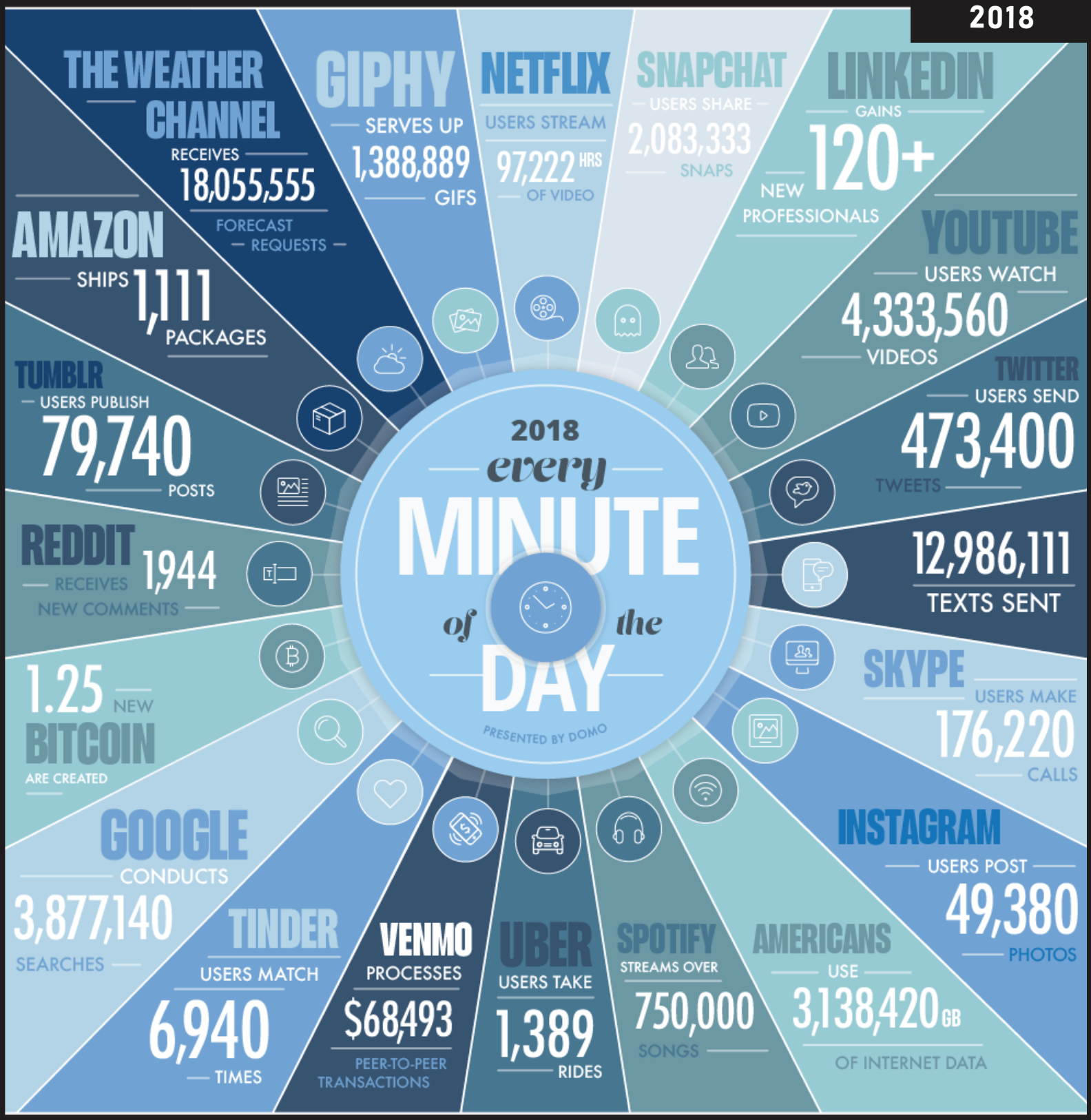
GLOBAL INTERNET POPULATION GROWTH 2012–2017
(IN BILLIONS)

With each click, swipe, share, and like, businesses are using data to make decisions about the future. Domo gives everyone in your business real-time access to data from virtually any data source in a single platform for smarter decision-making at any moment.

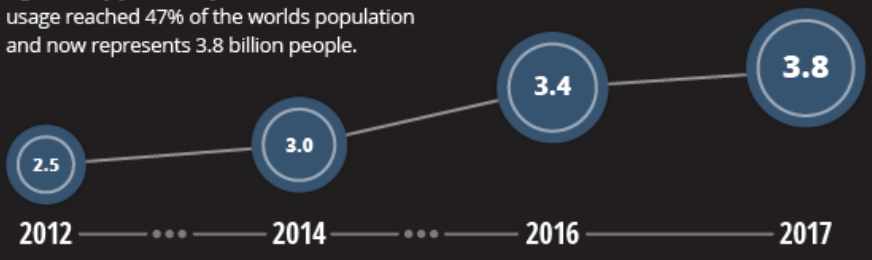
Learn more at domo.com

SOURCES: EXPANDEDRAMBLINGS.COM, WEARESOCIAL.COM, WIKIPEDIA, FORBES, ADWEEK.COM, FORTUNE.COM, BLOOMBERG.COM, ONEREACH.COM, IBM, BUZZFEED, INTERNET LIVE STATS, INTERNET WORLD STATS, BBC

DOMO



The world's internet population is growing significantly year-over-year. In 2017, internet usage reached 47% of the worlds population and now represents 3.8 billion people.



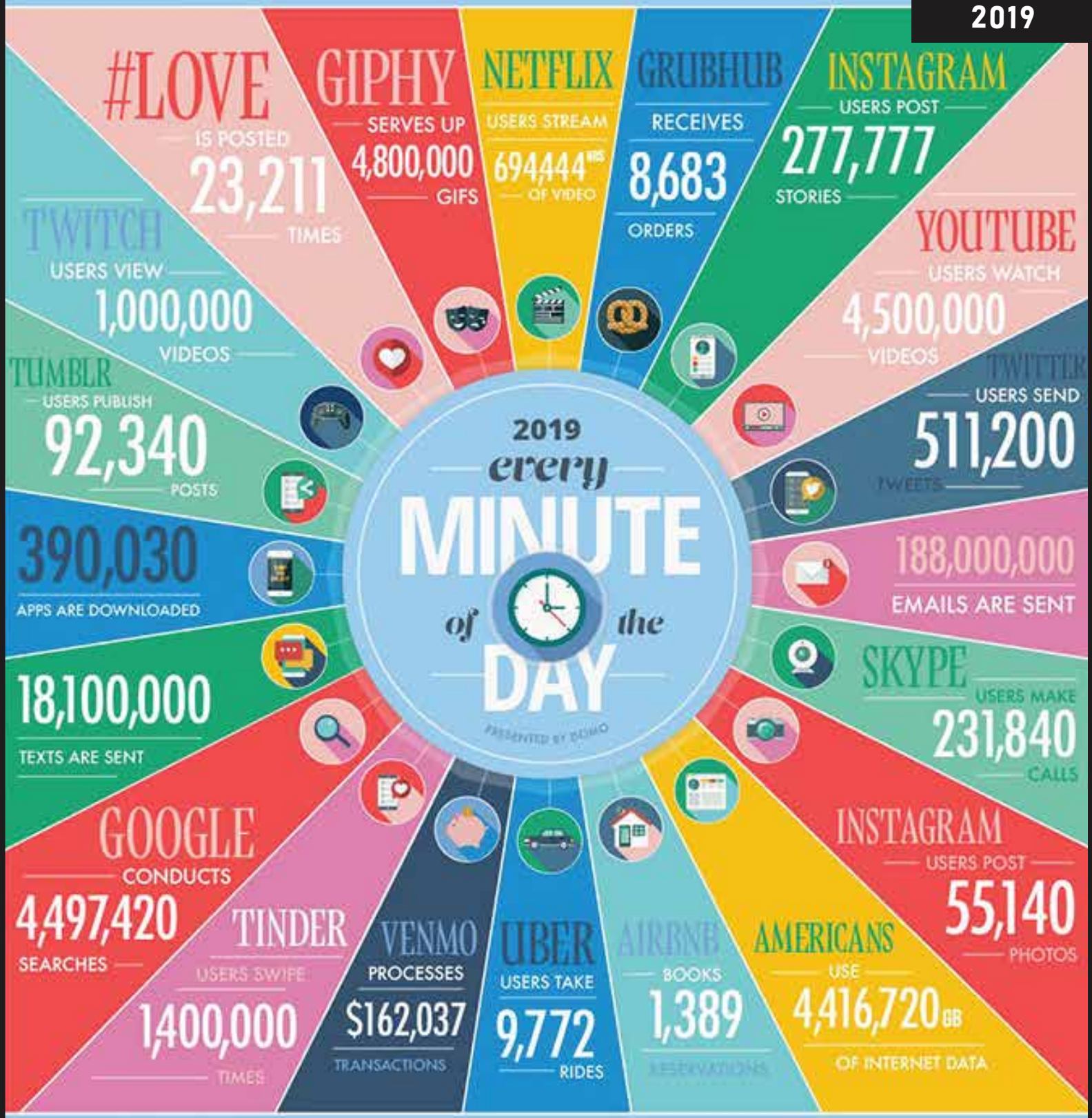
GLOBAL INTERNET POPULATION GROWTH 2012–2017
(IN BILLIONS)

The ability to make data-driven decisions is crucial to any business. With each click, swipe, share, and like, a world of valuable information is created. Domo puts the power to make those decisions right into the palm of your hand by connecting your data and your people at any moment, on any device, so they can make the kind of decisions that make an impact.

Learn more at domo.com

SOURCES: STATISTA, LINKEDIN, INTERNET LIVE STATS, EXPANDED RAMBLINGS, SLASH FILM, RIAA, BUSINESS OF APPS, INTERNATIONAL TELECOMMUNICATIONS UNION, INTERNATIONAL DATA CORPORATION

DOMO



The world's internet population is growing significantly year-over-year. As of January 2019, the internet reaches 56.1% of the world's population and now represents 4.39 billion people — a 9% increase from January 2018.

GLOBAL INTERNET POPULATION GROWTH 2012–2018
(IN BILLIONS)

The ability to make data-driven decisions is crucial to any business. With each click, swipe, share, and like, a world of valuable information is created. Domo puts the power to make those decisions right into the palm of your hand by connecting your data and your people at any moment, on any device, so they can make the kind of decisions that make an impact.

Learn more at domo.com

SOURCES: STATISTA, INTERNET LIVE STATS, EXPANDED RAMBLINGS, NATIONAL ASSOCIATION OF CITY TRANSPORTATION OFFICIALS, WIRED

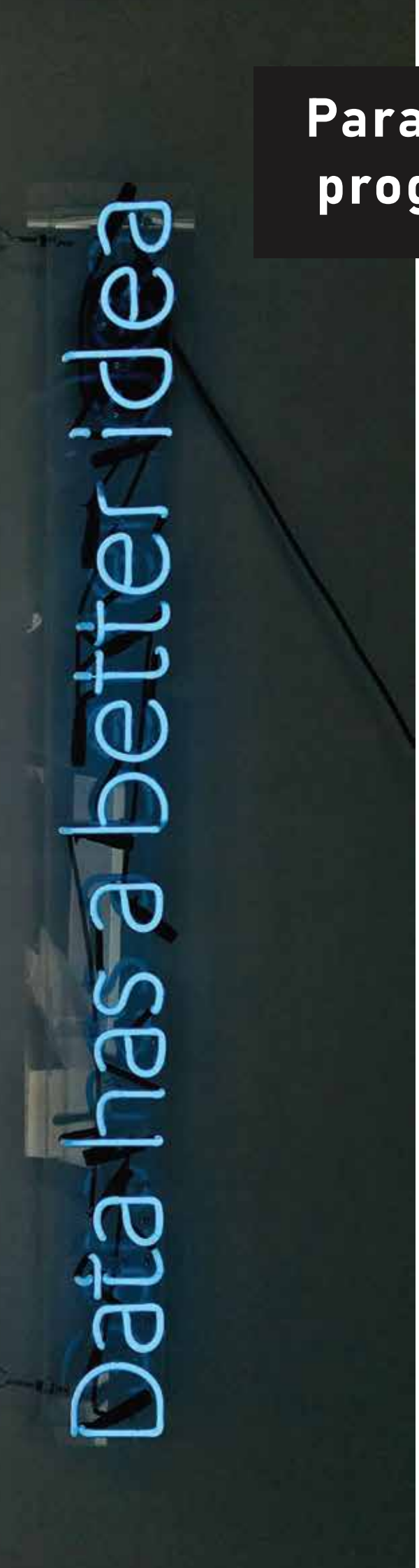
?

Sabia que

A evolução do tráfego global da Internet (em gigabytes por segundo) não dá sinais de desacelerar:

2002	100 Gbs
2007	2.000 Gbs
2017	46.000 Gbs
2022	150.700 Gbs

Nações Unidas



Para entender o ser humano, programa leu 700 mil textos

Darren Thackeray

Escritor. Texto publicado originalmente na Global Agenda do World Economic Forum (WEF). Reproduzido sob licença do autor.

Estudo analisou 700 mil textos anónimos escritos por 67 mil indivíduos. Correlação entre humores positivos e sono, alimentação saudável e exercício. Quase uma em cada cinco crianças e adolescentes tem uma desordem mental. IA pode ser usada para identificar a desordens da saúde mental nos media sociais.

A inteligência artificial (IA) pode dizer-nos mais sobre os benefícios da saúde mental ao olhar para nós.

Investigadores da Universidade de Waterloo (Canadá) recolheram mais de 700 mil entradas anónimas em jornais online escritas por mais de 67 mil utilizadores usando uma aplicação móvel de registo de humores. Eles desenvolveram depois um modelo informático de IA que podia identificar palavras-chave no texto.

O que nos faz sentir felizes?

O estudo, publicado em Janeiro passado, demonstrou uma forte correlação entre humores positivos e qualidade do sono, alimentação saudável e exercício físico. Em resumo, quanto mais olhamos para nós, mais felizes parecemos ser. Mesmo as actividades "produtivas" como um corte de cabelo estavam ligadas a sentir calma e felicidade.

Ligação entre saúde mental e física

Sabemos já há algum tempo que a saúde mental e física estão fortemente ligadas, mas há ainda muito trabalho a ser feito para nos ajudar a entender essa correlação.
Investigação como esta revela a ligação entre termos cuidado connosco – por exemplo, ao comer de forma saudável, dormir melhor e fazer exercício – e o nosso bem-estar psicológico. O coordenador do estudo, Lukasz Golab, elogia a tecnologia responsável pela investigação, afirmando que ela pode eventualmente ser usada como um tipo de "ferramenta de triagem"para sinalizar possíveis problemas de saúde mental entre utilizadores dos media sociais.
Segundo a Organização Mundial da Saúde (WHO), cerca de uma em cada cinco crianças e adolescentes têm uma desordem mental. A depressão é a mais prevalente, afectando um total de 254 milhões de pessoas em todo o mundo.

Felicidade e inteligência artificial

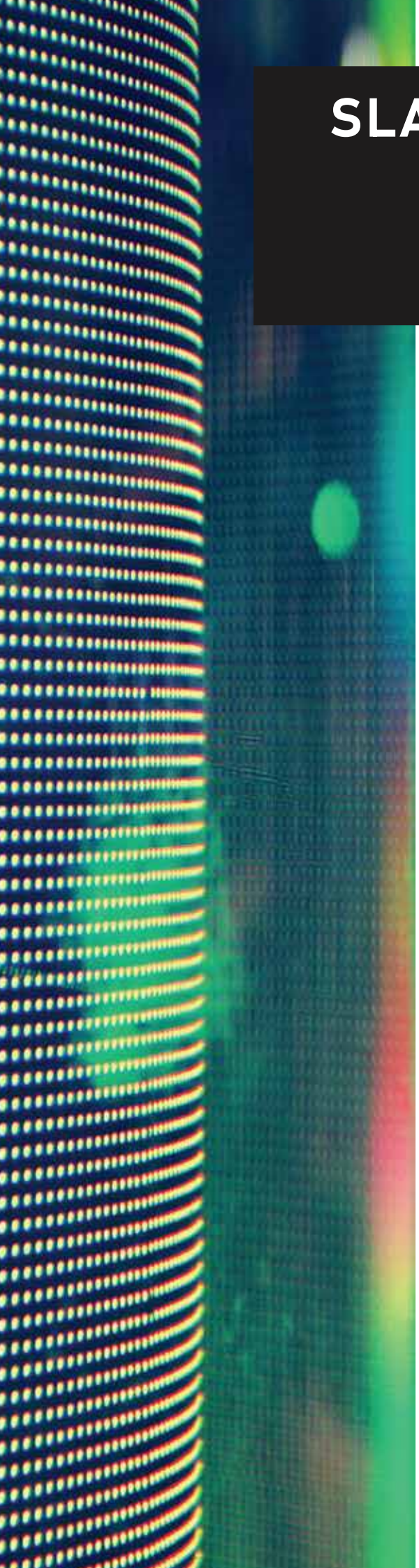
Este não é o primeiro uso da IA para tentar descobrir o segredo da felicidade. Um estudo em 2019 usou um modelo de IA para analisar 8 milhões de livros e 65 milhões de notícias de jornais, criando um "índice de felicidade nacional" que reporta até 1820. Entre as principais descobertas estava que vidas mais longas significam vidas mais felizes, um aumento do rendimento nacional leva a uma crescente felicidade nacional e que a guerra pode, de forma pouco surpreendente, reduzir drasticamente o estado de espírito nacional.

?

Sabia que

O número de foguetões lançados com sucesso desde 1957 foi de cerca de 5.560, que colocaram em órbita mais de 9.600 satélites. 5.500 continuam no espaço com cerca de 2.300 activos. Contam-se ainda 34 mil objectos com mais de 10 cm, considerados lixo espacial.

United Nations Office for Outer Space Affairs, Pixalytics



SLAPPS: Processo Judicial Estratégico contra a participação pública

European Centre for Press and Media Freedom & OBC Transeuropa

Artigo originalmente publicado no Resource Centre on Media Freedom in Europe, revisto por Charlie Holt, da Greenpeace International Legal Unit.

1. A definição

1.1. Como a pedra atirada à água

"Uma grande empresa processa um activista ambiental, que expôs um escândalo relacionado com poluição, na esperança de que o processo assuste outros activistas. Um empresário poderoso processa um jornalista por difamação, depois de o seu nome aparecer numa história impactante e verdadeira sobre corrupção. Um promotor imobiliário ameaça processar para silenciar a oposição comunitária a um novo projecto imobiliário. E assim por diante".

Isto é o que um SLAPP, um processo judicial estratégico contra a participação pública, é na prática.

De acordo com o grupo de acção dos activistas internacionais e advogados Protect the Protest, os indicadores de um SLAPP são que este tem como alvo as várias formas de liberdade de expressão, aproveita-se de um desequilíbrio de poder, ameaça levar à bancarrota o réu, tenta manter-se em tribunal o máximo tempo possível, faz geralmente parte de uma maior ofensiva de relações públicas destinadas a intimidar os críticos e segue um padrão de bullying em série, dado que o queixoso tem normalmente um historial de usar SLAPPs ou ameaçar com processos por forma a silenciar críticos.

Como afirmado em 1989, estas ações judiciais são meramente ferramentas jurídicas que visam "impedir os cidadãos de exercer os seus direitos políticos ou puni-los por o terem feito. Os SLAPPs passam uma mensagem clara: há um 'preço' pela expressão política". Originalmente o fenómeno dos SLAPPs era uma preocupação apenas para os activistas ambientais e comunitários. Agora, tem como alvo uma grande variedade de indivíduos e organizações que actuam pelo interesse público, tais como activistas da sociedade civil, líderes comunitários, jornalistas, informadores e cidadãos em geral.

Os SLAPPs tornaram-se uma séria ameaça à liberdade dos meios de comunicação e à participação democrática, o que requer uma reacção firme. "Como a pedra atirada à água" - escreveu Penolope Canan em "The SLAPP from a Sociological Perspective (1989)" – "um único SLAPP pode ter efeitos muito para além do seu impacto inicial". Estes efeitos na liberdade de expressão e qualidade de vida, na democracia e qualidade do jornalismo têm-se mantido basicamente inalterados ao longo dos anos. Este artigo irá abordá-los de diferentes perspectivas.

1.2. Intimidação e disparidade

Um dos elementos chave de um SLAPP é a disparidade de poder e recursos entre o queixoso e o réu. O queixoso tem noção do desequilíbrio de poder e, tirando partido de disposições legais elásticas e vagas, consegue converter assuntos de interesse público em litígios técnicos de direito privado, geralmente com pedidos de indemnização exorbitantes e alegações destinados a intimidar o réu e drená-lo dos seus recursos financeiros.

Um SLAPP não precisa de ser bem-sucedido em tribunal para ter o efeito desejado. Aliás, os queixosos sabem geralmente desde o início que as suas alegações são infundadas ou exageradas, mas mesmo que um juiz reconheça este facto e o rejeite, o caso pode continuar em tribunal durante anos, ser altamente dispendioso e causar danos reputacionais ao réu.

Tais acções judiciais transformam o

sistema judicial numa arma e têm um grave efeito dissuasor na liberdade de expressão e no direito à informação, uma vez que muitos optam por abdicar dos seus direitos se não estiverem aptos a suportar os custos do litígio.

1.3. Avisos preventivos e o preço do silêncio

Para colocar activistas e jornalistas sob pressão, os SLAPPs podem ser usados para chantagear explicitamente as vítimas e comprar o seu silêncio.

Os acusados enfrentam vários tipos de pressão. Por um lado, são intimidados pelos elevados custos de um litígio e tendem a autocensurar-se com o objetivo de evitar despesas. Por outro lado, em alguns casos, é-lhes mesmo pedido que abdiquem dos seus direitos de liberdade de expressão em troca da retirada do processo judicial.

Neste caso, não é necessário dar entrada da ação judicial: É suficiente que uma ação judicial seja "anunciada", como acontece por exemplo na Alemanha, onde os serviços jurídicos dos meios de comunicação social assistem a um aumento das tentativas de advogados de impedir que os jornalistas relatem. Isto foi descoberto no estudo recente "If you write that, I will sue you! Preventive strategies of lawyers against media", publicado pela fundação alemã Otto Brenner em cooperação com a [sociedade para os direitos civis] Gesellschaft fur Freiheitsrechte. De acordo com as suas conclusões, os serviços jurídicos dos meios de comunicação social recebem em média três avisos preventivos por mês.

1.4. Uma perda de dinheiro, tempo e credibilidade: como funciona

As tácticas de um SLAPP são bastante fáceis de detetar. Da perspetiva do queixoso, quanto mais tempo demorar, melhor. Como descrito no guia co-editado pela Greenpeace, a definição de um SLAPP pode começar por se descrever como ele funciona.

Nas palavras utilizadas pela equipa de peritos, advogados e activistas na publicação, "uma acção judicial pode arrastá-lo durante anos, mesmo que seja eventualmente retirada. Durante a litigância, os **bullies** do SLAPP exigem muitas vezes acesso aos seus emails, ficheiros do computador e outros detalhes da vida pessoal. Um SLAPP pode obrigá-lo a pagar milhares de dólares em taxas legais, ao mesmo tempo que se preocupa infindavelmente em ir à falência caso o outro lado ganhe. As pessoas que outrora apoiavam o seu trabalho podem começar a questionar a sua credibilidade. Pode desperdiçar anos a tentar defender-se da acção judicial em vez de trabalhar no que realmente lhe interessa. No fim de contas, como muitos outros, pode concordar em pôr fim à sua campanha".

Um silêncio no valor de 400 milhões de dólares

O preço do silêncio para os activistas que protestavam contra a construção da barragem Site C no Nordeste da Columbia Britânica atingiu mais de 400 milhões de dólares canadianos [cerca de 260 milhões de euros]. "Se assinar este compromisso de se manter calado no futuro, o nosso processo pode ser resolvido". Isto foi o que a BC Hydro, uma empresa da Coroa, propriedade do governo e do povo da Columbia Britânica, disse a Ken Boon, um agricultor que protestava contra a construção do Site C. Em 2016, Ken e mais cinco residentes em Peace Valley foram processados no valor de 420 milhões de dólares num processo judicial de 13 páginas que os acusava de "conspiração, intimidação, invasão, criar incómodo público e privado e

interferência intencional em relações económicas através de condutas ilegais. Eles ocuparam um terreno durante 63 dias para evitar a desflorestação de um local histórico. Então, foi-lhes pedido que "parassem de protestar" para sempre. O preço do seu silêncio foi estipulado em 420 milhões de dólares canadianos.

2. A abordagem das organizações internacionais

O problema dos SLAPPs varia de país para país, dependendo dos quadros jurídicos que podem facilitar este fenómeno como, por exemplo, o montante das custas legais, as leis que visam a liberdade de expressão na ausência de salvaguardas ou instrumentos de dissuasão.

No entanto, nos últimos tempos, as organizações internacionais têm vindo a prestar mais atenção a esta questão, o que pode ser importante para proporcionar soluções viáveis.

2.1. Nações Unidas: protecção para o povo

Em várias ocasiões, os mecanismos das Nações Unidas e procedimentos especiais destacaram a questão das obrigações dos Estados em facilitar o exercício dos direitos de liberdade de expressão, manifestação pacífica e associação.

Em particular, os Estados devem "assegurar um processo justo e proteger as pessoas de acções civis sem fundamento" e "devem introduzir meios de protecção aos organizadores e participantes de manifestações contra acções judiciais apresentadas levianamente ou com o propósito de dissuadir a participação pública". De acordo com os alertas da ONU, os Estados devem também promulgar legislação anti-SLAPP, permitindo o termo antecipado (com a atribuição de custos) de tais processos e o uso de medidas para sancionar abusos.

2.2. Conselho da Europa: descriminalização

A Plataforma online para promover a proteção do jornalismo e a segurança dos jornalistas gerida pelo Conselho da Europa (que "visa melhorar a protecção dos jornalistas e melhor responder à violência e ameaças feitas contra profissionais dos meios de comunicação social, encorajar mecanismos de alerta precoce e a capacidade para a resposta dentro do Conselho da Europa") enumera diferentes tipos de ameaças à liberdade dos meios de comunicação social e dos jornalistas, sem uma distinção restrita entre ameaças directas e indirectas. Os SLAPPs - mesmo nunca lá mencionados com este acrónimo mas ocorrendo por exemplo com processos judiciais ou ameaça de acções judicias por difamação - estão incluídos no grupo de actos com um efeito dissuasor na liberdade dos meios de comunicação social.

Por um lado, o Conselho da Europa, "consciente do potencial efeito dissuasor das leis de difamação superprotectoras na liberdade de expressão e debate público" promove "a descriminalização da difamação". De acordo com o Conselho da Europa, os jornalistas não devem ser nem detidos, nem ameaçados com uma sentença de prisão, quando acusados de violar o direito à reputação de outras pessoas e as suas violações não deveriam ser consideradas crimes, mas infracções civis.

Por outro lado, é possível obter um forte efeito dissuasor mesmo que a difamação seja descriminalizada. É por isto que o Conselho da Europa, além de promover a descriminalização "oferece orientações aos seus Estados membros de

forma a assegurar a proporcionalidade das leis de difamação e a sua aplicação no que diz respeito aos direitos humanos".

Os efeitos dissuasores enumerados pelo Conselho da Europa na sua série Freedom of the Press and the protection of one's reputation incluem "indemnizações injustamente elevadas durante o processo por difamação e falta de medidas de segurança eficazes e adequadas na legislação e na prática". As acções judiciais por difamação com uma indemnização muito elevada têm, de facto, um efeito dissuasor na liberdade de expressão, como afirmado pelo Tribunal Europeu dos Direitos do Homem.

2.3. Tribunal Europeu dos Direitos do Homem: um preço demasiado elevado

Existem vários acórdãos do Tribunal Europeu dos Direitos do Homem que respeitam ao conflito e equilíbrio entre a liberdade de expressão e a protecção da reputação de uma pessoa. Um, em particular, é mencionado na Plataforma do Conselho da Europa como pioneiro. De acordo com os observadores internacionais, é um dos SLAPPs mais conhecidos da história europeia.

Em Junho de 2017, o Tribunal teve de decidir sobre um caso de indemnização numa acção judicial por difamação, em que o editor do jornal diário irlandês The Herald tinha sido condenado a pagar mais de um milhão de euros. O jornal tinha publicado uma série de artigos sobre um consultor de relações públicas, em que relatava os rumores da sua relação íntima com um ministro do governo. Processado por difamação, o jornal foi condenado a pagar 1.250,000 euros. O editor alegou que a indemnização era excessiva e violava o seu direito à liberdade de expressão.

O Tribunal Europeu afirmou que "não é necessário decidir se os danos impugnados tiveram de facto um efeito dissuasor na imprensa. Por uma questão de princípio, indemnizações imprevisivelmente elevadas em casos de difamação são capazes de produzir tal efeito e requerem, portanto, uma análise mais aprofundada (...) e uma justificação muito forte". Além disso, "medidas de salvaguarda eficazes" dever-se-iam aplicar ao processo de litígio, bem como ao seu resultado.

2.4. OSCE: liberdade de expressão

A missão do Representante da OSCE para a Liberdade dos Media consiste em proteger e promover a liberdade de imprensa em todos os Estados da OSCE [Organização para a Segurança e Cooperação na Europa], acompanhar a evolução dos meios de comunicação social e as violações da liberdade de expressão e da liberdade de imprensa. As actividades neste campo visam garantir a segurança dos jornalistas e promover a descriminalização da difamação, uma vez que "os jornalistas não devem ser acusados criminalmente pelo seu trabalho".

A OSCE não aborda diretamente o SLAPP, mas em 2019, com a assinatura da "Twentieth Anniversary Joint Declaration: Challenges To Freedom Of Expression In The Next Decade" [Declaração Conjunta do 20º Aniversário: Desafios à Liberdade de Expressão na Próxima Década], declarou que os Estados deveriam promover a liberdade de expressão e a segurança dos jornalistas, proporcionando regras jurídicas e quadros políticos adequados e "limitando as restrições à liberdade de expressão em matéria penal, com o propósito de não dissuadir o debate público sobre assuntos de interesse público".

?

Sabia que

O jornal The New York Times conseguiu lucros de mais de 800 milhões de dólares no digital em 2019 e, dos 5,2 milhões de assinantes, 4,4 milhões estão no digital. O Wall Street Journal chegou pela primeira vez aos dois milhões de assinantes digitais e, do total de 1,6 milhões de assinantes, a revista The Economist tem 790 mil exclusivamente digitais.

NiemanLab, Audit Bureau of Circulations

2.5. União Europeia: harmonização, missão impossível

As instituições europeias também manifestaram a sua preocupação relativamente a esta questão. A liberdade dos media é um direito fundamental salvaguardado a nível europeu através da Convenção Europeia dos Direitos do Homem e pela Carta Europeia dos Direitos Fundamentais, enquanto pilar da democracia moderna e componente essencial do debate aberto e livre.

O Parlamento Europeu salientou, através de várias resoluções, a importância, entre outras coisas, de "elaborar uma directiva da UE anti-SLAPP, com o objectivo de proteger os meios de comunicação independentes de ações judiciais vexatórias destinadas a silenciá-los ou a intimidá-los" e "incentiva a Comissão e os Estados-Membros a apresentarem propostas legislativas ou não legislativas para a proteção dos jornalistas na UE que são regularmente objecto de acções judiciais, destinadas a censurar o seu trabalho ou a intimidá-los, incluindo regras anti-SLAPP pan-Europeias".

Em 2018, numa iniciativa interpartidária, vários deputados enviaram uma carta à Comissão Europeia solicitando uma resposta europeia relativamente ao problema SLAPP. No entanto, o debate ainda está em curso.

No âmbito da sua acção em defesa dos jornalistas e da liberdade de imprensa, a Comissão Europeia financia actualmente vários projectos europeus. Entre eles contam-se alguns geridos pelo European Centre for Press and Media Freedom e pelos seus parceiros, que por sua vez prestam assistência prática e jurídica a jornalistas ameaçados, mantendo também uma plataforma de mapeamento (mapping platform) que reporta as ameaças à liberdade de imprensa e fornece treino organizado em autodefesa digital para jornalistas.

3. Difamação, calúnia e os media

3.1. Uma definição, muitos enquadramentos

Embora os SLAPPs possam ser usados para causar diferentes tipos de danos (à propriedade, rendimentos, negócios, saúde...), tendo por base diferentes tipos de infrações (invasão de propriedade, privacidade, honra...), os processos judiciais mais escandalosos em todo o mundo dizem respeito a danos à reputação, afectando assim a actividade dos jornalistas e o direito à liberdade de expressão. É por isso que as leis de difamação são o terreno mais comum onde um SLAPP pode prosperar. Como confirmado por um estudo do Conselho da Europa, há algumas diferenças de país para país e uma distinção geral entre difamação oral, difamação escrita, afirmação incorrecta de factos e palavras falsas que não podem ser proferidas. Cada quadro legislativo tem as suas próprias diferenças e termos. Enquanto a calúnia é escrita, a difamação é falada. Porém, estas distinções não podem ser transferidas para a legislação, uma vez que cada sistema tem de se adaptar rapidamente às mudanças das tecnologias de informação. Outras palavras usadas geralmente, quando se refere um quadro internacional, são difamação, insulto, abuso, afrontas à honra e à dignidade, e calúnia. Todos estes termos têm um significado legislativo próprio, quando referidos num quadro nacional específico.

3.2. O abuso de uma ferramenta legal

Como referido num estudo comparativo pedido pelo Representante da OSCE para a Liberdade dos Media, "as leis de difamação

continuam a ser aplicadas com algum grau de regularidade na região da OSCE, incluindo contra os meios de comunicação social. Continuam a existir zonas particularmente problemáticas no Sul da Europa (especialmente na Grécia, Itália, Portugal e Turquia), na Europa Central (especialmente na Hungria), na Ásia Central e no Azerbaijão, embora continuem a haver condenações ocasionais de jornalistas em estados considerados fortes defensores da liberdade de imprensa, como a Dinamarca, Alemanha e Suíça".

Esta aplicação das leis de difamação, seja em direito criminal ou civil, tem relativamente pouco a ver com uma possível relação causa-efeito entre difamação e SLAPPs: embora algumas leis de difamação sejam mais facilmente abusadas do que outras, a difamação é realmente apenas um pretexto, uma desculpa, um falso terreno usado e abusado com o único objectivo de silenciar críticas e parar investigações jornalísticas.
De facto, a verdadeira questão neste contexto, em que a legislação e a prática concordam em equilibrar a liberdade de expressão e o direito à defesa da reputação, não é a lei em si, mas sim o abuso da lei, sendo que os SLAPPs são, na verdade, abusos da lei.

3.3. Princípios e boas práticas

Considerando que um número significativo de acções judiciais estratégicas para silenciar o criticismo são apresentadas tendo por base leis de difamação, a atenção das organizações internacionais focou-se durante anos na difamação e na sua regulamentação. Nas últimas duas décadas, a Article 19 desenvolveu uma carta de princípios comuns como base de debate e análise: o objectivo é "estabelecer um equilíbrio adequado entre o direito humano à liberdade de expressão e a necessidade de proteger as reputações individuais". Os Princípios, publicados pela primeira vez em 2010 e revistos em 2017, baseiam-se no direito e normas internacionais, e incluem somente a relação entre a liberdade dos meios de comunicação e a proteção da reputação, excluindo áreas como a privacidade, a auto-estima ou o discurso de ódio.

3.3.1. A situação na Escandinávia

Em Dezembro de 2019, o Observatório Balcani Caucaso Transeuropa (OBCT) participou numa missão exploratória, liderada pelo ECPMF com o objectivo de encontrar e analisar as melhores práticas na liberdade de imprensa.

Tendo em conta a ausência de qualquer sinal ou ameaça de SLAPPs tanto na Dinamarca como na Suécia, a situação foi de alguma forma difícil de explicar. De facto, ambos os países têm alguns elementos em comum com países onde os SLAPPs são comuns como, por exemplo, a difamação ser um crime e o facto de as formas mais graves de difamação serem punidas com prisão. Não obstante, os SLAPP não são simplesmente um problema, nem na Dinamarca nem na Suécia.
Quando lhes foi pedido para explicar o facto de não haver este tipo de abusos, os jornalistas e os advogados entrevistados pela delegação abordaram dois elementos que podem ser considerados como dissuasores ao recurso de acções judiciais para intimidar repórteres e activistas. Estas características, embora possam ser consideradas boas práticas, parecem ser bastante difíceis de "exportar":

- em ambos os países, a tradição democrática continua a unir as pessoas:

apesar de algumas tendências para a polarização, a liberdade de expressão e a liberdade de imprensa são consideradas um alicerce do sistema constitucional e um pilar da coesão social. Por um lado, na maioria dos casos, a jurisprudência pronuncia-se a favor do jornalista e os juízes tendem também, na maioria das vezes, a rejeitar acções judiciais contra jornalistas. Por outro lado, é também uma questão de reputação - ninguém processaria um jornalista, visto ser motivo de vergonha;

- uma característica do direito civil, onde geralmente os SLAPPs prosperaram por todo o mundo, é que as compensações são muito baixas: além de ser inconveniente sob um ponto de vista ético, processar é muito caro em comparação com o que se poderia obter como dano. Sendo as compensações (se concedidas) tão baixas, a ameaça potencial de um efeito dissuasor é completamente vazia.

Croácia
Hrvoje Zovko, presidente da Associação Croata de Jornalistas (HND), relatou em Janeiro de 2019 haver "mais de 1,000 julgamentos a decorrer contra jornalistas croatas ou meios de comunicação social". Zovko está também a ser processado por calúnia pelo seu antigo empregador, a televisão pública HRT, que o despediu em Setembro de 2018. "Na Croácia, está aberta a época de caça aos jornalistas", disse ao OBCT relativamente ao aumento de ataques a jornalistas. Além dele, a televisão pública croata processou por difamação 36 meios de comunicação e jornalistas, incluindo os seus próprios trabalhadores nos últimos dois anos.

Sérvia
As acções judiciais contra jornalistas "estão a tornar-se prática comum na Sérvia, por muito que os factos usados nas suas investigações sejam verificados. E muitas vezes altos funcionários, como ministros, processam os media": como Stevan Dojčinović, director do portal de investigação KRIK, disse a Francesco Martino, correspondente do OBCT, um meio de comunicação pode ser "processado quatro vezes diferentes pela mesma notícia" e o tribunal pode negar o pedido para fundir os quatro processos. "Assim, estamos actualmente a gastar uma quantidade enorme de tempo, dinheiro e energia para nos defendermos".

Números
Os números não chegam para contar uma história. Por exemplo, este é o caso da luta de Antonella Napoli para se livrar de uma acção judicial movida contra ela há mais de 20 anos. Um único SLAPP pode capturar toda uma vida. Os números podem ser muito impressionantes, como para Federica Angeli, jornalista que tem vivido os últimos seis anos sob protecção e está a lutar contra dezenas de processos por difamação. Em Dezembro de 2019, celebrou a sua 111ª vitória em tribunal contra um processo de difamação.

4. A procura por soluções

Por falar em soluções, George Pring já estava ciente em 1989 que tinha de ser encontrada uma onde estava o problema, ou seja, em tribunal. "As melhores destas soluções encontram-se com os nossos tribunais, a instituição concebida para proteger as liberdades individuais e direitos políticos, mas que, no entanto, ironicamente, é a instituição a ser manipulada para produzir o 'efeito dissuasor' dos SLAPPs".

4.1. Legislação anti-SLAPP nos EUA e no Canadá

De acordo com um guia escrito por Austin Vining e Sarah Matthews para o Reporters Committee for Freedom of the Press, "a legislação anti-SLAPP dá aos réus uma maneira de rapidamente rejeitarem acções

judiciais sem fundamento movidas contra eles por terem exercido os seus direitos da Primeira Emenda. Estas leis visam desencorajar a apresentação de processos SLAPP e impedir a imposição de custos significativos com a litigância e dissuadir a liberdade de expressão".

Vários estados nos EUA adotaram ou alteraram as suas leis anti-SLAPP. Em Outubro de 2019, 30 estados juntamente com o Distrito de Columbia tinham leis anti-SLAPP. No Canadá há uma lei anti-SLAPP na Colúmbia Britânica, Ontário e Quebeque.

As protecções anti-SLAPP variam significativamente de estado para estado. Na sua maioria, as leis anti-SLAPP são suficientemente amplas para cobrir processos SLAPP destinados a silenciar ou retaliar contra jornalistas ou meios de comunicação críticos. De acordo com o West Coast Environmental Law, um grupo sem fins lucrativos canadiano composto por advogados e estrategas ambientais, dedicados a salvaguardar o meio ambiente através da lei, a legislação anti-SLAPP da Colúmbia Britânica no Canadá irá implementar um processo mais rápido para os réus pedirem ao tribunal que rejeite uma acção judicial, e eles podem fazê-lo se o processo interferir com a sua liberdade de expressão. Tal como outros estatutos anti-SLAPP, a lei vai permitir igualmente ao tribunal que atribua ao queixoso custos punitivos adicionais.

4.2. A olhar para as soluções europeias

Os Estados-Membros da UE são livres de introduzir leis importantes sobre a difamação e de implementar diferentes normas de protecção da liberdade de expressão. No entanto, a falta de harmonização a nível europeu permite a proliferação de abusos através da aplicação do direito internacional privado (DIP), um conjunto jurídico que trata de disputas entre particulares que vivem em jurisdições diferentes. Em particular, estão em causa o Regulamento Bruxelas I (que rege a escolha da jurisdição em matéria civil e comercial) e o Regulamento Roma II (que rege a lei aplicável às obrigações não-contratuais).

Um caso emblemático foi o que envolveu Daphne Caruana Galizia e o Pilatus Bank que, apesar de ligações irrefutáveis a Malta, intentou uma ação judicial por difamação no Reino Unido e nos Estados Unidos. Tal foi possível, uma vez que o Regulamento Bruxelas I permite ao queixoso, em processos de difamação, escolher entre o foro do domicílio do réu e o local onde alegadamente foram sofridos danos. Além disso, como a difamação está explicitamente excluída do alcance de aplicação do Regulamento Roma II, a lei aplicável será a do país em que ocorre o dano (Art. 4). Na prática, estas regras especiais em casos de difamação permitem ao queixoso escolher o fórum e a lei do país onde os padrões de liberdade de imprensa são inferiores, implicando uma possível violação do direito do réu a um julgamento justo.

A suscetibilidade de casos de difamação de forum shopping é suficientemente grande para limitar a liberdade de imprensa, o que implica que defender um processo numa jurisdição estrangeira leva a custos mais elevados e a um maior sofrimento psicológico causado pela falta de familiaridade com o direito estrangeiro.

Em Fevereiro de 2018, seis membros do Parlamento Europeu escreveram uma carta à Comissão Europeia para lançar rapidamente legislação relacionada com a protecção do jornalismo de investigação na Europa. Os deputados de vários partidos

afirmaram que os SLAPPs exigem uma resposta da UE e pediram à Comissão para tomar medidas. Em Junho de 2018, o Vice-Presidente Timmermans respondeu aos eurodeputados argumentando que a EU não tem competência para harmonizar a legislação substantiva em matéria de difamação.

No entanto, um estudo de Justin Borg-Barthet afirma que a UE tem competência para intervir nesta questão, uma vez que a base jurídica da directiva relativa à protecção dos autores de denúncias pode também aplicar-se a uma directiva anti-SLAPP. De facto, "se é possível argumentar que a protecção contra os autores de denúncias tem um efeito directo sobre o funcionamento do mercado interno, como a Comissão faz na sua dependência do Art. 114 do TFUE [Tratado sobre o Funcionamento da União Europeia], deve seguir-se que isto também é assim para a difamação". (O parecer jurídico de Borg-Barthet foi apresentado na palestra sobre soluções anti-SLAPP organizada pelo ECPMF e outros parceiros a 12 de Novembro de 2019).
Além disso, o estudo sugere a alteração da legislação existente e a introdução de novos instrumentos. Em especial, as regras sobre a jurisdição do Regulamento Bruxelas I deverão ser alteradas e seguir os tribunais do domicílio do réu, devendo o Regulamento Roma II ser alterado com o objectivo de harmonizar as regras relativas à escolha da lei em matéria de difamação, tornando assim a lei aplicável mais previsível e limitar o forum shopping.

Porém, devem ser realizados mais estudos sobre a legislação processual e substantiva nacionais em casos de difamação, tendo em vista a adopção de uma directiva que harmonize as medidas de segurança mínimas em matéria de liberdade de expressão. Por conseguinte, a nível da UE, o debate continua em curso e centra-se num conjunto de soluções a curto e longo prazo. Posto isto, uma vez que ainda não foi alcançado um acordo entre os Estados-Membros sobre uma proposta legislativa, existem, no entanto, outras medidas que podem ser adoptadas para contrastar o fenómeno SLAPPs.

5. Itália: acções judiciais como armas

O termo SLAPP ainda não foi adoptado em Itália, onde as ações judiciais estratégicas são chamadas de "querele pretestuose, cause bavaglio, liti temerarie", salientando a importância da sua natureza ilusória, amordaçadora, imprudente e sem fundamento. Apesar disso, o problema é uma emergência diária para os jornalistas.

O ambiente dos meios de comunicação italiano está gradualmente a deteriorar-se devido a uma série de assuntos que estão firmemente interligados. A crise económica, a legislação e os desenvolvimentos políticos têm gerado um clima hostil para com a imprensa.
Os "Reporters Sans Frontières" colocaram a Itália na 43ª posição em 2019, quando o nível de violência e de ameaças contra jornalistas é alarmante e continua a aumentar. Cerca de 20 jornalistas italianos estão sob protecção da polícia devido a várias ameaças ou tentativas de homicídio por parte da máfia ou de grupos extremistas. A Itália também registou o crescimento mais acentuado no número de alertas de liberdade de imprensa em 2018, de acordo com um relatório feito pela **"Platform for the protection of journalism and the safety of journalists"** gerida pelo Conselho da Europa.

Entre todos os problemas dos jornalistas relacionados com o seu trabalho, a Entidade Reguladora no domínio da Comunicação Social italiana identificou

que o abuso das acções judiciais é a ferramenta principal usada para sabotar a liberdade de imprensa. O chamado "querele temerarie", processos de difamação frívolos e sem fundamentos, é reconhecido como uma "emergência democrática" pelas organizações dos jornalistas. Como afirmado por Carlo Verna, Presidente da Câmara Italiana de Jornalistas, são uma restrição objectiva ao direito de informar e ser informado.

5.1. O enquadramento legislativo

Uma vez que a protecção da reputação dos indivíduos pode colidir com a liberdade de expressão, é necessário equilibrar constantemente os casos em lados opostos. Os critérios para o efeito são definidos num acórdão histórico da Corte di Cassazione (Tribunal de Cassação, em 1984). Em especial, estabelece-se que o exercício do direito à informação verdadeira está protegido se houver:

- uma utilidade social ou relevância social da informação;

- uma veracidade da informação (que pode ser presumida se o jornalista tiver verificado seriamente as suas fontes);

- uma restrição ("continenza"), referindo-se à forma civilizada da expressão, que não pode "violar a dignidade mínima a que qualquer ser humano tem direito".

A difamação é ainda uma infracção penal punível pelo Código Penal e pela Lei da Imprensa. Os jornalistas podem enfrentar até seis anos e uma multa (até 50 mil euros), embora o Tribunal Europeu dos Direitos Humanos tenha repetidamente avisado Itália do potencial efeito dissuasor causado pela mera existência de sentenças de prisão por difamação, que constitui uma interferência desproporcionada com o direito de liberdade de expressão (ex.: Belpietro v. Itália e Ricci v. Itália). Para mais, de acordo com a Lei da Imprensa, em caso de difamação, os directores/ directores-adjuntos e o editor ou impressor (para a imprensa não-periódica) podem ser responsabilizados em termos civis e criminais pela falta de supervisão do conteúdo da publicação. Em resumo, uma acção judicial vexatória é uma acção perfeitamente legal que pode ser realizada tanto em tribunais civis, quanto criminais: pode ser apresentada como processo criminal por difamação ou como acção civil para indemnização por danos.

5.1.1. Afirmações civis vs. acções judiciais criminais

O Código de Processo Civil italiano introduz várias vantagens processuais que tornam os processos civis ainda mais ameaçadores do que os criminais. De facto, em processo civil:

- não há escrutínio preliminar pela autoridade judicial (isto significa procedimentos mais longos e mais caros, enquanto os procedimentos criminais são, a maior parte das vezes, derimidos mesmo antes do julgamento);

- não há limite para a compensação de danos (enquanto no procedimento criminal ronda os 50 mil euros, mas, neste caso, foi considerado excessivo e desproporcional);

- há um período muito mais longo de limitação para apresentar uma acção (cinco anos, opondo-se aos 90 dias no procedimento criminal). Contudo, deve ser considerado que o crime prescreve ao fim de seis anos. De acordo com o Art. 2947 par. 3 do Código Civil, o mesmo período de prescrição aplica-se à acção civil.

O legislador está a trabalhar no Código de Processo Civil para introduzir instrumentos legais mais efectivos, pois os existentes - como os danos punitivos e a mediação obrigatória - não são suficientes.

5.1.2. Uma abordagem difícil com números

Apesar de os SLAPPs terem sido definidos como uma "emergência democrática", é difícil quantificar o fenómeno. O principal motivo recai no facto de que os dados das acções civis e criminais são registados de maneira diferente. Para o sistema criminal, a base de dados do Instituto Nacional de Estatística da Itália (ISTAT) regista acções com base no crime. Por outro lado, na esfera civil, os processos são registados de acordo com a acção civil: portanto, seria necessária uma análise aprofundada a cada processo civil para a compensação de danos, pois é impossível entender quais estão directa ou indirectamente ligados à difamação e ao jornalismo. Além disso, as estatísticas não consideram um número extensivo de resoluções extrajudiciais de litígios e actos de autocensura. Porém, vale a pena mencionar que cerca de 70% dos casos criminais são resolvidos mesmo antes de irem a julgamento devido ao escrutínio preliminar pela autoridade judicial (juiz para a investigação preliminar ou GIP, de Giudice per le Indagini Preliminari). Tendo em consideração a extensa solução extrajudicial de controvérsias, o efeito dissuasor que causam os casos de autocensura e a falta de disposições que possam efectivamente desencorajar os autores a iniciar os SLAPPs, é fácil supor que este seja um problema ainda mais amplo e mais sério.

year	criminal lawsuits filed according to the Press Law (with accusation of fact)	stopped by the Judge for the preliminary investigation	going to trial
2011	4524	3057 (67,6%)	710 (16%)
2017	9479	6350 (67%)	625 (6,6%)

De acordo com Instituto de Estatísticas Nacional de Itália (ISTAT), em 2017 houve 9.479 queixas de difamação criminal "definidas" pelo Juiz para a Investigação Preliminar (GIP): 67% foram arquivadas. Comparando com o ano de 2011, as queixas de difamação duplicaram.

Olhando para o cenário internacional, a difamação é um crime na maioria dos países, como, por exemplo, em 75% dos Estados da OSCE. No entanto, muitas organizações internacionais de liberdade de imprensa e direitos humanos defendem "a descriminalização total da difamação e a consideração justa de tais casos em órgãos de resolução de disputas ou tribunais civis".

Mas a descriminalização da difamação e a abolição de penas de detenção por difamação são dois pedidos diferentes, mesmo que sejam frequentemente confundidos. De facto, se a difamação for descriminalizada, o sistema italiano já não irá fornecer a garantia de um filtro de um juiz e todas as afirmações de danos vão durar anos, tal como acontece actualmente. Até agora, as alterações legislativas propostas em Itália não incluem a descriminalização.

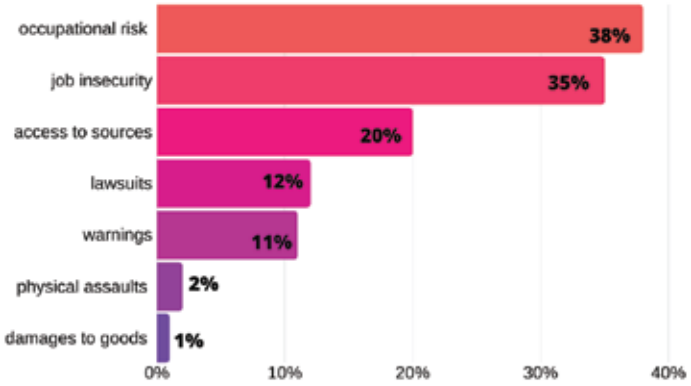
Outra coisa é pedir a abolição da prisão como castigo. Neste caso, a difamação continuaria a ser um crime (e o sistema garantia um juiz imparcial), mas seria punida com uma sanção financeira em vez de encarceramento.

Outra característica quanto a Itália, provavelmente um paradoxo de acordo com padrões internacionais, é o abuso recorrente do discurso de ódio e difamação feita através de meios de comunicação capturados por partidos políticos e/ou políticos. Muitas vezes, os media são usados naquilo que se denomina de atiradores de lama para deslegitimar os adversários políticos. É por isso que, embora cientes da importância do equilíbrio entre a liberdade de expressão e a protecção da reputação, muitos observadores - como Alessandro Galimberti, presidente da Câmara Regional de Jornalistas de Milão, ou Antonella

Napoli, do Articolo 21 - sentem a necessidade de manter a difamação como crime, como freio e impedimento ao abuso da liberdade de insulto, que muitas vezes leva ao incitamento ao ódio.

5.2. Factores que promovem o efeito dissuasor

Um alto nível de insegurança no trabalho exclui a capacidade financeira de reagir a estes processos e acções judiciais. Geralmente, os jornalistas são precários ou freelancers e, na maioria das vezes, quando são alvos de um SLAPP, são deixados sozinhos e não podem contar com o apoio do editor, especialmente a nível local.



Perceção dos jornalistas às ameaças (AGCOM - Osservatorio sul giornalismo, 2017)

Além disso, uma simples ameaça de longos e custosos procedimentos legais tem um efeito forte assustador na liberdade de imprensa, levando a uma autocensura e desencorajando os jornalistas a fazerem o seu trabalho.

Em Itália, o efeito dissuasor destes processos judiciais é crescente pela duração excessiva dos julgamentos (cerca de seis anos por uma sentença de primeira instância), criticados e condenados várias vezes pelo Tribunal Europeu de Direitos Humanos. Outro elemento que contribui para um efeito dissuasor é que é extremamente fácil de apresentar um processo e, visto não haver limites à compensação por danos, as multas podem ser excessivamente desproporcionais.

5.3. O Estado da arte no parlamento italiano

No final de 2019, no Parlamento italiano, estavam quatro propostas de lei com medidas para impedir acções judiciais estratégicas e alterar as leis dos meios de comunicação (relativas à responsabilidade do editor, o direito a ter uma correção imediata das notícias, a criação de uma nova autoridade de juízes, indemnizações, multas em vez de prisão pelo crime de difamação). As propostas legislativas diferem em muitos aspectos mas têm uma coisa em comum, nomeadamente o cancelamento da prisão como castigo pela difamação.

No que diz respeito às provisões anti-SLAPP, todas as propostas de lei introduzem um tipo de "responsabilidade civil agravada" com correspondentes danos punitivos por pedidos de indemnização sem fundamento: se o juiz decidir que o pedido foi apresentado de má-fé, o queixoso pode ser condenado a pagar uma compensação. Os projectos de lei diferem na quantia a ser paga pelo queixoso. O projecto de lei do Partido Democrático propõe algo como uma multa, e não como compensação, para o acusado. (Ver a nossa análise legal para mais detalhes).

Um dos projectos de lei foi priorizado por ter um elemento inovador para o sistema italiano e que é o parâmetro fixo para o juiz decidir o valor da compensação. Quanto mais elevado for o pedido de reivindicação, mais alta será a multa. Este princípio de proporcionalidade é visto como o principal entrave para os processos judiciais estratégicos, visto serem perigosos no que diz respeito à liberdade de expressão, não

apenas pela sua falta de fundamento, mas também pela desproporção nos pedidos de indemnização. Sem fundamento e com muito dinheiro é a pior combinação para um grande "efeito dissuasor" nos jornalistas. Questões críticas levantadas por alguns analistas e confirmadas por alguns membros do governo italiano incluem as penas demasiado severas, a possível violação da igualdade, o risco de mudar as regras e a necessidade de encontrar novas formas, extrajudiciais. A 17 de Dezembro de 2019 foi aprovada uma versão alterada do projeto de lei de Di Nicola na Comissão de Justiça: a indemnização punitiva foi reduzida para 25% do alegado dano (em vez de metade). Isto parece aumentar a hipótese de sucesso de uma possível solução anti-SLAPP em Itália.

5.4. Autodefesa e contra-ataque

Considerando que os processos estratégicos são vistos pelos jornalistas como "uma emergência democrática" e que as tentativas legislativas para impedi-los foram infrutíferas na sua aplicação ou abortadas no Parlamento, os jornalistas desenvolveram várias "soluções de emergência" para se defenderem:

- como explicado por Antonella Napoli, uma jornalista sob proteção policial, a melhor forma de ajudar colegas sob ameaça ou processados por um SLAPP é dar-lhes um "guarda-costas dos media" -para que não se sintam sozinhos, os colegas devem republicar as suas investigações e seguir o que já foi encontrado;

- como decidido em Maio de 2019 pelo Conselho Nacional da Câmara de Jornalistas, de Itália, há o compromisso em implementar qualquer ferramenta para apoiar os jornalistas sujeitos a SLAPPs;

- em 2011, a "Associazione Stampa Romana" abriu o centro de ajuda "Roberto Morrione querele temerarie", no qual os advogados ajudam pro bono os jornalistas processados. Desde 2015, a "Ossigeno per l'Informazione" oferece assistência legal pro bono a jornalistas e bloggers que estão a enfrentar acusações legais ou processos.

?

Sabia que

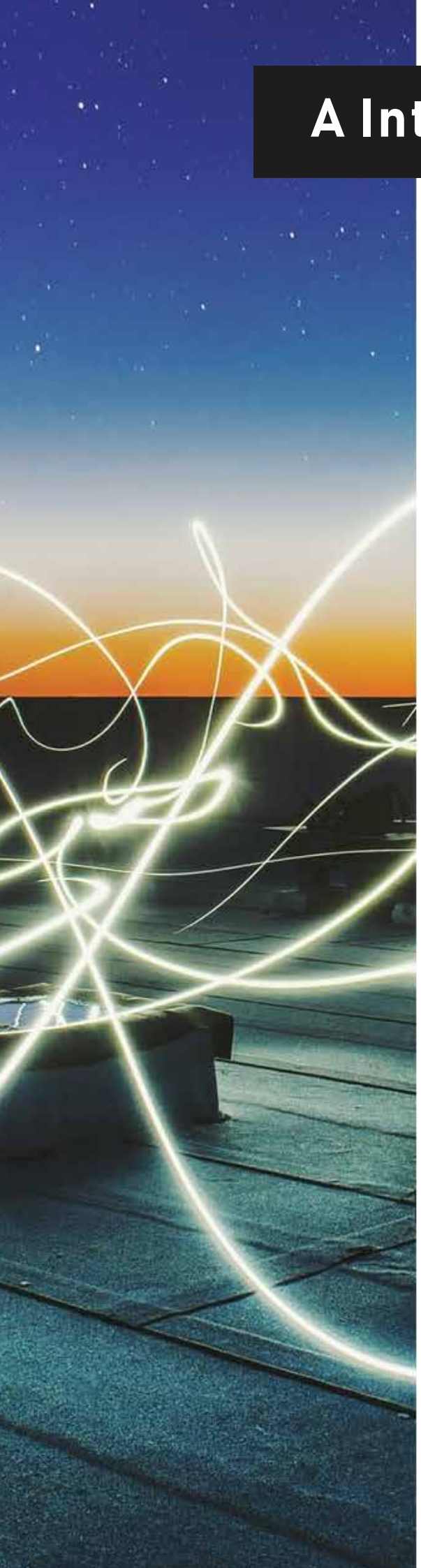
O tráfego na Web pode ser definido em três eras:

- a primeira, The SEO Age (2000 – 2010), foi dominada pelo tráfego através da “homepage” ou dos “bookmarks”, pelas hiperligações e optimização dos motores de busca (SEO);

- seguiu-se a The Social Age (2011 – 2017) com as plataformas sociais;

- a terceira, The Algorithms-Plus Age (2017 – ?), junta a estas vários elementos algorítmicos, a curadoria humana e a personalização.

Montague Street Media



A Internet desde 1858 a 2020

1858 *FTL Design*

1903 *Telegraph Construction & Maintenance Co Ltd*

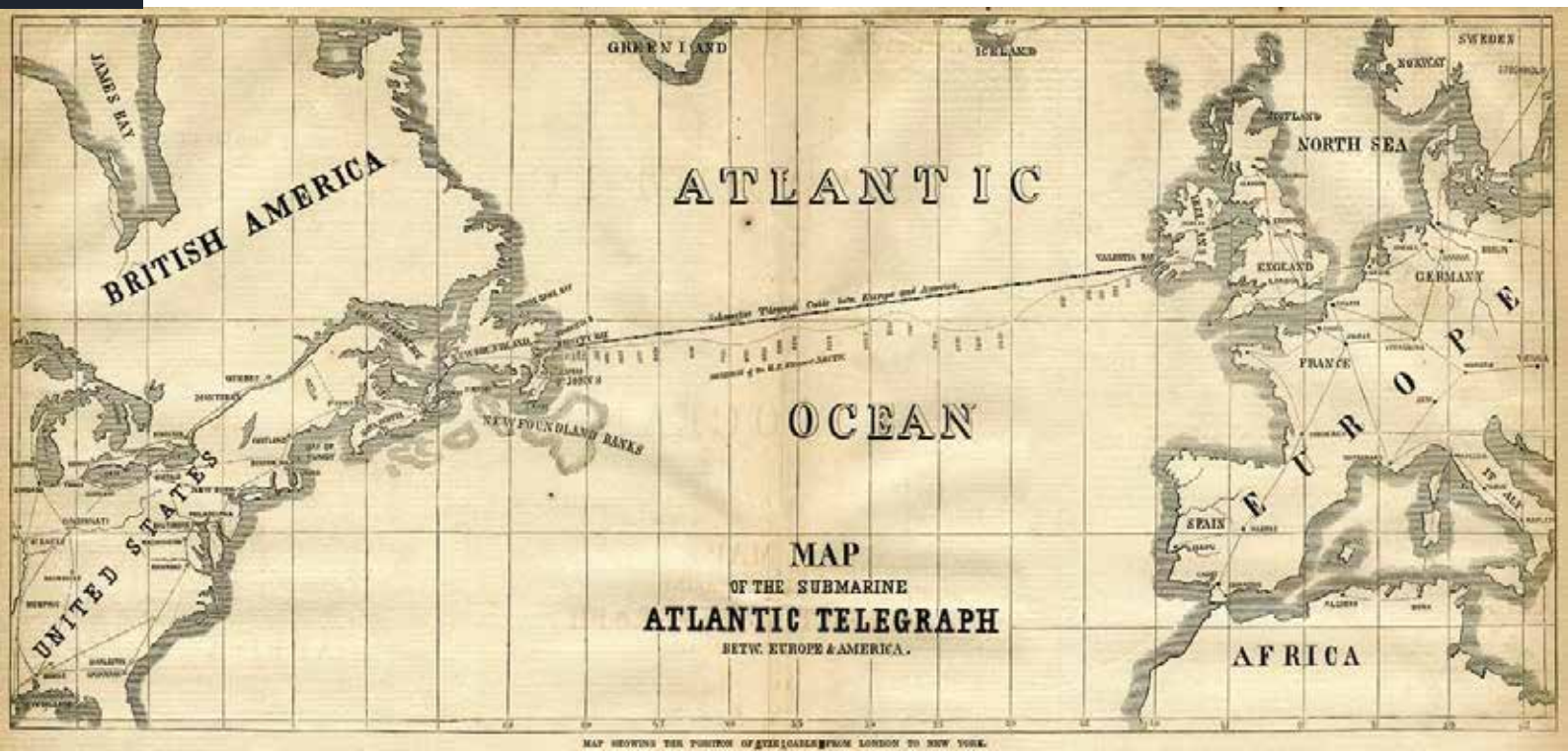
1924 *George Schreiner, a partir de compilação do International Telegraph Bureau*

1969 *UCLA*

2009/2015/2019/2020 *TeleGeography*

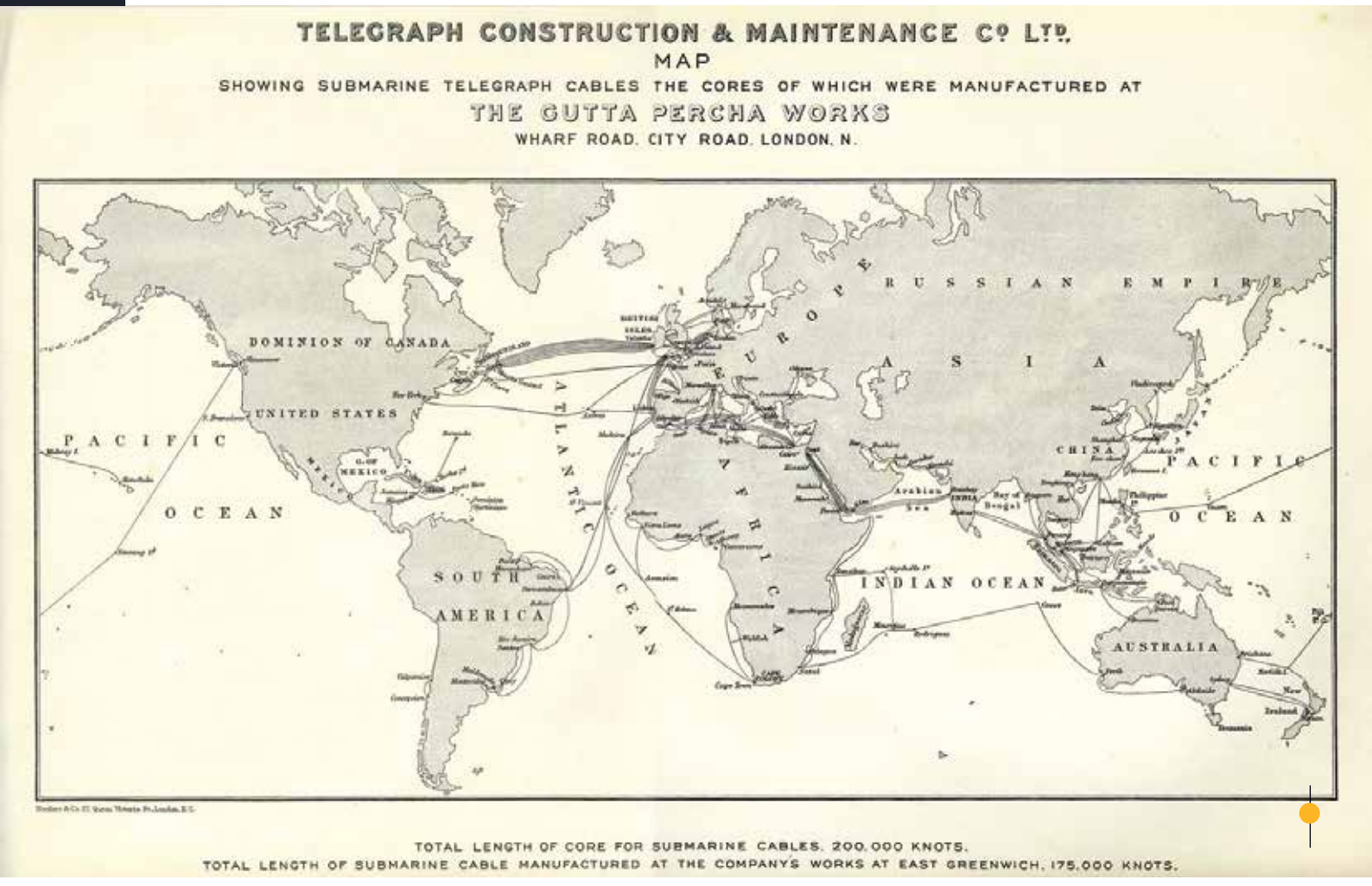
Os cabos submarinos distribuem a Internet por todo o mundo e são responsáveis pela transmissão de 99% dos dados internacionais. Eis alguns exemplos da sua evolução ao longo de mais de século e meio.

1858

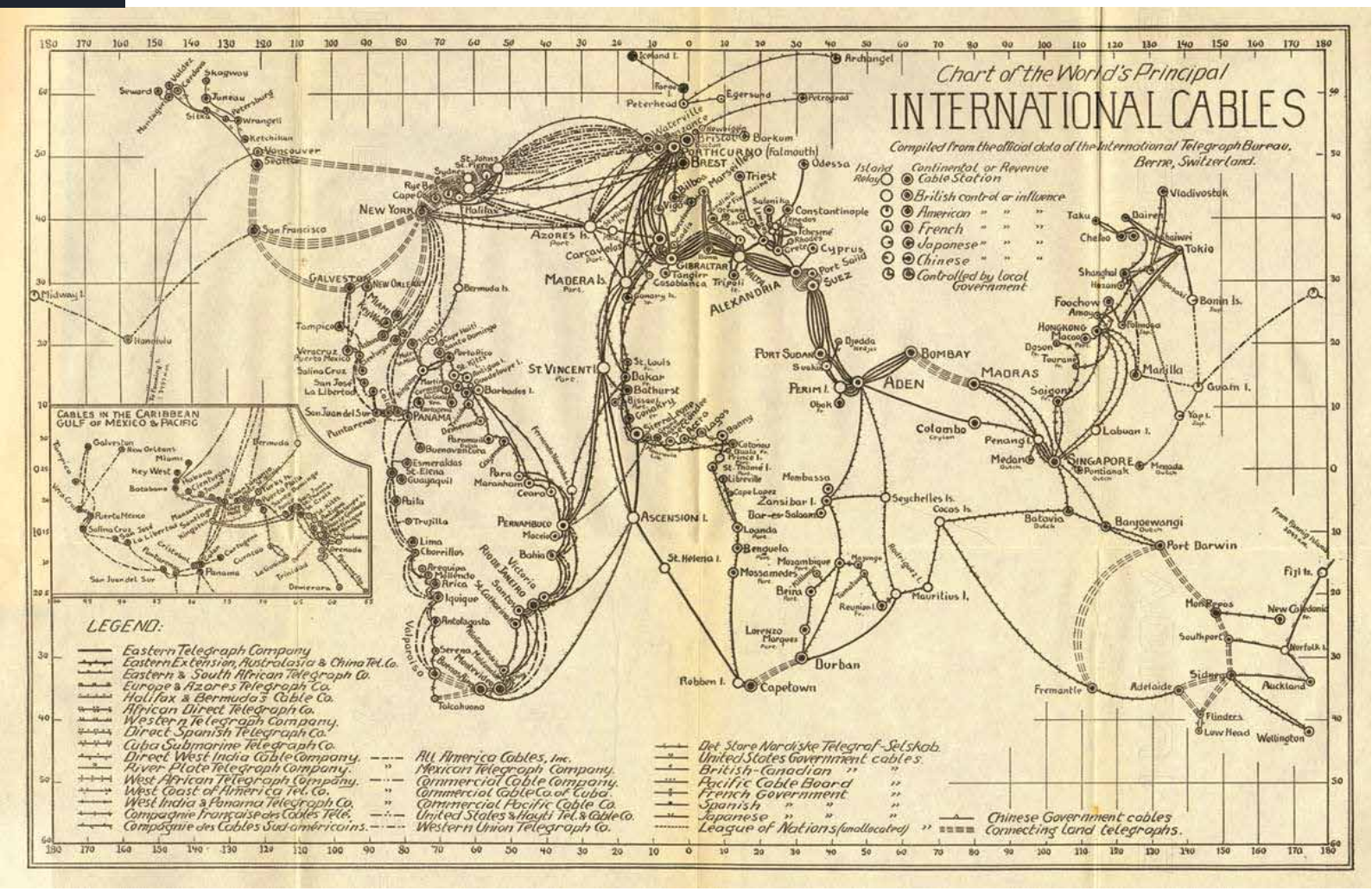


MAP SHEWING THE POSITION OF THE CABLES FROM LONDON TO NEW YORK.

1903



1924



1969

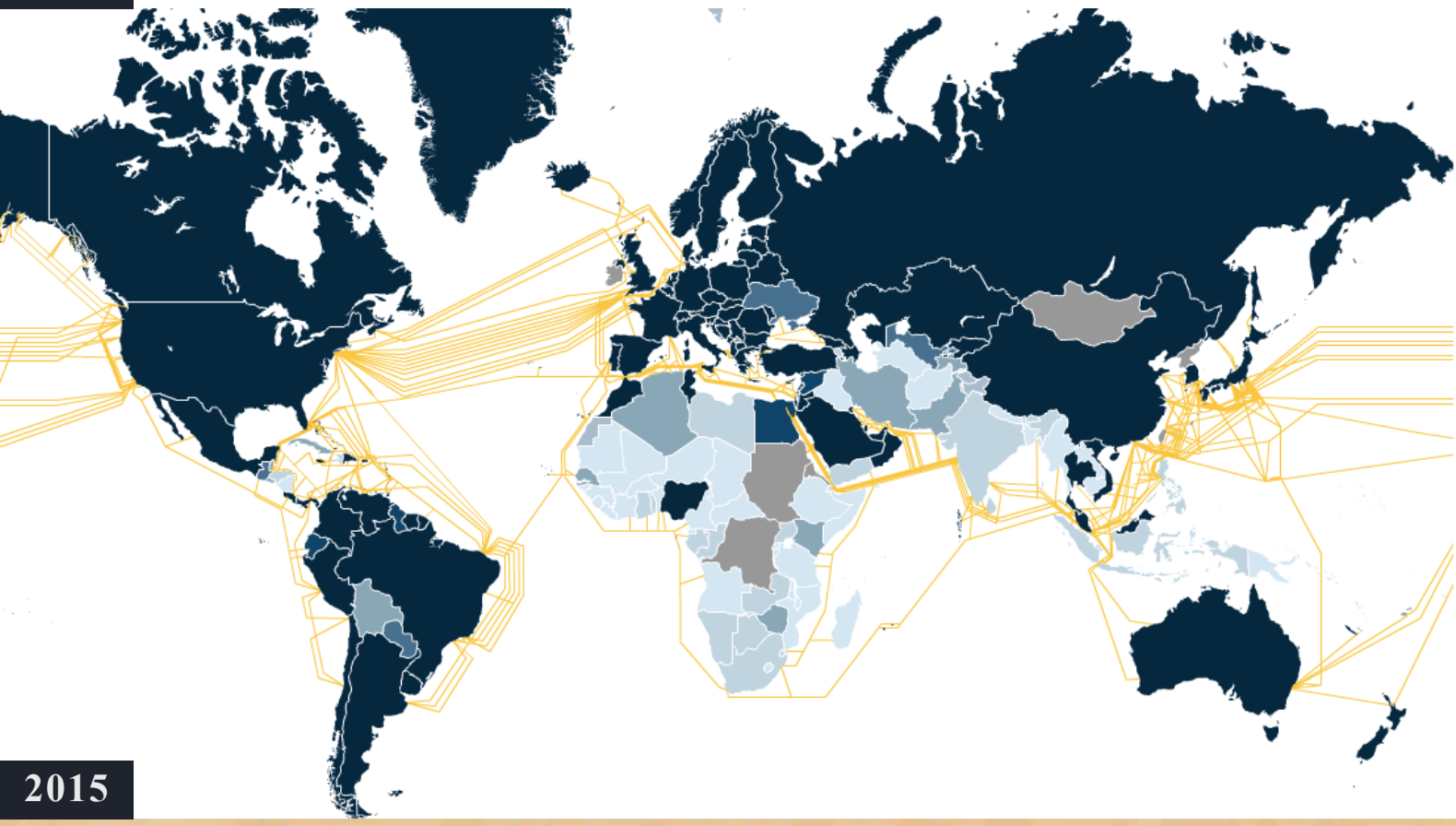
?
Sabia que

Em 1969, existiam apenas quatro nós da Internet por onde circulou o primeiro pacote de dados.

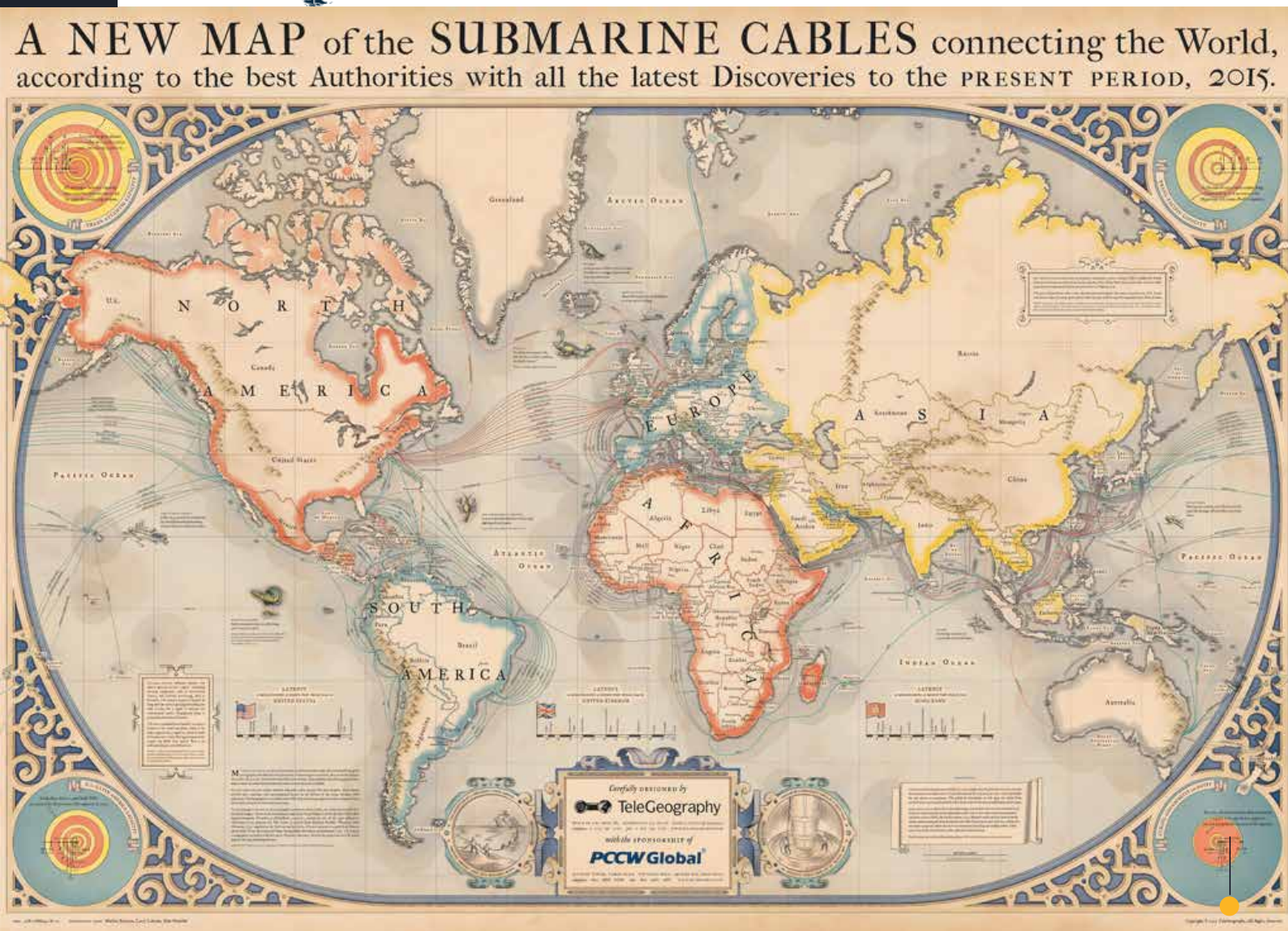
Actualmente, estão online 21,7 mil milhões de equipamentos e a cada segundo são enviados 74,5 GB de dados.

Cisco

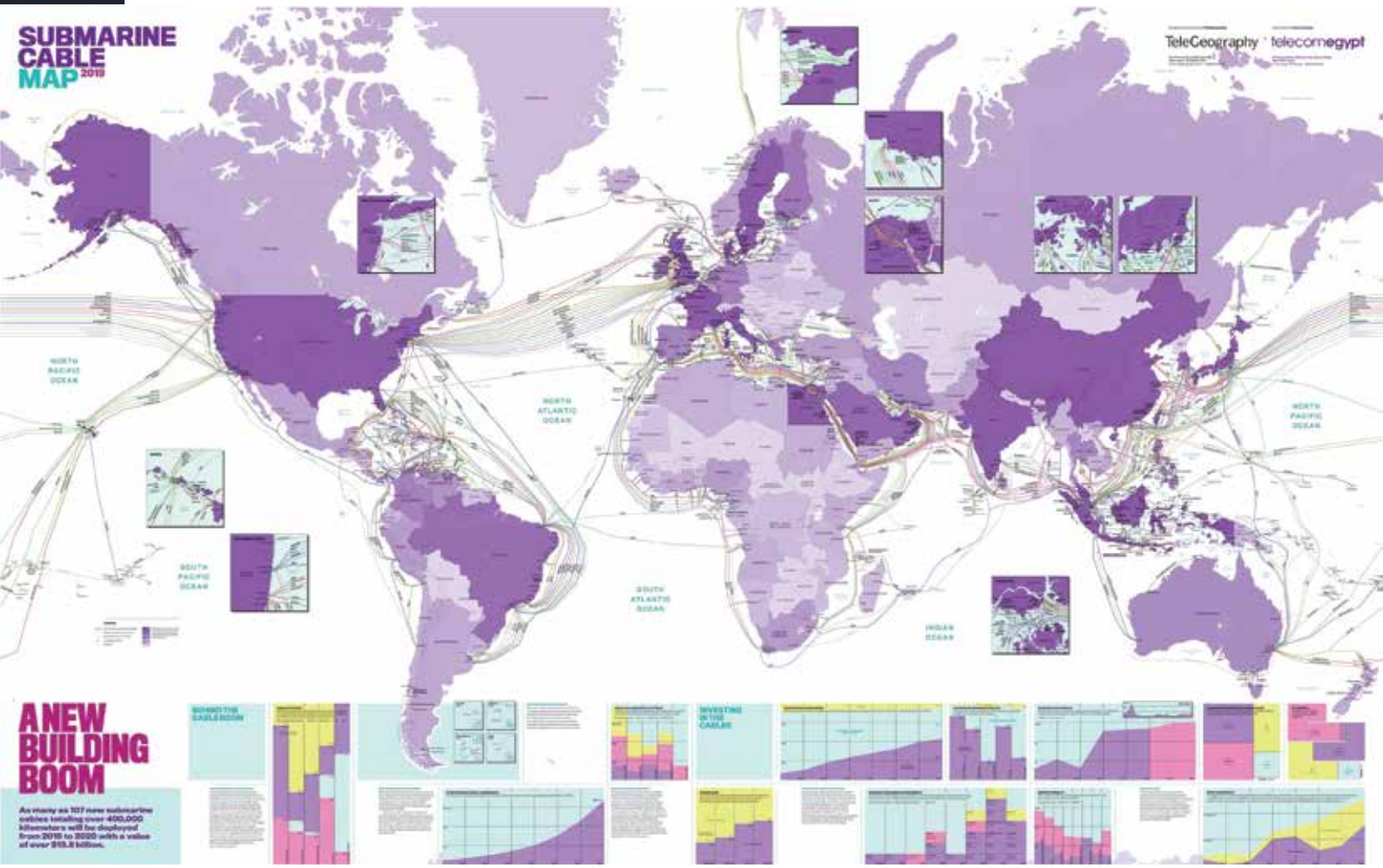
2009



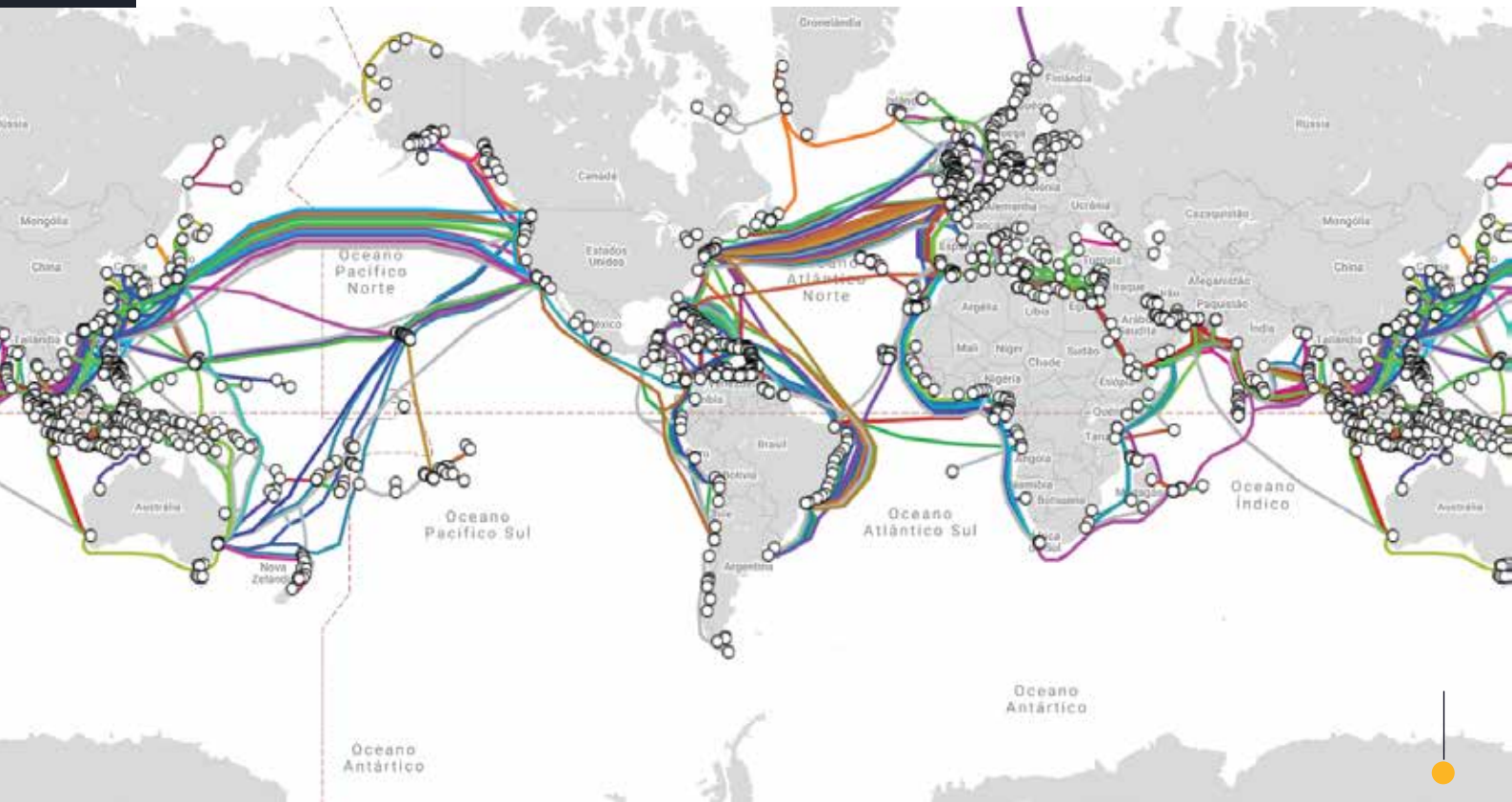
2015


A NEW MAP of the SUBMARINE CABLES connecting the World,
according to the best Authorities with all the latest Discoveries to the PRESENT PERIOD, 2015.
NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
Carefully designed by
TeleGeography
with the sponsorship of
PCCW Global

2019


SUBMARINE CABLE MAP 2019
TeleGeography
telecomegypt
NORTH PACIFIC OCEAN
NORTH ATLANTIC OCEAN
SOUTH PACIFIC OCEAN
SOUTH ATLANTIC OCEAN
INDIAN OCEAN
A NEW BUILDING BOOM
As many as 107 new submarine cables totaling over 400,000 kilometers will be deployed from 2019E to 2020 with a value of over $13.0 billion.

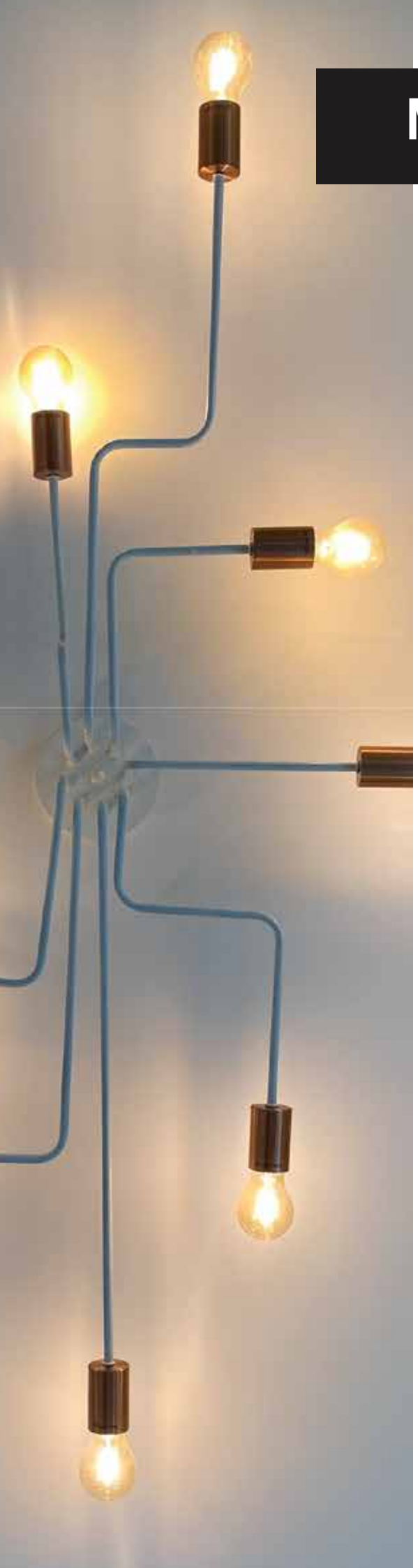
2020


Groenlândia
Finlândia
Rússia
Canadá
Mongólia
China
Estados Unidos
México
Oceano Pacífico Norte
Oceano Atlântico Norte
Argélia
Líbia
Egito
Arábia Saudita
Iraque
Afeganistão
Paquistão
Índia
Mali
Níger
Chade
Sudão
Nigéria
Etiópia
Quénia
Tanzânia
Angola
Namíbia
Botsuana
África do Sul
Brasil
Bolívia
Paraguai
Argentina
Austrália
Nova Zelândia
Oceano Pacífico Sul
Oceano Atlântico Sul
Oceano Índico
Oceano Antártico
Oceano Antártico

?

Sabia que

Dos satélites operacionais no fim do ano passado, 777 eram de comunicações, 710 de observação da Terra, 223 de desenvolvimento tecnológico e 137 de navegação e posicionamento. A maior parte é para utilizadores comerciais, seguindo-se governos, defesa e usos civis.



Mergulho em alto mar

Geoff Huston

Chief Scientist do Asia-Pacific Network Information Centre (APNIC). *Texto publicado originalmente na The ISP Column. Reproduzido sob licença do autor.*

[Em Janeiro de 2019] participei da reunião do New Zealand Network Operator ´s Group (NZNOG'20). Uma das palestras mais interessantes foi dada por Beatty Lane-Davis da Cisco sobre o estado actual da tecnologia dos cabos submarinos. Há algo bastante convincente na engenharia de uma peça de tecnologia de ponta que se destina a ser largada de um barco e depois a operar sem falhas durante os próximos 25 anos ou mais nas profundezas silenciosas dos oceanos! Ela junta física avançada, tecnologia marinha e engenharia para criar algumas peças realmente surpreendentes da infra-estrutura de comunicações.

História potencial (e regionalmente enviesada) dos cabos submarinos

No dia 5 de Agosto de 1856, após um par de falsas partidas, a Atlantic Telegraph Company completou o primeiro cabo telegráfico submarino transatlântico. Era um cabo simples com sete fios condutores de cobre, envoltos em três camadas do novo material maravilha, guta-percha (ou, como o conhecemos hoje, borracha). Isto foi depois embrulhado em cânhamo alcatroado e uma bainha helicoidal de 18 fios de ferro. Não durou muito, pois o engenheiro eléctrico da companhia de cabos, Wildman Whitehouse, tinha uma solução preferida para o desvanecimento do sinal ao aumentar a voltagem do circuito (ao contrário do de William Thompson (mais tarde Lord Kelvin) que escolheu a opção de aumentar a sensibilidade dos seus receptores de galvanómetro em espelho). Um ajuste de potência de 2 kVDC revelou-se fatal para o isolamento do cabo, que simplesmente deixou de funcionar a partir desse momento.

Nos anos seguintes, as técnicas melhoraram, com a adição de amplificadores em linha (ou repetidores) para permitir a propagação do sinal a distâncias mais longas, e melhorias progressivas no processamento do sinal para melhorar a capacidade destes sistemas. O telégrafo transformou-se em telefonia, as válvulas transformaram-se em transístores e os polímeros substituíram a borracha, mas o desenho básico permaneceu o mesmo: um revestimento condutor de cobre numa cobertura isolante estanque, com camisa de aço para proteger o cabo nos segmentos em mais contacto com superfícies.

No contexto australiano, o primeiro sistema telegráfico, concluído em 1872, utilizou uma rota terrestre para Darwin, e depois curtos segmentos submarinos para ligar a Singapura e de lá para a Índia e para o Reino Unido.

Estes cabos eram usados para a telegrafia, e os primeiros sistemas telefónicos trans-oceânicos eram baseados em rádio; demorou algumas décadas até que os avanços na electrónica oferecessem um serviço de voz usando cabos.

Um dos primeiros sistemas a servir a Austrália foi comissionado em 1962. O COMPAC [de Commonwealth Pacific Cable System] suportava canais de voz 80 x 3Khz ligando a Austrália através da Nova Zelândia, Fiji e Hawai ao Canadá, e de lá por um serviço de micro-ondas através do Canadá e depois via CANTAT [de Canada TransAtlantic Telephone Cable] para o Reino Unido. Este cabo usava repetidores submarinos baseados em válvulas. O COMPAC foi desativado em 1984, quando o cabo ANZCAN [acrónimo de Australia/New Zealand-Canada] foi encomendado.

O ANZCAN seguiu um caminho semelhante

através do Pacífico, com segmentos submersos desde Sydney até à Norfolk Island, depois Fiji, Hawai e Canadá. Era um sistema analógico de 14Mhz com repetidores de estado sólido espaçados a cada 13,5km.

Ele foi substituído em 1995 pelo sistema de cabos PACRIM, com capacidade para dois sistemas analógicos de 560 Mhz. O COMPAC teve uma vida útil de 22 anos, e o ANZCAN de 11 anos. O PACRIM teve uma vida comercial inferior a dois anos, porque já era substituível por circuitos submarinos de 2,5 Ghz em sistemas totalmente ópticos, e era terrivelmente inadequado para a procura explosiva da emergente Internet.

Actualmente, existem quase 400 cabos submarinos em serviço em todo o mundo, com uma extensão de 1,2 milhões km.

Propriedade

Os primeiros sistemas de cabo eram incrivelmente caros em comparação com o tamanho das economias que serviam. Os elevados custos de construção e operação tornaram o serviço excessivamente proibitivo para a maioria dos potenciais utilizadores. Por exemplo, quando o Australian Overland Telegraph foi concluído, um telegrama de 30 palavras para o Reino Unido custava o equivalente a três semanas de um salário médio. Em resultado disso, os primeiros utilizadores limitaram-se à imprensa e às agências governamentais.

O sistema de telégrafo terrestre utilizava estações 'repetidoras' onde os operadores humanos gravavam as mensagens recebidas e as re-introduziam no próximo segmento de cabo. Considerando que em toda a Ásia poucos destes operadores de estações repetidoras eram falantes nativos de inglês, não é surpreendente que a taxa de erros nestes telegramas fosse de até um terço das palavras numa mensagem. Portanto, o serviço era ao mesmo tempo extremamente caro e propenso a inúmeros erros.

O que talvez seja mais surpreendente é que as pessoas persistiram apesar desses impedimentos e, com o tempo, o custo baixou e a fiabilidade aumentou.

Muitos desses projetos foram financiados por governos e usaram empresas especializadas que geriam cabos próprios. No final do século XIX, havia a British Indian Submarine Telegraph Company, a Eastern Extension Australasia, a China Telegraph Company e a British Australia Telegraph Company, entre muitas outras. As ligações aos governos eram evidentes, assim como o controlo de todos os serviços de cabos fora da Grã-Bretanha durante a Primeira Guerra Mundial. A emergência do modelo de operador telefónico nacional público na primeira parte do século XX foi espelhada pela natureza pública da propriedade dos sistemas de cabo.

O modelo de propriedade dos consórcios de cabos foi desenvolvido no âmbito de uma estrutura mais ampla, onde um cabo era lançado como uma sociedade anónima privada que levantava capital para construir o cabo como dívida para as instituições bancárias comerciais convencionais. A empresa era efectivamente "propriedade" das transportadoras nacionais que adquiriam capacidade no cabo, onde a quota de propriedade equivalia à quota da capacidade adquirida.

A capacidade adquirida num cabo assumia geralmente a forma de compra de um direito de uso imprescritível (IRU), dando

ao proprietário do IRU acesso exclusivo à capacidade do cabo por um período fixo (geralmente entre 15 e 25 anos, e em grande parte alinhado à vida útil esperada do cabo). O IRU inclui convencionalmente a obrigação de pagar por uma proporção dos custos operacionais do cabo.

Quando o principal cliente dos sistemas de cabos submarinos era o sector nacional de comunicações, os custos de cada um dos IRUs eram normalmente partilhados igualmente entre os dois operadores nos términos dos circuitos do IRU. (Isto fazia parte do regime de liquidação financeira equilibrada dos operadores nacionais, onde o custo da infra-estrutura comum para interligar os serviços de comunicações nacionais era dividido igualmente entre as partes da ligação). Enquanto este modelo foi desenvolvido no mundo dos operadores nacionais monopolistas, a desregulamentação progressiva do mundo dos operadores não teve grande impacto neste modelo de consórcio de propriedade de cabos durante muitas décadas. Parte da lógica deste modelo de custos partilhados de meios circuitos construídos em IRUs de propriedade conjunta era a de que os operadores cooperavam no capital e nos custos recorrentes de construção e operação de instalações e competiam nos serviços.

Um dos elementos essenciais deste estilo burocrático de propriedade era que o preço da capacidade do cabo era determinado pelo consórcio, apresentando qualquer transportador ou grupo de transportadores para desvalorizar os outros membros do consórcio. A intenção era preservar o valor de mercado do cabo, evitando a subcotação e o “dumping”. O resultado real foi um caso clássico de racionamento do lado da oferta e a fixação de preços onde a capacidade do cabo foi lançada no mercado em pequenos incrementos, garantindo que a procura sempre excedesse a capacidade disponível ao longo da vida útil do cabo, e que os preços do cabo permanecessem dinâmicos.

O boom da construção da Internet nos anos 90 coincidiu com a desregulamentação em larga escala de muitos mercados de telecomunicações. Isso permitiu que outras entidades obtivessem direitos de instalação de cabos para muitos países, o que levou à entrada de grossistas no mercado dos cabos submarinos e também ao conceito de "capacidade total de propriedade" ["wholly owned capacity"] no sistema de cabos. Os primeiros participantes nesses mercados eram fornecedores retalhistas do sector emergente dos ISPs, como a Global Crossing, por exemplo, mas não demorou muito para as grandes empresas de conteúdos, incluindo a Google, o Facebook e outras empresas, entrarem neste mercado de capacidade de cabos submarinos com os seus próprios investimentos. A diferença essencial nessa forma de operação é a eliminação da fixação de preços, permitindo que os preços dos cabos reflitam as condições prevalecentes de oferta e procura do mercado.

Cabos

O design básico do cabo físico usado actualmente nestes sistemas submarinos é muito semelhante aos anteriores. O design básico do cabo físico usado hoje para esses sistemas submarinos é praticamente o mesmo dos designs anteriores. O portador do sinal mudou do cobre para a fibra, mas o resto do cabo é praticamente o mesmo. Um membro de aço é fornecido com os portadores de sinal e esses cabos de sinal são enrolados em gel para evitar a abrasão.

?

Sabia que

Entre 2016 e 2021 devem investir-se dois mil milhões de dólares por ano em novos cabos submarinos. Os históricos operadores de redes de comunicações estão a ser substituídos como principais investidores por fornecedores de conteúdos e de cloud Google, Facebook, Amazon ou Microsoft.

TeleGeography

Ao redor do pacote de sinais há um invólucro de cobre para fornecer energia, depois um revestimento impermeabilizado (uma resina de polietileno) e, dependendo da localização pretendida para o específico segmento de cabo, camadas de proteção. Quanto menor a profundidade do segmento do cabo e quanto maior a quantidade de transmissões comerciais, maior o número de elementos de protecção, para que o cabo sobreviva a algumas formas de obstrução acidental.

Normalmente, o cabo é colocado no fundo do mar mas, em áreas de elevada actividade marinha, o cabo revestido de aço pode ser colocado numa vala cavada e, em circunstâncias especiais, pode ser colocado numa calha cortada numa plataforma de rocha do fundo do mar.

A técnica de colocação de cabos não mudou de nenhuma forma significativa. Um segmento inteiro submerso é carregado num navio de assentamento de cabos, testado de ponta a ponta e, em seguida, o navio começa a percorrer o caminho do cabo numa única viagem. A velocidade e a posição do navio são determinadas com cuidado, a fim de posicionar o cabo no fundo do mar sem o colocar sob tensão. O navio navega numa única jornada sem parar, colocando o cabo no fundo do mar, cuja profundidade média é de 3.600 metros e até 11 mil metros na sua maior profundidade. O cabo é esticado durante o assentamento até 8.000 metros atrás do navio.

A reparação do cabo também é tida em consideração. Demora cerca de 20 horas a colocar um segmento a uma profundidade de 6.000 metros, e essa profundidade é praticamente a profundidade máxima possível das operações de reparação dos cabos. Os cabos nas regiões mais profundas não são reparados directamente, mas ligados em ambos os lados. A implicação é que, quando os segmentos de cabo em águas muito profundas falham, a sua reparação pode ser um processo demorado e complexo.

Enquanto os primeiros sistemas de cabo forneciam conectividade ponto a ponto simples, as oportunidades comerciais de usar um único sistema de cabo para conectar muitos pontos finais estimulou a necessidade de fornecimento de unidades de ramificação. A forma mais simples duma unidade de ramificação óptica é dividir as fibras físicas no núcleo do cabo. Actualmente, é mais comum ver o uso de multiplexadores ópticos "add-drop" (ROADMs) reconfiguráveis. Estas unidades permitem que comprimentos de onda individuais ou múltiplos transportando canais de dados sejam adicionados e/ou descartados ["added and/or dropped"] de uma fibra de transporte comum sem a necessidade de converter os sinais em todos os canais multiplexados por divisão de comprimento de onda em sinais electrónicos e voltar depois a ter sinais ópticos. As principais vantagens do uso de ROADMs é o adiamento do planeamento de toda a atribuição de largura de banda com antecedência, pois o ROADMS permite reconfigurar a capacidade do sistema em resposta à procura. A reconfiguração pode ser feita como e quando necessário, sem afectar o tráfego que já está a passar no ROADM.

O sistema submarino é normalmente chamado de segmento húmido e esses sistemas fazem interface com sistemas de superfície em estações de cabo. Essas estações alojam o equipamento que fornece a energia ao cabo. A configuração de energia é DC e os sistemas de cabo de longo curso são alimentados por sistemas que normalmente usam alimentações de 10 kVDC nas duas extremidades do cabo. A

estação de cabo também inclui tipicamente o equipamento de terminação de comprimento de onda e o Line Monitoring Equipment [equipamento de monitorização de linha].

Repetidores ópticos

Os "repetidores" ópticos talvez sejam um nome impróprio hoje em dia. Os repetidores elétricos anteriores operavam num modo de repetição convencional, usando um receptor para converter o sinal analógico de entrada num sinal digital e, em seguida, recodificar os dados num sinal analógico para o injectar no segmento seguinte do cabo.

Actualmente, os repetidores dos cabos ópticos são amplificadores de fotões que operam com ganho total no fundo do oceano por uma vida útil prevista de 25 anos. A luz (a 980nm ou a 1480nm) é bombeada para um relativamente curto segmento de fibra envernizado com érbio. Os iões de érbio fazem com que um fluxo de luz em torno dos 1550nm seja amplificado. A energia bombeada faz com que os iões de érbio entrem num estado de energia mais elevado e, quando estimulado por um sinal de fotão, o ião decai para um nível de energia mais baixo, emitindo um fotão no nível de energia do estado estimulado, mas com uma frequência de luz igual ao sinal de entrada activado. Este sinal amplificado emitido partilha convenientemente a mesma direcção e fase do sinal luminoso recebido. Estes são chamados de unidades EDFA (de "Erbium Doped Fibre Amplifiers"). Isto foi totalmente revolucionário para os cabos submarinos. Todo o segmento húmido, incluindo os repetidores, é totalmente agnóstico em relação ao sinal da operadora. O número de comprimentos de onda a funcionar, a codificação e descodificação do sinal e toda a capacidade do cabo dependem agora do equipamento nas estações em cada extremidade do cabo. Isso prolongou a vida útil dos sistemas ópticos, de onde é possível extrair capacidade adicional dos cabos implantados, colocando novas tecnologias nas estações de cabo em cada extremidade, deixando o segmento húmido inalterado. A planta húmida é agnóstica em relação à capacidade de carga de cabos em todos os sistemas ópticos.

As unidades repetidoras ópticas submarinas foram concebidas para funcionar durante toda a vida operacional do cabo sem qualquer intervenção adicional. O design inclui um elemento de redundância, pois se um repetidor falhar, a capacidade do cabo poderá ser degradada em certa medida, mas ainda funcionará com uma capacidade viável.

As unidades EDFA têm um enviesamento de amplificação em toda a faixa de frequência operacional e é necessário adicionar um filtro passivo ao sinal amplificado para gerar um espectro de potência menos turbulento. Isso permite que a soma cumulativa desses amplificadores em linha produza um resultado que maximize o desempenho do sinal para todo o espectro da banda usada no cabo. Em longas distâncias, isso ainda é insuficiente, e os cabos também podem usar unidades activas, chamadas de "Gain Equalisation Units". As configurações de número, espaçamento e equalização usadas nessas unidades fazem parte do design personalizado de cada sistema de cabos.

Nos sistemas terrestres, o controlo do amplificador pode ser gerido dinamicamente e, à medida que os canais são adicionados ou removidos, os amplificadores podem ser reconfigurados para produzir um ganho ideal. Os amplificadores submarinos não têm esse

controlo dinâmico e são configurados para ganhar saturação, ou sempre no "máximo". A fim de evitar sobrecarregar os canais a funcionar, todos os canais de espectro não utilizados são ocupados por um sinal de "não ocupado".

Os repetidores são um componente de custo significativo do custo total do cabo, e há um compromisso entre um espaçamento "estreito" de repetidores, a cada 60 km ou mais, ou estendendo a distância entre repetidores para 100 km e fazendo uma economia significativa no número de repetidores no sistema. Em suma, quanto mais se estiver preparado para gastar no sistema de cabos, maior será a sua capacidade de carga.

A observação aqui é que um cabo submarino não é construído montando componentes padrão e ligando-os usando um conjunto consistente de regras de projecto de engenharia, mas personalizando cada componente dentro de um projecto sob medida para produzir um sistema construído para optimizar os resultados do seu serviço num ambiente específico em que o cabo deve ser implantado. Em muitos aspectos, qualquer projecto de cabo submarino é construído do zero.

Capacidade de cabo e codificação de sinal

Os primeiros sistemas ópticos de cabos submarinos foram concebidos nos anos 80 e implantados no final dessa década. Esses primeiros sistemas de cabos coaxiais usavam equipamentos de regeneração e amplificação eléctricos, e os amplificadores geralmente eram implantados a cada 40 km no cabo. A primeira medida usada para aumentar a capacidade do cabo foi usar um sistema que havia sido o principal suporte do mundo do rádio por muitos anos, a saber, a multiplexação por divisão de frequência (FDM). Os primeiros cabos de amplificação eléctrica de transmissão óptica usavam a FDM para criar vários circuitos de voz num único transportador de cabo coaxial. Esses cabos suportavam uma capacidade total de 560Mb divididos em cerca de 80 mil circuitos de voz.

Havia planos para duplicar a capacidade dos cabos por portador coaxial desses sistemas ópticos/eléctricos híbridos quando os sistemas EDFA totalmente ópticos foram introduzidos. As primeiras implantações dos sistemas de cabos submarinos EDFA ocorreram em 1994. Esses cabos usavam a mesma forma de frequência por multiplexação baseada em óptica, em que cada cabo óptico é dividido em vários canais discretos de comprimento de onda ("lambda") numa estrutura de partilha análoga ao denominado WDM (Wave Division Multiplexing).

À medida que a frequência do sinal do operador aumentava, juntamente com cabos maiores, o factor de dispersão cromática tornava-se mais crítico. A dispersão cromática descreve o fenómeno em que a luz viaja a velocidades ligeiramente diferentes em diferentes frequências. O que isto significa é que uma entrada de onda quadrada será recebida como uma onda suavizada e, nalgum momento, a distorção introduzida empurrará o sinal além da capacidade do DSP ("digital signal processor" ou processador do sinal digital) para uma descodificação fiável. A resposta à dispersão cromática é o uso de segmentos de fibra de dispersão negativa, onde a envernização do cabo de dispersão negativa com dióxido de germânio é configurada para compensar essa dispersão cromática. Não é de forma alguma uma solução perfeita e, embora

seja possível conceber um sistema de compensação de dispersão que compense esta na [faixa de] frequência média da C-band, as frequências nas extremidades ainda mostrarão uma dispersão cromática significativa ao usar cabos maiores.

Esta primeira geração de sistemas totalmente ópticos utilizava a codificação simples de ligar/desligar (OOK de "on/off keying") do sinal digital na luz do fio. Essa técnica de codificação de sinal OOK foi usada para velocidades de sinal até 10 Gbps por "lambda" num sistema WDM, alcançado em 2000 em sistemas implantados, mas os cabos com capacidade ainda maior por "lambda" são inviáveis para longos pedaços de cabos devido à combinação da dispersão cromática e da dispersão no modo de polarização.

Neste ponto, as técnicas de modulação de radiofrequência coerentes foram introduzidas nos processadores de sinais digitais usados para sinais ópticos, combinados com a multiplexação por divisão de ondas. Isso foi possível com o desenvolvimento de técnicas aprimoradas dos DSP emprestadas do domínio do rádio, onde o equipamento receptor foi capaz de detectar mudanças rápidas na fase do sinal do operador de entrada, bem como as alterações na amplitude e polarização.

Usando esses DSPs é possível modular o sinal em cada "lambda" executando a modulação da fase do sinal. A "Quadrature Phase Shift Keying" (QPSK) define quatro pontos de sinal, cada um separado em mudanças de fase de 90 graus, permitindo que 2 bits sejam codificados num único símbolo. A combinação da codificação no modo de polarização de dois pontos e do QPSK permite 2 bits por símbolo. O resultado prático é que um sistema de transporte óptico de 5Thz em C-band usando QPSK e DWDM pode ser configurado para transportar uma capacidade total em todos os seus canais de cerca de 25Tbps, assumindo uma razoavelmente boa relação sinal/ruído. O outro resultado benéfico é que essas velocidades extremamente elevadas podem ser alcançadas com componentes muito mais acessíveis. Um canal 100G é construído como portadores individuais de 8 x 12,5G.

Esta codificação pode ser aumentada ainda mais com a modulação de amplitude. Além do QPSK, há o 8QAM que adiciona outros quatro pontos à codificação QPSK, somando ofertas de fase adicionais de 45 graus e metade da amplitude. O 8QAM permite uma codificação de grupo de 3 bits por símbolo, mas requer uma melhoria na relação sinal/ruído de 4db. O 16QAM define, como o seu nome sugere, 16 pontos discretos no espaço de amplitude de fase, o que permite a codificação de 4 bits por símbolo, a um custo de mais 3db na relação s/r mínimo aceitável. O limite prático de aumentar o número de pontos de codificação no espaço de amplitude de fase é a relação sinal/ruído do cabo, pois quanto mais complexa a codificação, maiores as exigências impostas ao decodificador. A outra técnica que pode ajudar a extrair um sinal digital denso de um sinal de um operador analógico propenso a ruído é o uso de códigos de Forward Error Correcting (FEC) no sinal digital. Com um custo de uma proporção da capacidade do sinal, os códigos FEC permitem a detecção e correção de um pequeno número de erros por sistema FEC.

O estado da arte actual no FEC é o código Polar, em que o desempenho do canal agora quase diminuiu a diferença para o limite de Shannon, que define a barra para a taxa máxima de uma determinada largura de banda e um determinado nível de ruído.

Agora é viável e económico implantar sistemas de cabos médios e longos com capacidades que se aproximam de 50Tbps numa única fibra. Mas esse não é o limite que podemos alcançar em termos de capacidade destes sistemas.

Existem duas bandas de frequência disponíveis para os projectistas de cabos. A banda convencional é a C-band, que mede comprimentos de onda de 1.530nm a 1.565nm. Existe uma banda adjacente, a L-band, que mede comprimentos de onda de 1.570nm a 1.610nm. Em termos analógicos, existem entre 4,0 e 4,8 THz em cada banda. O uso de ambas as bandas com codificação DWDM e QPSK pode resultar em sistemas de cabos que podem sustentar cerca de 70Tbps por fibra através de 7.500 km de cabo.

A obtenção dessa largura de banda tem um preço considerável, uma vez que as unidades EDFA operam nas faixas C ou L, para que os sistemas de cabos que possuem bandas C e L precisem do dobro do número de amplificadores EDFA (o que, obviamente, exige o dobro da potência injectada nas estações de cabo). Nalgum momento do exercício de projecto de cabos, pode ser mais económico aumentar o número de pares de fibras num cabo do que usar mecanismos de codificação cada vez mais complexos, embora existam algumas limitações à quantidade total de energia que podem ser injectados em cabos submarinos de longa distância; portanto, esses sistemas de longa distância geralmente não têm mais que 8 pares de fibras.

Uma forma diferente de amplificação óptica é usada no Fiber Ramen Amplifier (FRA). O princípio do FRA baseia-se no efeito Stimulated Raman Scattering (SRS). O meio de ganho é a fibra óptica não ser envernizada e a energia transferida para o sinal óptico por um processo óptico não linear conhecido como efeito Raman. Um fotão incidente excita um electrão para o estado virtual e a emissão estimulada ocorre quando o electrão des-excita para o estado vibracional da molécula de vidro. As vantagens dos FRAs são a amplificação variável do comprimento de onda, a compatibilidade com a fibra de modo único instalada e a sua adequação para estender os EDFAs. Os FRAs requerem lasers de potência muito alta e um sofisticado controlo de ganho, no entanto, uma combinação de EDFA e FRA pode resultar numa potência média mais baixa num curto período de tempo. Os FRAs operam numa banda de sinal muito ampla (1280nm - 1650nm).

No entanto, tudo isto pressupõe que o vidro em si seja um meio passivo que exibe distorção (ou ruído) apenas de maneira linear. Duas vezes o cabo, duas vezes a atenuação do sinal e duas vezes o grau de dispersão cromática e assim por diante. Quando grandes quantidades de energia, na forma de fotões, são bombeadas para o vidro, ele exibe um comportamento não linear e, à medida que os níveis de energia aumentam, os comportamentos não lineares tornam-se significativamente mais evidentes.

O efeito Optical Kerr é visto com injecção a laser em cabos ópticos, onde a intensidade da luz pode causar uma alteração no índice de refração do vidro, que por sua vez pode produzir instabilidade na modulação, particularmente na fase da modulação usada nos sistemas ópticos. A dispersão de Brillouin resulta da dispersão de fotões causada por fonões em larga escala e baixa frequência. Raios intensos de luz através do vidro podem induzir vibrações acústicas no meio vidro que geram esses fonões. Isso causa a remodulação do feixe de luz,

bem como a modificação das características de amplificação e absorção da luz.

O resultado é que a sinalização de alta densidade em cabos requer uma elevada potência, o que resulta em distorção não linear do sinal, particularmente em termos de distorção de fase. As vantagens são equilibrar o orçamento de energia, a distorção cromática e de fase e a capacidade do cabo. Algumas das abordagens usadas nos sistemas de cabos actuais incluem codificação diferente para diferentes "lambdas" para optimizar a capacidade total de transporte nos cabos.

O design actual dos cabos desde 2010 deixa amplamente a dispersão para o DSP e elimina os segmentos de compensação de dispersão no próprio cabo. O DSP executa agora a compensação de "feedback". Isso permite uma maior coerência do sinal, embora a um custo de maior complexidade no DSP. Agora, o design do cabo também está a olhar para o diâmetro maior do núcleo de vidro em fibra SPF. O tamanho efectivo maior do núcleo de vidro reduz os efeitos não lineares de tanta energia sendo bombeada no vidro, levando a até dez vezes a capacidade utilizável nesses sistemas de fibra de núcleo maiores. Há também quem esteja a analisar DSPs de maior potência que podem executar mais funções. Isso depende, em certa medida, da Lei de Moore em operação. Aumentar o número de portas num processador permite que uma maior funcionalidade seja carregada no chip DSP e ainda tenha requisitos viáveis de energia e de refrigeração. Mal os DSPs possam operar com compensação de "feedback", eles também podem executar codificação e decodificação adaptáveis. Por exemplo, um DSP pode alternar entre duas codificações PSK para cada par de símbolos. Por exemplo, se todos os símbolos foram codificados com 8QAM e 16QAM alternados, então o resultado é uma média de 7 bits por símbolo, reduzindo os grandes incrementos entre os vários níveis de codificação PSK. O DSP também pode testar os vários pontos de amplitude de fase e reduzir o uso de símbolos com maior probabilidade de erro. Isto é chamado de Probabilistic Constellation Shaping ou PCS. Pode ser combinado com o FEC operando em torno de 30% para fornecer uma ampla gama de níveis de capacidade utilizável para um sistema.

Tendo tudo isto em conta, qual é a capacidade dos sistemas de cabos implantados actualmente? Agora, o cabo com maior capacidade em serviço é o cabo MAREA, [da Facebook, Microsoft e Telxius, que] liga Bilbau na Espanha a Virginia Beach nos EUA, com uma capacidade de 208 Tbps.

Futuros

Não estamos de maneira alguma perto do fim do caminho na evolução dos sistemas de cabos submarinos, e abundam ideias sobre como melhorar o seu custo e o desempenho. A capacidade de transmissão óptica aumentou em um fator de cerca de 100 a cada década nas últimas três décadas e, embora seja imprudente prever que esse ritmo de melhoramento da capacidade será interrompido abruptamente, também é preciso admitir que aguentar esse crescimento assume um grau considerável de inovação tecnológica para os próximos anos.

Uma observação é que o trabalho até agora se concentrou em obter o máximo de um único par de fibras. A questão é que, para conseguir isso, estamos a executar o sistema num modo de energia muito ineficiente, em que uma grande parte da energia é convertida em ruído óptico, que é

necessário filtrar. Uma abordagem alternativa é usar uma coleção de núcleos numa fibra com vários núcleos e conduzir cada núcleo com um nível de energia muito menor. A capacidade do sistema e a eficiência de energia podem ser aprimoradas com essa abordagem.

Os refinamentos dos DSPs continuarão, mas podemos ver alterações nos sistemas que injectam o sinal no cabo. Da mesma maneira que os sistemas DSL vectorizados usam uma pré-compensação no sinal injectado para compensar a distorção do sinal no "loop" de cobre, pode ser possível usar a pré-distorção nos "drivers" do laser ou, possivelmente, nos segmentos EDFA, para obter um desempenho ainda mais elevado destes sistemas submarinos.

Sabia que

A velocidade de largura de banda larga deve duplicar dos 45,9 Mbps em 2018 para 110,4 Mbps em 2023 e nesse ano 300 mil milhões de apps móveis serão transferidas em 2023, a nível global, lideradas pelos media sociais, jogos e produtividade.

Cisco

A governação da internet e o posicionamento de Portugal

Manuel da Costa Cabral

Especialista em Relações Externas da ANACOM. *Texto originalmente publicado em 2014, na Revista de Concorrência e Regulação, edição nº 14/15. Reproduzido sob licença do autor. O presente artigo reflete opiniões pessoais, comprometendo em exclusivo o seu autor.*

I - Introdução

Quem controla a Internet? Quem é "dono" da informação? Quem a pode aceder? Qual o papel dos Governos? Qual a melhor solução para implementar o modelo multistakeholder? Estas são questões fundamentais para as quais não existem respostas óbvias.

No *Global Agenda Outlook 2013*[1], publicado no início de 2013 pela World Economic Forum, a Governação da Internet[2] é apontado como um dos quinze assuntos cuja resolução é mais urgente a nível global, num ranking liderado pela "instabilidade da economia mundial" e pela "fragilidade da zona euro".

A Agenda de Tunis para a Sociedade de Informação[3][4] define Governação da Internet como "o desenvolvimento e aplicação de princípios, normas, regras e procedimentos de tomada de decisão, que moldam a evolução e o uso da Internet, por parte dos Governos, setor privado e sociedade civil, no âmbito das suas competências". Lê-se ainda na Agenda de Tunis que "a Governação da Internet deve ser multilateral, transparente e democrática, compreendendo o total envolvimento de Governos, setor privado, sociedade civil e organizações internacionais. Deve assegurar uma distribuição de recursos equitativa, facilitar o acesso para todos e assegurar um funcionamento estável e seguro da Internet, tendo em consideração o multilinguismo".

Está, pois, consagrado que a Governação da Internet assenta no modelo de *multistakeholder*, no qual entidades públicas e privadas cooperam para atingir os objetivos identificados.

Em termos práticos, poderemos ver a Governação da Internet de duas formas distintas: num contexto mais restrito, que aponta a Governação da Internet como a gestão de um conjunto de componentes técnicos que permitem a Internet funcionar; num contexto mais lato, onde, para além dos aspetos técnicos, se inclui um conjunto de fatores que moldam as políticas em torno da Internet, como os custos de acesso, a privacidade, liberdade de expressão ou segurança. É este segundo contexto que mais nos interessa, porque é nele que se desenvolve o debate em torno da Internet nos variados fóruns internacionais que abordam o tema.

Com base na análise feita sugerimos, por fim, um posicionamento para a atuação de Portugal nesta matéria.

II – O quadro global da Governação da Internet: identificação das grandes questões

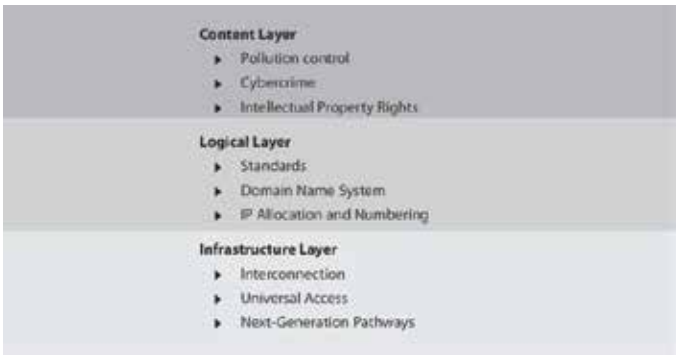
1. Considerações prévias

A urgência do debate da Governação da Internet não é alheia ao papel vital que a mesma assume nas sociedades atuais, nem à enorme controvérsia que o assunto tem vindo a suscitar, nomeadamente em fóruns internacionais como a União Internacional de Telecomunicações (UIT), agência das Nações Unidas para as Telecomunicações. Diversos países, nomeadamente Rússia, China, e alguns Estados Árabes, têm demonstrado desconfiança em relação ao *Internet Corporation for Assigned Names and Numbers (ICANN)*, instituição que desempenha funções na gestão de recursos de numeração, nomes e endereçamento IPs. Para um conjunto de países, num cenário ideal, as funções do ICANN deveriam ser assumidas por um organismo de direito internacional, como a própria UIT. Não sendo tal cenário facilmente realizável,

atendendo à oposição dos EUA, e seus aliados, tem vindo a ser exigido o reforço do poder dos Governos nestas matérias e em concreto no processo de tomada de decisão do ICANN. Por outro lado, Estados Unidos, diversos países da Europa e outros aliados, como Canadá, Austrália ou Japão consideram que algumas das exigências de reforma das instituições que controlam a Internet têm objetivos não confessáveis que passam pelo reforço das medidas de controlo e/ou barramento das comunicações, ou por outras palavras, pelo reforço da possibilidade de vigilância e censura. Consideram, assim, que as propostas de alguns Estados-Membros põem em causa a Internet livre e aberta que conhecemos. Os EUA garantem ainda que não dispõem de instrumentos para influenciar as decisões vitais do ICANN.

É neste cenário, de profunda divisão, que há quem sugira que nos encontramos perante uma Guerra Fria digital[5].

Mas a Governação da Internet está longe de se circunscrever a disputas entre países. O tema suscita debate entre Governos e Sociedade Civil; operadores tradicionais e prestadores *over-the-top* (OTT)[6]; ou entre a liberdade individual e a segurança nacional. Procuraremos aprofundar o que está em causa nesse debate, sendo certo que dada a definição abrangente consagrada na Agenda de Tunis, a Governação da Internet respeita a um leque muito variado de assuntos. Akash Kapur[7] dividiu o tema da Governação da Internet em três níveis: Infraestrutura, lógico e conteúdo.



Consideramos que a sistematização em três níveis oferecida por Kapur continua útil, se bem que naturalmente, com o transcurso do tempo, a caracterização dos tópicos relevantes em cada um dos níveis se tenha vindo a alterar.

No presente artigo, exploraremos alguns dos tópicos mais controversos na atualidade a nível internacional, a saber:

- Custos de acesso (nível de infraestrutura);
- Qualidade de serviço e neutralidade de rede (nível de infraestrutura);
- *Domain Name System* – DNS – *Sistema de nomes de domínios (nível lógico);*
- Numeração e endereçamento (nível lógico);
- Segurança (transversal a todos os níveis);

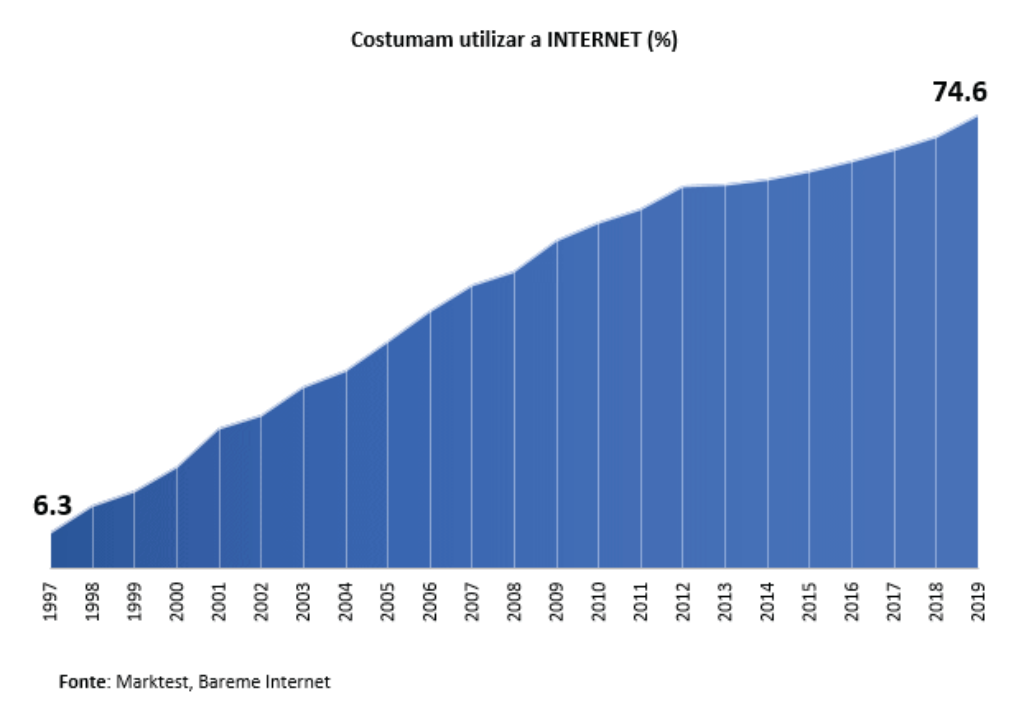
2. Custos de acesso

A *International Internet Connectivity* pode ser definida como o acesso internacional ao conjunto de meios através do qual um país pode aceder ao *backbone* da Internet Global. Este conjunto de meios inclui satélites e cabos de fibra ótica (terrestres ou submarinos).

O custo de acesso à Internet tem sido um tópico crucial para os países em desenvolvimento, em particular, em África e América do Sul, regiões onde os custos de acesso são elevados em comparação com outras regiões, o que condiciona o acesso à Internet pelas populações. Na verdade, o modelo em que assenta a Internet, a que alguns designam como *"receiver pays"* (no qual os *Internet Service*

Sabia que

Portugal tem 6,3 milhões de utilizadores de Internet. A percentagem de utilizadores passou de 6,3% em 1997 para os actuais 74,6%.



Marktest

Providers – ISPs - que recebem a informação pagam o circuito internacional por completo), contribui para estes custos acrescidos. Uma vez que os conteúdos estão alojados fundamentalmente em países desenvolvidos, os países em desenvolvimento alegam estarem mais dependentes da largura de banda internacional[8]. Por isso mesmo, têm defendido, nos diversos fóruns internacionais, a revisão da fórmula para a repartição dos custos.

De notar, contudo, que a propagação de Internet *exchange points* (IXPs), infraestruturas que permitem que diversos *players* se interliguem diretamente entre si, tem contribuído para melhorar a qualidade de serviço e reduzir custos de transmissão. Os IXPs contribuiram para um desenvolvimento da Internet na América do Norte, Europa e Ásia e têm gradualmente vindo a ser implementados nas regiões mais desfavorecidas de África ou América Latina[9], muitas vezes com o apoio técnico e financeiro proporcionado por programas de desenvolvimento. A propagação de IXPs tem contribuído para diminuir os custos de acesso nos países em desenvolvimento, embora haja ainda um largo percurso a percorrer até porque se trata de uma infraestrutura que exige elevados investimentos e conhecimentos técnicos, que não estão ao alcance de grande parte desses países.

Esta questão parece ser, de resto, crucial para o desenvolvimento futuro da Internet, atendendo a que o crescimento mais acelerado de produção de conteúdos e de volume tráfego se verificará precisamente nos países em desenvolvimento.

3. Qualidade de serviço e neutralidade de rede

A qualidade de serviço e a neutralidade de rede expõem uma tensão crescente entre os operadores de telecomunicações tradicionais e os prestadores *over-the-top* (OTT).

Os operadores tradicionais de telecomunicações, e em particular a *European Telecommunications Network Operators' Association* (ETNO)[10], têm defendido que o atual modelo de Internet resulta num desequilíbrio entre o esforço de investimento e a receita gerada. Assim, alegam que enquanto os operadores de telecomunicações investem na proliferação e melhoria das redes, têm sido os prestadores OTT a beneficiar desse investimento, dado que obtêm elevadas receitas pela prestação de serviços/aplicações que "correm" sobre as redes construídas por terceiros.

No processo de preparação para a *World Conference on International Communication* (WCIT-12), organizada pela UIT e realizada em dezembro de 2012, com o intuito de rever o Regulamento das Telecomunicações Internacionais[11], os operadores tradicionais apresentaram propostas para diminuir o alegado desequilíbrio entre investimento e receitas. As propostas dos operadores apontavam para a criação de um novo ecossistema para a interligação IP, o que facilitaria a que paralelamente a uma qualidade de serviço baseada no princípio *best-effort*[12], subsistisse uma qualidade de serviço *end-to-end*[13]. Com base no princípio *end-to-end* seria exequível estabelecer uma política de interligação que diferenciasse a qualidade de serviço de acordo com o tipo de serviço e tráfego. No fundo, os operadores defendem que se um OTT pretende assegurar a "entrega" de um serviço / aplicação com um determinado nível de qualidade de serviço assegurado, terá de pagar um *fee* para o efeito. Deste modo, os operadores poderiam aumentar receitas e fazer face às exigências de

investimento, nomeadamente em redes de nova geração. De notar, contudo, que estas propostas não mereceram o apoio da WCIT-12.

Ainda assim, as exigências dos operadores tradicionais têm-se feito ouvir não apenas no âmbito da UIT, mas também a nível europeu. Neste contexto, parece ser de particular relevância a proposta de regulação *"Connected Continent"* recentemente tornada pública pela Comissão Europeia[14]. No seu art.º 23 (*"Freedom to provide and avail of open internet access, and reasonable traffic management"*), a Comissão pretende consagrar a proibição de os operadores bloquearem, tornarem mais lento ou degradarem determinado tipo de conteúdo, aplicações ou serviços (art.º 23º § 5). Por outro lado, a Comissão estabelece a possibilidade de os prestadores de conteúdo, aplicações e serviços acordarem com os operadores de telecomunicações a transmissão de determinado tipo de tráfego com uma qualidade de serviço pré-definida, ou com capacidade dedicada (art.º 23º § 2). Salvo melhor opinião, a Comissão parecia abrir assim a porta às pretensões dos operadores, reforçando a legitimidade do princípio da qualidade de serviço garantida *end-to-end* na prestação de serviços de Internet.

Neste sentido, a proposta da Comissão para a revisão do enquadramento regulatório tem o mérito de inovar pois alarga o seu âmbito aos prestadores OTT.

No entanto, as discussões no Conselho Europeu (no qual têm assento países que adotaram legislação proibitiva de práticas que possam pôr em causa o princípio da neutralidade de rede, como a Holanda, Luxemburgo ou Eslovénia[15]), e especialmente no Parlamento Europeu[16] fazem prever que se deverão manter restrições à aplicação de um modelo baseado numa qualidade de serviço *end-to-end*. Aguarda-se, assim, com expectativa o resultado de todas estas negociações.

4. *Domain Name System* – DNS – Sistema de nomes de domínios

No topo de uma pirâmide que gere os recursos críticos de Internet encontra-se o ICANN (*Internet Corporation for Assigned Names and Numbers*). O ICANN é uma organização norte-americana de direito privado, que se orgulha de atuar de acordo com o modelo *multistakeholder*, segundo o qual Governos, setor privado, Academia e sociedade civil têm a possibilidade de fazer ouvir os seus pontos de vista e contribuir para a tomada de decisão.

Na sequência de um memorando assinado entre o Departamento de Comércio (DoC) dos EUA e o ICANN em Novembro de 1998, a gestão do *Domain Name System* – DNS (Sistema de nomes de domínios) passou para o controlo do ICANN[17]. Este Memorando teve precisamente por objetivo libertar estas funções do controlo governamental dos EUA. Salienta-se contudo que o DoC dos EUA mantém a autoridade de alterar o detentor do poder de gestão do DNS, significando que em casos extremos o DoC poderia não renovar o contrato com o ICANN, o que na prática determinaria o fim desta organização. Por outro lado, o DoC tem o poder de aprovar modificações ao chamado *root zone file* (*Root Zone* refere-se ao nível mais elevado da estrutura do DNS, que contém a informação necessária ao funcionamento de todos os domínios de topo), pelo que a adição de novos domínios de topo passa também pela aprovação do DoC.

A influência dos EUA na Internet tem naturalmente uma razão histórica

relevante: A Internet foi inventada pelos norte-americanos. É, assim, natural que as instituições que gerem alguns dos seus recursos críticos sejam o legado desse facto histórico.

De qualquer forma, a autoridade que os EUA detêm sobre o ICANN acaba por descredibilizar a ideia defendida pelos norte-americanos segundo a qual o seu poder de influência sobre o ICANN não se sobrepõe ao de outros Estados, sendo, por isso, crescente a pressão para que esse poder seja efetivamente reduzido.

Foi neste contexto, sintomática, a Declaração de Montevideu, assinada por diversas entidades relevantes na comunidade da Internet, incluindo o próprio ICANN, em outubro de 2013, apelando, nomeadamente, a uma globalização do ICANN, subentendendo-se um apelo a um menor controlo dos EUA sobre o ICANN[18].

Adicionalmente, conforme indicado anteriormente um conjunto alargado de países, incluindo alguns BRICS[19], acredita que num cenário ideal, as funções do ICANN deveriam ser assumidas por um organismo de direito internacional, como a própria UIT. No lado oposto, EUA e diversos aliados opõem-se vivamente a todas as iniciativas que procurem dotar a UIT de poderes na gestão do DNS, considerando que o caráter dinâmico e inovador da Internet ficaria fortemente ameaçado se as decisões sobre a gestão dos seus recursos críticos passassem a ser tomadas por uma agência das Nações Unidas, cujos processos de tomadas de decisões alguns consideram lentos e pouco ágeis.

Atendendo à difícil concretização de reformas mais profundas, diversos países exigem, pelo menos, o reforço do poder dos Governos nestas matérias e em concreto no processo de tomada de decisão do ICANN. Neste contexto, têm sido particularmente audíveis as exigências de reforma do *Governmental Advisory Committee* (GAC)[20] do ICANN, organismo no qual se fazem representar os Governos, e cujas opiniões sobre políticas públicas deverão ser tomadas em consideração pelo *Board* do ICANN. Deste modo, tem vindo a ser pugnado um reforço dos poderes do GAC de modo a que os seus pareceres adquiram uma natureza tendencialmente vinculativa, pretendendo-se que o *Board* do ICANN[21] tenha uma menor margem de manobra para atuar ao arrepio dos pareceres do GAC. Na realidade, este grupo de países, do qual o Brasil se tem assumido como um dos líderes, considera que o GAC é um órgão fraco, que não garante as condições necessárias à efetiva participação dos governos nos processos de tomada de decisão. Todo este contexto de pressão internacional terá seguramente contribuído para que os EUA, em Março de 2014, tenham emitido uma declaração na qual convidam o ICANN a reunir os diversos *stakeholders* com o intuito de formular uma proposta de transferência das atuais funções dos EUA na coordenação do *Domain Name System* - DNS[22].

- É importante realçar, contudo, que muitos pontos de interrogação se levantam com esta declaração, desconhecendo-se, nomeadamente, quem assumirá as funções de coordenação do DNS e quais são exatamente as funções a que os EUA se referem.

De qualquer modo, este parece ser um marco relevante, que abre a porta a que importantes desenvolvimentos venham a ocorrer na forma como o ICANN e em concreto a coordenação do DNS são organizados.

a) Caso prático: A tensão em torno dos novos gTLDs

A aprovação dos novos domínios genéricos de topo (ex: .hotel; .site; .nyc)[23] surge como uma das faces visíveis dos antagonismos patentes no processo de tomada de decisão do ICANN. O processo de criação destes novos domínios foi controverso desde a sua origem (2005), suscitando muitas reservas, nomeadamente por parte do GAC, quanto a questões de segurança, proteção de consumidores e defesa da propriedade industrial[24]. Paradigmático foi o caso dos novos domínios de topo ".Amazon" ou ".wine" / ".vin". Em função das pressões do Brasil e de outros países daquela região, o GAC opôs-se à criação do ".Amazon", que havia sido solicitada pela *Amazon*, empresa de vendas online. Na base da oposição do Brasil, esteve o facto de a Amazónia ser uma região do Brasil e de outros países sul-americanos, pelo que o uso desse domínio de topo deveria ser vedado a uma empresa privada. De notar que neste processo apenas os EUA apoiaram a pretensão da criação do ".Amazon" pela empresa Amazon. A decisão final sobre o domínio de topo ".Amazon" ainda está pendente, apesar do parecer do GAC, uma vez que o *Board* do ICANN ainda não tomou a decisão final.

Com base em argumentos similares, a Comissão Europeia contestou a possibilidade de virem a ser criados os domínios de topo ".wine" e ".vin". Em carta remetida a Fadi Chehadé, Presidente e CEO do ICANN, em setembro de 2013, Nellie Kroes, Vice-presidente da Comissão, declarava *"under no circumstance can we agree having .wine and .vin and on the internet, without sufficient safeguards which efficiently protect the rights and interest of both Geographic Indicator right holders and consumers and wine and wine products"*[25].

O ICANN ainda não tomou uma decisão sobre os domínios ".wine" e ".vin" devendo fazê-lo proximamente. Poderá dizer-se, para sintetizar, que os diferendos em torno da questão da gestão dos domínios têm uma dimensão política na qual alguns os governos procuram ter um maior poder no processo de tomada de decisão. Não se pode, porém, negligenciar uma dimensão económica: só por si a empresa Amazon terá investido cerca de 14 milhões de dólares em processos de candidatura de novos domínios de topo[26].

5. Numeração e endereços IP

Cada equipamento conectado à Internet é identificado por um endereço IP. Estes endereços, que são usados para encaminhar os pacotes de dados, são um recurso finito. O ICANN, através da IANA (*Internet Assigned Names Authority*)[27], tem também a função de gerir a alocação de endereços IP. Assim, o ICANN distribui as moradas IP a cinco *Regional Internet Registries* (RIRs) que por sua vez atribui os endereços aos ISPs ou diretamente a empresas que necessitem dos endereços IP para o desenvolvimento das suas redes internas. Na Europa, a função de RIR está atribuída à *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) [28].
Atualmente a maior parte dos equipamentos utiliza o chamado IPv4 (exemplo de endereço IPv4: 192.0.2.235), que permite em teoria gerar um conjunto de 4 mil milhões de endereços[29]. No entanto, devido ao crescimento galopante do número de equipamentos ligados à Internet, os endereços IPv4 acabaram por escassear, pelo que foi desenvolvido uma nova versão de endereços IP, o IPv6 (exemplo de endereço IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334) que permitirá gerar, em teoria, um número praticamente inesgotável de endereços IP.

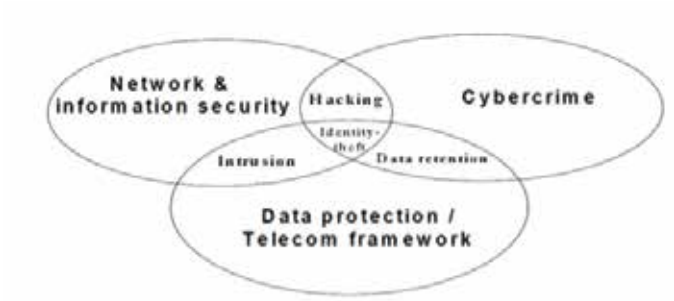
A exaustão de recursos IPv4 disponíveis e a migração para o IPv6 tem servido de pretexto para exigências de reforma na Governação dos endereços IP. Estas reformas podem ser sistematizadas em dois níveis: operacional e institucional.

No plano operacional, nos fóruns internacionais tem-se vindo a discutir a forma de alocação dos endereços IPv6. Alguns países sustentam que a política de alocação deve ser similar à realizada no IPv4, isto é, com base no *"first come, first serve"*, tendo como pressuposto uma necessidade demonstrável. Contudo, outro conjunto de países advoga que o princípio utilizado no IPv4 levou uma rápida ocupação de recursos finitos, pelo que se for novamente utilizado na distribuição de endereços IPv6, os países que procurem mais tardiamente tais recursos endereços IPv6, tipicamente os países em desenvolvimento, sairão prejudicados. Para estes países a alocação de endereços IPv4 não decorreu de forma eficiente, argumentando que existe uma proporção muito significativa de endereços que nunca foram usados, apesar de já terem sido atribuídos a diversas organizações[30].

No plano institucional, enquanto alguns países advogam uma transformação profunda do modelo institucional, sugerindo, por exemplo, que a própria UIT atue como um RIR, ficando responsável pela atribuição de endereços, outros países referem que uma melhoria dos processos das atuais instituições será suficiente para garantir uma eficiente migração para o IPv6. Para este último grupo, a intervenção da UIT neste processo teria consequências negativas, uma vez que o iria tornar necessariamente mais pesado e burocrático.

6. Segurança e Privacidade

As questões de segurança e privacidade são para muitos o problema central da Governação da Internet. Assuntos como a recolha e retenção da vida de cada um de nós, o poder das corporações que armazenam tais dados, o papel e ao eficácia do legislador para combater práticas abusivas, o combate ao cibercrime, e as ações de espionagem são incontornáveis na discussão da Governação da Internet. De acordo com a Comissão Europeia, as questões de segurança podem ser sumarizadas no seguinte diagrama:



Fonte: Comissão Europeia[31]

Considera-se que os três vetores são aplicáveis quando se discutem questões de segurança na Internet. No entanto será de realçar que, na sua maioria, os países desenvolvidos procuram limitar o âmbito da discussão da Governação da Internet ao vetor da "Network and Information Security", alegando que as restantes dimensões alargariam o âmbito da Governação da Internet para assuntos como os de foro criminal. No entanto, os três vetores são, na prática, abordados nos principais fóruns internacionais, como a UIT ou o *Internet Governance Forum* (IGF), pelo que daremos breve nota de alguns aspetos que têm gerado polémica.

- **"Network and Information Security"**

A Comissão Europeia define: *"Network and information security can be understood as the*

ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems". Neste vetor de Segurança de redes e de Informação realça-se a importância de se construir redes resilientes e robustas, o que acaba por ser do interesse geral.

▪ Cibercrime

Esta é uma área que em geral os países desenvolvidos querem ver afastada dos fóruns de Governação da Internet, alegando que a mesma deverá ser tratada ao nível da cooperação judicial. Um leque alargado de países desenvolvidos são subscritores da Convenção de Budapeste sobre Cibercrime, tratado internacional acordado no âmbito do Conselho da Europa para definir os crimes praticados por meio da Internet e agilizar a cooperação para identificar e localizar os autores dos mesmos. Embora se trate de um texto acordado no âmbito de uma instituição europeia, países não europeus, como o Canadá, Japão, Estados Unidos e África do Sul, são igualmente signatários do Tratado. No total, 29 países, entre os quais Portugal, já ratificaram a Convenção de Budapeste, enquanto que outros 17 países já assinaram, mas ainda não ratificaram. Há, no entanto, Membros do Conselho da Europa que ainda não assinaram a adesão ao Tratado, destacando-se neste grupo Rússia e Turquia[32].

Em Portugal, a Convenção sobre Cibercrime é concretizada na Lei nº109/2009, de 15 de setembro.

Apesar de poder ser considerado um assunto que ultrapassa o âmbito da Governação da Internet, diversos países, tipicamente os não signatários da Convenção de Budapeste, insistem para que algumas questões de cibercrime sejam analisadas em fóruns como a UIT, atendendo a que consideram que a prevenção de alguns crimes passa por ações de cariz técnico. Assim, são, por exemplo, frequentes debates em torno de temas como a *child online protection*, discutindo-se soluções técnicas e formas de cooperação que, por exemplo, impossibilitem o acesso a determinados conteúdos por crianças.

▪ Proteção de dados / Privacidade

Conforme referimos anteriormente Estados Unidos e diversos aliados consideram que as exigências de reforma da Governação da Internet constituem uma ameaça séria a uma Internet livre e aberta que hoje conhecemos, pois encobrem o desejo de um maior controlo dos conteúdos que são transmitidos pela Internet. Neste contexto, podemos dizer que o assunto da segurança sempre foi debatido nestes fóruns e que na base desse debate esteve latente uma desconfiança, ou uma suspeita, que determinados conteúdos pudessem ser, ou vir a ser, monitorizados por um determinado Estado-Membro.

A este propósito, as notícias sobre violações da privacidade por parte da *National Security Agency* (NSA), que denunciaram um programa de espionagem de larga escala (PRISM) visando comunicações estabelecidas através da Internet, deram ampla visibilidade pública a temas que têm vindo a ser debatidos em diversos fóruns mundiais, nomeadamente, na UIT. Contudo, estas denúncias parecem ter alterado a forma de encarar o tema da vigilância e de a discutir nestes fóruns.

Assim, as revelações em torno do PRISM serviram de pretexto para que o debate em

torno da espionagem de comunicações deixasse de estar dissimulado em considerações técnicas ou jurídicas. Os relatos[33] que surgem do IGF de 2013, que se realizou em outubro, na Indonésia, são eloquentes quanto à forma clara e incisiva como o tema da espionagem foi tratado nesse fórum. Adicionalmente, estas denúncias contribuíram para reforçar o caráter político e de alto nível das discussões em torno da Governação da Internet, a ponto de Dilma Rousseff, Presidente do Brasil, ter transformado o assunto na sua principal bandeira, no seu recente discurso na 68ª Assembleia Geral das Nações Unidas[34 35].

Finalmente, e não menos importante, estas revelações poderão estar a contribuir para alterar o xadrez geopolítico. A este propósito, saliente-se a proposta de resolução conjunta que Brasil e Alemanha apresentaram à Assembleia Geral da ONU, sobre o direito à privacidade na era digital[36], e que viria a ser aprovada por unanimidade por aquela Assembleia em dezembro de 2013.
Na Europa, o debate sobre a privacidade das comunicações e em particular dos dados armazenados na Internet, também parece estar a ser influenciado com a revelação do caso PRISM. A Comissão Europeia, por intermédio da Comissária para os Assuntos de Justiça, Viviane Reding, havia apresentado uma proposta de reforma das regras de proteção de dados[37] em janeiro de 2012. Esta proposta revelou-se, porém, muito controversa, com a Comissão a ser acusada, por alguns Estados-Membros, de ser demasiado exigente com determinados prestadores, incluindo os OTT.

As primeiras revelações de Edward Snowden, em maio de 2013, parecem ter contribuído para uma alteração das vontades políticas, o que tem sido aproveitado pela Comissão Europeia para dar novo fôlego à proposta sobre as regras para a proteção de dados. Referindo que, de acordo com algumas estimativas, as revelações sobre o PRISM poderão custar à indústria da *cloud computing* norte-americana, entre $22 a $35 mil milhões de dólares de receita nos próximos 3 anos, Viviane Reding[38] assumiu a necessidade de reforçar a confiança dos cidadãos na "economia digital".

Concretizando o apoio político à reforma proposta pela Comissão, o Conselho Europeu de 24 e 25 de outubro de 2013, declarou que a mesma "é essencial para a realização do mercado único digital até 2015"[39]

Adicionalmente, em março de 2014 o Parlamento Europeu votou favoravelmente à reforma da legislação sobre proteção de dados, que assenta em 4 pilares fundamentais:

- **Primeiro pilar**: Um continente, uma Lei. Para ajudar a concretizar este pilar, a reforma aprovada pelo Parlamento Europeu compreende um regulamento e uma diretiva sobre o assunto. Sendo o regulamento de aplicação direta pelos Estamos-Membros, não requerendo transposição, a harmonização legislativa é mais facilmente concretizável;

- **Segundo Pilar**: As empresas não europeias que operem na União Europeia, vão ter de obedecer às regras comunitárias

- **Terceiro Pilar**: Consagração do direito a ser esquecido, isto é, sempre que um utilizador desejar que os seus dados pessoais não continuem a ser armazenados por um qualquer prestador de serviço, tais dados deverão ser removidos, desde que não existam razões legítimas que justifiquem o contrário;

· Quarto Pilar: Criação de um "One-stop-shop" para empresas e cidadãos, no sentido de facilitar a apresentação de denúncias contra uma empresa sediada noutro país.

A reforma aprovada pelo Parlamento terá ainda de ser adotada pelo Conselho da União Europeia.

III – O debate institucional em torno da Governação da Internet

Uma vez identificados alguns dos principais assuntos da Governação da Internet, importa indicar os mais relevantes fóruns de direito privado e direito internacional em que esta matéria é debatida internacionalmente e na qual os Governos têm vindo a participar ativamente.

1. Entidades de direito privado

São de mencionar as seguintes:

· GAC do *ICANN*: Entidade a que nos referimos no ponto anterior

· *Internet Society* (ISOC)[40]: Entidade que reúne milhares de membros, entre os quais os principais OTT, e que persegue diversos objetivos, como o desenvolvimento de normas, protocolos e infraestrutura técnica para a Internet. A ISOC procura ainda a criação de comunidades para a discussão de políticas nacionais e internacionais para o desenvolvimento da Internet. Esta função é atualmente distribuída por 90 comunidades nacionais, designadas "chapters"[41]

· *The Internet Engineering Task Force* (IETF): é uma das ramificações do ISOC, de particular relevância na área da normalização para a Internet, tendo desenvolvido, por exemplo, o IPv6.

2. Organizações internacionais

Sistematizaremos as organizações internacionais que têm a Governação da Internet na sua agenda em três grupos: Nações Unidas, OCDE, e União Europeia.

a) Nações Unidas

A Assembleia Geral da ONU tem sido palco de variados debates e decisões sobre o Governação da Internet. Entre as decisões relevantes conta-se a criação da *World Summit on Information Society* e a renovação do mandato do *Internet Governance Forum* (ver adiante Fóruns Internacionais).

Adicionalmente esta matéria é discutida em diversas agências das Nações Unidas, destacando-se, neste particular a:

· *União Internacional das Telecomunicações* (UIT) - como vimos anteriormente alguns Estados-Membros reclamam que esta organização assuma as principais funções do ICANN e/ou que assuma o papel de RIR, isto é, o papel de distribuição dos endereços IP aos ISPs. A UIT organiza como veremos seguidamente diversos fóruns relevantes para a Governação da Internet.

▪ *United Nations Education, Science and Cultural Organisation* (UNESCO) - a participação desta organização visa potenciar a Internet como catalizador do desenvolvimento humano, contribuindo para a consolidação de sociedades democráticas através da livre circulação de informação e ideias.

▪ *World Intellectual Property Organization* (WIPO) – Esta agência tem tido particular relevo no registo de novos domínios genéricos de topo, cujo processo tem levantado problemas de direitos de autor.

Ainda no âmbito das Nações Unidas

saliente-se ainda o *High-level UN Group on Information Society* (UNGIS), que tem por missão assegurar a coordenação das diversas agências da ONU.

Vários fóruns são organizados sob a égide das Nações Unidas:

▪ *World Summit on Information Society* (WSIS): A WSIS consistiu de dois eventos sobre a Sociedade da Informação que ocorreram em 2003 em Genebra e em 2005 em Túnis (da qual resultou a Agenda de Tunis, referida no Capítulo da Introdução do presente *paper*).

Esta Cimeira foi o resultado de uma Resolução da Assembleia Geral das Nações Unidas, em 2001, que atribuiu à UIT o papel de organizador do evento, em coordenação com outras agências das Nações Unidas.

▪ *World Conference on International Telecommunication (WCIT-12)*: A WCIT-12, organizada pela UIT, decorreu de 3 a 14 de dezembro de 2012, no Dubai, Emirados Árabes Unidos e reuniu 151 Estados-Membros, acabou por ser um marco importante para expor as fortes divergências que existem a nível global face à Governação da Internet. Na realidade, a Conferência foi agendada com intuito de rever o Regulamento das Telecomunicações Internacionais que estabelece princípios gerais para a prestação e operacionalização das telecomunicações internacionais, mas acabou por se centrar em larga medida no debate sobre o controlo da Internet e o peso dos Governos nessa matéria. A divisão patente nessa Conferência, resultou em Atos Finais[42], que não foram assinados pelos países da União Europeia, bem como pela maioria dos países desenvolvidos.

▪ *Internet Governance Forum (IGF)*: Estabelecido na WSIS de 2005, o IGF tem como objectivo a criação de um fórum *multistakeholder* em que Governos, Academia e Sociedade Civil debatem matérias da Governação da Internet. Por decisão de dezembro de 2010, da Assembleia Geral das Nações Unidas, foi renovado o mandato do IGF até 2015. Pela mesma decisão, a Comissão das Nações Unidas para a Ciência e Tecnologia (CSTD) foi mandatada a desenvolver propostas visando a melhoria do IGF, tendo sido criado, no âmbito desse mandato, um Grupo de Trabalho, no qual têm vindo a participar 22 Governos.

O IGF 2013, que se realizou em Outubro, na Indonésia, foi dominado pelas questões de segurança e privacidade.

b) Organização para Cooperação e Desenvolvimento Económico (OCDE)

Esta organização tem dado importantes contributos para abordagem de questões económicas da Internet. Em junho de 2011, a OCDE aprovou os Princípios para a Política para a Internet[43], os quais pretendem contribuir para uma Internet propulsora da Inovação e do Crescimento.

c) Europa e União Europeia

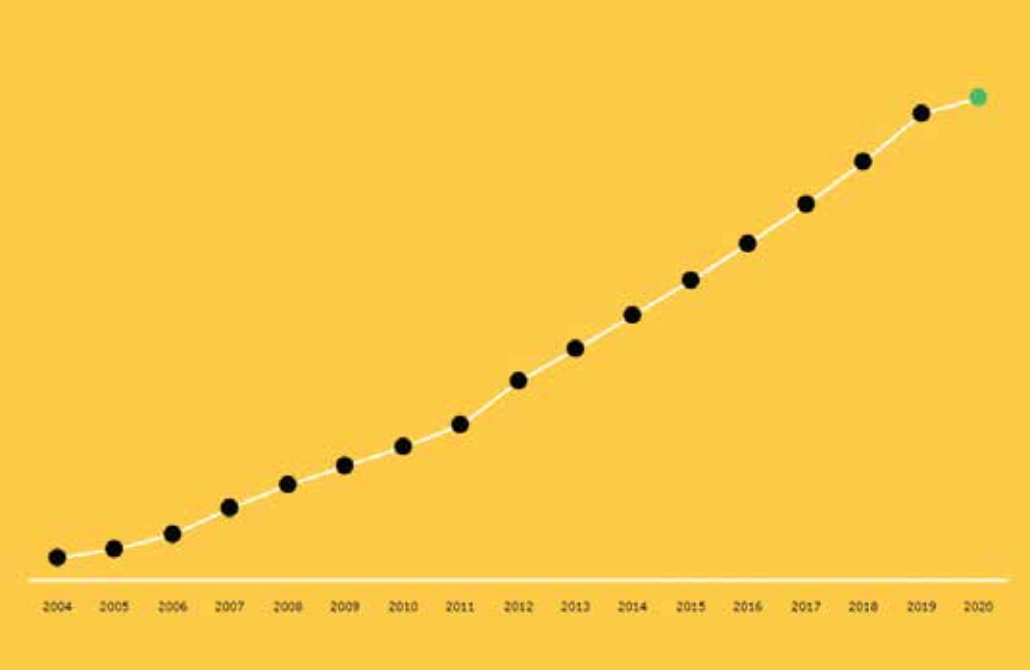
Na Europa, devemos desde logo destacar a *European Conference of Postal and Telecommunications Administrations* (CEPT), que integra 48 países da Europa, e que, entre outras competências, define a posição Europeia na UIT.

A União Europeia tem vindo a debater naturalmente matérias relacionadas com a Governação da Internet. Destaque-se, neste ponto, o *High-Level Group on Internet Governance* (HLIG), que é presidido pela Comissão Europeia, no qual participam os Estados-Membros da UE, Noruega e Suíça, e onde se discute a posição da UE para

?

Sabia que

Em 2019, o domínio de topo .pt atingiu um novo recorde, com 121.359 novos registos (mais 10.799 do que no ano anterior). Do total dos 1,2 milhões de endereços registados, quase 369 mil estavam activos e mais de 453 mil eram registos automáticos de Empresa na Hora.



fóruns como o GAC do ICANN ou o IGF.

Refira-se que em maio de 2013, a Comissão Europeia anunciou a criação da *Global Internet Policy Observatory* (GIPO), que pretende ser uma plataforma on-line com vista a melhorar a participação de todos os *stakehholders* nos debates e decisões sobre política de Internet. O GIPO foi desenvolvido em ligação com países como o Brasil e a Suíça, e organizações como a União Africana e a *Internet Society*.

IV- Portugal e a Governação da Internet

1. Situação atual

Procuraremos em cada uma das matérias tratadas anteriormente, identificar a entidade ou entidades com responsabilidade de acompanhamento / deliberação sobre as mesmas.

A questão dos *custos de acesso* é uma questão da responsabilidade do regulador setorial das comunicações, a ANACOM. Desde logo, a Lei 5/2004, de 10 de fevereiro, conforme revista pela Lei n.º 51/2011, de 13 de setembro (Lei das Comunicações Eletrónicas), confere à ANACOM a incumbência de "Eliminar os obstáculos existentes à oferta de redes de comunicações eletrónicas[44], de recursos e serviços conexos e de serviços de comunicações eletrónicas a nível europeu" (conforme n.º 3 alínea a) do art 5ª).

As questões de "*Qualidade de serviço e de neutralidade de rede*" estão igualmente sob a alçada do regulador das comunicações. Conforme referido anteriormente a proposta para nova revisão do enquadramento regulamentar europeu parece indicar que estas matérias tornar-se-ão ainda mais relevantes para as ARNs europeias.

No que concerne ao *Domain Name System*, a entrada em vigor do Decreto-Lei n.º 55 / 2013 de 17 de abril[45], procedeu à extinção da FCCN, tendo as funções dessa entidade respeitante à gestão do domínio de topo ".pt" transitado para a Associação DNS.PT[46], associação privada sem fins lucrativos, formalmente criada a 9 de maio de 2013. Assim, nos termos desse diploma, os direitos e obrigações até então por prosseguidos pela FCCN, no âmbito da delegação efetuada pela IANA a 30 de junho de 1988 (RFC 1032, 1033, 1034 e 1591), foram transmitidos para a Associação DNS.PT[47].

A Associação DNS.PT, tem como fundadores a Fundação para a Ciência e a Tecnologia, IP (FCT)[48], Associação do Comércio Eletrónico e Publicidade Interativa (ACEPI), Associação Portuguesa para a Defesa do Consumidor (DECO) e o representante designado pela IANA como responsável pela delegação do ccTLD.pt. A Autoridade Nacional de Comunicações (ANACOM) é uma das entidades que integra o Conselho Consultivo da DNS.PT. Note-se ainda que com a extinção da FCCN todas as suas restantes funções foram transferidas para a FCT.

Ao nível da *Numeração e endereços IP (nível lógico)* as entidades nacionais têm reduzida margem para intervenção, uma vez que o processo está centralizado na RIPE NCC, que assume as funções de RIR na Europa e que atribui diretamente estes recursos aos ISPs.

Nas questões de *segurança e privacidade*, as responsabilidades estão partilhadas por diversas entidades. A Lei das Comunicações Eletrónicas atribui à ANACOM a incumbência de "assegurar que seja mantida a integridade e a segurança das redes de comunicações públicas" e confere à mesma entidade a responsabilidade de "Contribuir para garantir um elevado nível de proteção dos dados pessoais e da pri-

vacidade". Em matéria de privacidade, destaque-se ainda a Comissão Nacional da Proteção de Dados que tem missão controlar e fiscalizar o processamento de dados pessoais, em respeito pelas liberdades e garantias consagradas na Constituição e na lei, devendo para o efeito cooperar com as autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

Na vertente do *Cibercrime*, realce-se o Gabinete de Coordenação da Atividade do Ministério Público na área da Cibercriminalidade (Gabinete Cibercrime)[49] que tem sede na Procuradoria-Geral da República, de que é diretamente dependente. Este Gabinete tem por missão assegurar a coordenação interna do Ministério Público, nesta área da criminalidade, garantir a formação específica e estabelecer canais de comunicação com fornecedores de serviço de acesso às redes de comunicação, que permitam facilitar a sua colaboração na investigação criminal.

De destacar ainda alguns projetos que resultam de parcerias de diversas entidades que pretendem contribuir para uma Internet mais segura. Neste âmbito, destacamos o Projeto InternetSegura[50]. Trata-se de uma iniciativa que nasce de consórcio coordenado pela FCT e que envolve, nomeadamente, o Ministério da Educação e a Microsoft Portugal. Este Projeto tem como principais objetivos o combate a conteúdos ilegais; a promoção de uma utilização segura da Internet; e a consciencialização da sociedade para os riscos associados à utilização da Internet.

A representação internacional é, em larga medida, assegurada pela FCT, que acompanha o GAC do ICANN, o IGF e a nível da União Europeia, o *HLIG*, e a ANACOM que acompanha a UIT e a CEPT.

2. O confronto com outros países europeus

Em outros países da Europa, as questões de custos de acesso, qualidade de serviço e neutralidade de rede são em grande medida da responsabilidade das ARNs, até porque tal função decorre das Diretivas Europeias para o setor das comunicações eletrónicas.

A situação é bem mais complexa nas questões de segurança e privacidade[51], uma vez que entre os países europeus convivem diferentes arranjos para tratar destas matérias. Se existe um traço comum entre os países europeus é o da multiplicidade de organismos com responsabilidades nestas áreas e a preocupação em criar mecanismos de coordenação entre os mesmos. Se alguns países atribuem à ARN uma responsabilidade central em matérias de segurança (como a Dinamarca, Finlândia, Suécia, Chipre ou Bulgária), a maioria dos países tende a atribuir esta responsabilidade a departamentos ministeriais (Reino Unido, Alemanha, França ou Espanha). Outra solução frequente entre os países europeus passa pela criação de plataformas ou grupos de trabalho interministeriais com o único objetivo de coordenar das entidades públicas e privadas relevantes (França, Irlanda, República Checa ou Bélgica).

No que respeita às questões de numeração, nomes e endereços, também subsiste uma considerável diferença na forma de acompanhamento destes assuntos.

Em alguns países a opção passou por atribuir aos reguladores de comunicações responsabilidades na gestão destes recursos críticos da Internet nos seus respetivos países. Na Finlândia, a ARN (Ficora) tem um papel de regulação do

domínio ".fi". Neste contexto, incumbe à ARN: (i) submeter anualmente ao Governo uma proposta com o valor das tarifas dos domínios ".fi"; (ii) supervisionar os cerca de 1000 *resgistrars* (entidades que vendem os domínios aos utilizadores finais).

A PTS, regulador da Suécia, assume responsabilidades nesta matéria. A PTS é responsável pela coordenação de um Grupo de Trabalho para a Governação da Internet, que reúne aproximadamente 20 organizações suecas (Ministérios das Comunicações, da Justiça e dos Negócios de estrangeiros, ISOC-SE, Academia e algumas empresas).

A BIPT, Bélgica, é igualmente uma ARN com responsabilidades pelo acompanhamento de aspetos relativos aos recursos críticos da Internet (números, nomes, e endereços). No seu Relatório Anual de 2012 pode ler-se que está entre as preocupações da BIPT a escassez dos endereços IPv4 e as suas implicações ao nível da segurança[52].

A RRT, Lituânia, assume as funções de gestão e supervisão dos recursos de numeração tradicionais e de outros "identificadores de rede", o que inclui os recursos de nomes e endereçamento.

Fora da União Europeia, destaque-se também para a Ofcom, da Suíça, como outro caso em que a ARN é o principal interlocutor nacional para as questões da Governação da Internet, no seu conjunto.

Em todos os casos descritos, as ARNs garantem o acompanhamento dos principais fóruns de Governação Internet, como sejam o GAC do ICANN, IGF ou a UIT.

3. Perspetivas de evolução em Portugal: algumas propostas

Não obstante a indefinição a nível internacional sobre o melhor modelo a adotar na Governação da Internet, estamos em crer que, a nível nacional, é possível aperfeiçoar, desde já, o modelo organizativo existente, de modo a adaptar o mesmo à realidade atual e a reforçar a coordenação e as sinergias das competências neste domínio.

Assim, para que a posição de Portugal se fortaleça a nível internacional, consideramos necessário um aprofundamento dos mecanismos de coordenação, entre entidades públicas, setor privado, Academia ou representantes da sociedade civil com responsabilidade / interesse nas matérias identificadas no capítulo II do presente artigo. Deste modo, à semelhança do que se verifica noutros países poder-se-á enveredar pela constituição de plataformas / grupos de trabalho que permitam agilizar procedimentos de partilha de conhecimentos entre as entidades interessadas.
No fundo, propõe-se que, à escala nacional, sejam desenvolvidos mecanismos que permitam dar um impulso adicional ao modelo *multistakeholder*.

Em tese, poder-se-á equacionar ainda a evolução do modelo de regulador 'tradicional' de telecomunicações, para um regulador setorial que atue num ambiente convergente, com responsabilidades acrescidas em algumas das matérias identificadas.

Uma vez criadas as condições internas para abordar a Governação da Internet de forma mais abrangente e consistente, Portugal estará em melhores condições para fazer passar o seu posicionamento na

matéria, a nível internacional. Na realidade, conforme se avançou no início deste trabalho, as cisões em torno da Governação da Internet são comparadas a uma Guerra Fria Digital, o que, no limite, poderá levar a que alguns países, não confiantes nas atuais instâncias de governação da Internet, avancem para a construção de uma rede alternativa, que não passe por essas entidades. Ora, isto seria a fragmentação da Internet, com efeitos negativos para todos os países, e naturalmente também para Portugal.

As posições de Portugal nos diferentes fóruns deverão ser coordenadas a nível europeu, tanto a nível da União Europeia, como da CEPT. Nas organizações europeias, entendemos que Portugal deverá trabalhar ativamente no sentido de reforçar a sua capacidade de influência sobre as orientações estratégicas europeias.

Noutro plano, Portugal deverá intensificar a sua atuação junto da CPLP no sentido de procurar harmonizar posições, identificando pontos de concordância e eventual discordância.
Nestes diferentes contextos, Portugal deverá defender alguns princípios fundamentais, a saber:

- O modelo multistakeholder, no qual Governos, sociedade civil, setor privado, organizações internacionais e academia participam e têm a oportunidade de se fazer ouvir.

Uma abordagem light touch. O dinamismo e a capacidade de inovação que tem caracterizado tudo aquilo que rodeia a Internet não podem ser constrangidos por desnecessárias intervenções regulatórias, embora em determinados casos se admita como necessária uma regulação mais ativa (vide escassez de endereços IPv4, em parte explicada por recursos que não são usados).

Na defesa destes princípios, Portugal deve ter presente a importância histórica que os Estados Unidos tiveram na criação da Internet e que é dos Estados Unidos que continuam a surgir muitas das mais inovadoras aplicações que fazem com que a Internet seja um bem indispensável nos nossos dias, ao ponto de as Nações Unidas terem decretado o Acesso à Internet como parte integrante dos Direitos Humanos[53].

Mas devemos ter também presente que é a universalização da Internet que faz da mesma aquilo que é hoje. O valor da Internet reside sobretudo nos cerca de 2,7 mil milhões de utilizadores em todo o mundo[54]. E esta universalização torna compreensível que vários países peçam mais poder de influência nas decisões que afetam a rede das redes, porque no fundo sentem que a Internet também é sua. Neste sentido, defendemos que deverão ser apoiadas as reformas que permitam a criação de um modelo institucional que melhor capte e traduza esta universalização, e que ao mesmo tempo deem garantias de salvaguarda do caráter livre, aberto, dinâmico e inovador da Internet.

Para sintetizar, consideramos que Portugal deverá ter como objetivo a mitigação dos fortes atritos que hoje ocorrem em torno da Governação da Internet e a criação de pontes entre os diferentes intervenientes.

Importa, por fim, não desprezar a influência que Portugal pode ter. Logicamente que não somos potência mundial, ou sequer potência regional. Mas Portugal é um país desenvolvido, da União Europeia e da OCDE, ao mesmo tempo que tem fortes ligações históricas, quer com o Brasil, já hoje um líder global, e particularmente ativo nas questões da Governação da Inter-

net, quer com vários países em desenvolvimento, de África, Ásia e demais América Latina. E, acima de tudo, não se pode negligenciar o facto de o Português ser a 5ª língua mais utilizada na Internet[55].

V. Notas conclusivas

A análise constante do presente artigo suporta a ideia de que a Governação da Internet está longe de estar confinada à gestão técnica de recursos críticos da Internet, como os nomes e endereços IP. A Governação da Internet passa também pelo desenvolvimento de infraestruturas e acesso às mesmas, passa pela qualidade de serviço e pela polémica questão da neutralidade de rede, e passa necessariamente pelas cruciais questões de segurança e privacidade. Outros temas não aprofundados no presente artigo, como direitos de autor ou a liberdade de expressão, fazem igualmente parte do âmbito da Governação da Internet.

Ficou também patente que apesar de a Internet fazer, há largos anos, parte do dia-a-dia dos cidadãos, ainda subsiste uma indefinição a nível internacional, e inevitavelmente a nível nacional, sobre o papel dos Governos nesta matéria. Consideramos que na base dessa indefinição está precisamente a importância política, social e económica da Internet, o que faz com que qualquer eventual reforma na sua Governação seja analisada à luz de múltiplos interesses e critérios. Neste contexto, sublinhámos que a Governação da Internet suscita divergências não apenas entre países, mas também entre Governos e Sociedade Civil; operadores tradicionais e prestadores *over-the-top* (OTT); a liberdade individual e a segurança nacional.

Com base em exemplos de outros países da União Europeia, procurámos demonstrar que, a nível nacional, há espaço para aperfeiçoar o modelo organizativo existente em Portugal, através do reforço dos mecanismos de coordenação entre os *stakeholders* interessados, melhorando a eficácia e coordenação da intervenção nacional.

Para finalizar, reflectimos sobre o papel que Portugal pode assumir a nível internacional nesta matéria e estabelecemos aquele que deverá ser o desígnio último do posicionamento de Portugal: evitar a indesejável fragmentação da Internet e contribuir para a procura de soluções de compromisso e o aproximar de posições entre diferentes intervenientes, de diferentes latitudes. No fundo, julgamos que Portugal deverá fazer simplesmente aquilo que melhor sabe fazer.

1. World Economic Forum, Global Agenda Outlook 2013, 2013 [consultado em outubro de 2013].

2. Não existindo tradução óbvia da expressão anglo-saxónica "Internet Governance", o autor opta por usar uma expressão frequente nos textos em Português: "Governação da Internet".

3. Declaração consensual emanada da World Summit on Information Society (WSIS), e adotada em novembro de 2005, em Tunis, Tunísia. Mais detalhes no capítulo III do presente artigo.

4. Tunis Agenda for the Information Society, 2005 [consultado em outubro de 2013].

5. "Internet Regulation – A Digital Cold War?",The Economist, 14 dezembro de 2012 [consultado em dezembro de 2012].

6. Prestadores de serviço / aplicações acessíveis através da Internet (eg. Google, Facebook e Skype).

7. kapur, 2005.

8. ***When an end user in Kenya sends E-Mail to a correspondent in the USA it is the Kenyan ISP who is bearing the cost of the International connectivity from Kenya to the USA. Conversely when an American end user sends E-Mail to Kenya, it is still the Kenyan ISP who is bearing the cost of the International connectivity, and ultimately the Kenyan end user who bears the brunt bypaying higher subscriptions*** ": Bell, 2002.

9. Mapa com a localização de IXPs no globo [consultado em outubro de 2013].

10. A ETNO é a associação que reúne os operadores incumbentes europeus.

11. Site da WCIT-12. Mais detalhes no capítulo III do presente artigo.

12. A Internet tem vindo sobretudo a funcionar **segundo o princípio** do "best-effort", segundo o qual as informações transmitidas serão entregues no destino caso existam recursos para tal, não existindo absoluta garantia de entrega.

13. Princípio que permite que um determinado nível de qualidade de serviço seja assegurado de ponto-a-ponto.

14. "Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012", 11 de setembro de 2013

15. Olmos & Castro, 2013.

16. Ver Relatório aprovado pelo Comité de Indústria, Investigação e Energia (ITRE) do Parlamento Europeu sobre "Proposal for a regulation of the European Parliament and of the Council laying down measures concerning European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012", 1 de abril 2014.

17. No que respeita ao DNS, o ICANN é responsável pela gestão do conjunto dos domínios alfanuméricos (chamado "Domain Name System" -DNS), funções que passam nomeadamente pela designação dos operadores dos domínios de topo ("top-level domains", TLD). De relevar que os domínios de topo estão agrupados em duas grandes famílias Generic (gTLD. Exemplo: .com ou .net) e country code (ccTLD. Exemplo: .pt). O ICANN é responsável por contratualizar com Registries a coordenação de cada gTLD. No caso dos ccTLD, o ICANN atribui a competência de gestão, registo e manutenção dos domínios a uma entidade em cada país, através de uma delegação técnica.

18. Declaração de Montevideu [consultado em janeiro 2014]

19. Brasil, Rússia, Índia, China e África do Sul

20. https://gac.icann.org/

21. http://www.icann.org/en/groups/board

22. "NTIA Announces Intent to Transition Key Internet Domain Name Functions", 2014 [consultado em março de 2014]

23. ICANN sobre os novos domínios de topo.

24. Kruger, 2013.

25. Kroes, 2013.

26. "Amazon Just Spent Millions Applying For Domain Names. Why?", 2012, Revista Forbes [consultado em outubro de 2013].

27. http://www.iana.org/

28. http://www.ripe.net/

29. Este número contudo não é estático, porque porque na prática a maior parte dos equipamentos estão ligados à Internet através de redes privadas que atribuiem endereços IP de forma dinâmica.

30. Algumas estimativas apontam para que a percentagem de endereços já atribuídos e não utilizados ronde os 30% do total dos endereços IPv4. Ver Asghari, 2012.

31. "Network and Information Security: Proposal for A European Policy Approach", Communication from the Commission to the Council, The European Parliament, the European Economic and Social Committee and the Committee of the Regions, 2001 [consultado em outubro de 2013].

32. Lista de países aderentes da Convenção de Budapeste [consultado em novembro de 2013].

33. "Surveillance: the hot topic at Internet Governance Forum", 2013, Talking New Media [consultado em outubro de 2013].

34. Rousseff, 2013.

35. A Presidente do Brasil pretende ainda aprovar um novo pacote legislativo, o designado "Marco Civil", o qual deverá estipular que "o armazenamento de dados de personalidades físicas ou jurídicas brasileiras por parte de fornecedores de aplicações de Internet que exerçam essa atividade de forma organizada, profissional e com finalidades económicas no país deve ser feito em

território nacional", significando isto, caso esta redação seja aprovada, que OTTs globais como o Facebook ou Google terão de armazenar os dados que dispõem sobre cidadãos ou organizações brasileiras em território brasileiro.

36. Proposta de Resolução conjunta do Brasil e Alemanha, 2013 [consultado em novembro de 2013].

37. Commission proposes a comprehensive reform of the data protection rules, 25 janeiro 2012 [consultado em setembro de 2013].

38. R2013.

39. Conclusões do Conselho Europeu de 24 a 25 de outubro de 2013 [consultado em outubro de 2013].

40. Internet Society.

41. Portugal Chapter.

42. Atos Finais da WCIT-12 [consultado em janeiro 2013].

43. Princípios para a Política para a Internet, 2011, OECD [consultado em abril de 2013].

44. «Rede de comunicações eletrónicas» são definidas na Lei n.º 5/2004, de 10 de fevereiro, como "os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos, nomeadamente elementos de rede que não se encontrem activos, que permitem o envio de sinais por cabo, meios radioeléctricos, meios ópticos, ou por outros meios electromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes de radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida" (sublinhado nosso).

45. Decreto-Lei n.º 55/2013, de 17 de abril [consultado em outubro de 2013].

46. Associação DNS [consultado em outubro de 2013].

47. Ver art. 21.º do Decreto-Lei n.º 55/2013, de 17 de abril.

48. Fundação para a Ciência e a Tecnologia, IP [consultado em outubro de 2013].

49. Gabinete Cibercrime da Procuradoria Geral da República [consultado em novembro de 2013].

50. Projecto InternetSegura.

51. "Country reports", 2011, European Union Agency for Network and Information Security (ENISA) [consultado em outubro de 2013].

52. Relatório Anual da BIPT, 2012 [consultado em outubro de 2013].

53. La Rue 2011.

54. UIT Stats [consultado em outubro de 2013].

55. Internet World Stats [consultado em outubro de 2013].

Bibliografia

Asghari, Hadi
2012 "Thirty percent of IPv4 space is still unused", Delft University of Technology.

Bell, Richard
2002 "The Halfway Proposition - Background Paper on Reverse Subsidy of G8 Countries by African ISPs,".

Kapur, Akash
2005 "Internet Governance: A primer", New Delhi: United Nations Development Programme–Asia-Pacific Development Information Programme (UNDP-APDIP) [consultado em outubro de 2013].

Kroes, Nellie
2013 Carta da Vice-Presidente da Comissão Europeia a Fadi Chehadé, Presidente e CEO do ICANN [consultado em outubro de 2013].

Kruger, Lennard
2013 "Internet Governance and the Domain Name System: issues for Congress".

La Rue, Frank
2011 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", UN General Assembly, Human Rights Council [consultado em novembro de 2013].

Olmos, Ana & Castro, Jorge
2013 OpenForum Academy, "Net Neutrality in the EU – Country Factsheets" [consultado em outubro de 2013].

Reding, Viviane
2013 "Data protection reform: restoring trust and building the digital single market", 4th Annual European Data Protection Conference [consultado em setembro de 2013].

Rousseff, Dilma
2013 Discurso na 68.ª Assembleia Geral das Nações Unidas [consultado em setembro de 2013].

?

Sabia que

A Wikipedia em cebuano é a segunda versão com mais artigos logo após a inglesa. A língua conhecida por 16,5 milhões de filipinos, tem apenas seis administradores e 14 utilizadores activos. A maior parte dos artigos (24 milhões em 29,5 milhões) é escrito pelo bot "Lsjbot", criado pelo físico sueco Sverker Johansson.

Onde descansam os dados

Os **centro de dados** ou "datacenters" são o receptáculo físico dos dados da Internet, onde estes são guardados de forma segura e geridos para processamento pelos clientes, seja para oferecerem soluções de cloud computing, gestão de jogos com milhões de jogadores em simultâneo ou testes de novas aplicações ou serviços. Para os utilizadores finais, de forma simples, é onde estão armazenadas as fotografias ou as músicas de serviços como o Flickr ou o Spotify, respectivamente.

Os centros de dados podem ser uns estranhos locais, instalados em condições muito específicas em igrejas como em abrigos nucleares.

Covilhã, Portugal

O "datacenter" da Altice foi idealizado para a Covilhã por, entre outras facilidades, estar afastado das placas tectónicas do litoral.

A escolha do local passou pela "segurança, acessibilidades, custos e sustentabilidade", a que se juntou o reduzido risco de sismos ou outras catástrofes naturais, o bom acesso a infra-estruturas de comunicações, energia e transportes, condições ambientais e interligação à universidade da Beira Interior, garantindo a criação de empregos locais, assegura a operadora.

O maior centro de dados em Portugal, obra do arquiteto Carrilho da Graça, foi concebido para ter uma elevada capacidade de poupança energética, apesar de poder ligar até 50 mil servidores à rede de fibra óptica da empresa.

Fort Pierce, EUA

A Data Shelter usou um antigo abrigo central ataques nucleares, construído em 1964 pela operadora AT&T e pelo U.S. Department of Defense. Localizado em Fort Pierce, no estado norte-americano da Florida, integra um sistema próprio de geração energética concebido para as comunicações militares e deve entrar em funcionamento ainda este ano.

Pólo Sul

Com uma temperatura média de 51,6°C negativos para valores máximos de 31,2°C negativos, foi assim que uma equipa de investigadores viveu em Maio de 2009 no Pólo Sul.

A equipa do IceCube Neutrino Observatory, um detector de partículas tapado por 2,5 quilómetros de gelo, recolheu uma enorme quantidade de dados na missão científica. Para os processar e armazenar, necessitou de centenas de núcleos de computação e de espaço de armazenamento de vários petabytes – para gerir diariamente a recolha média de um terabyte de dados.

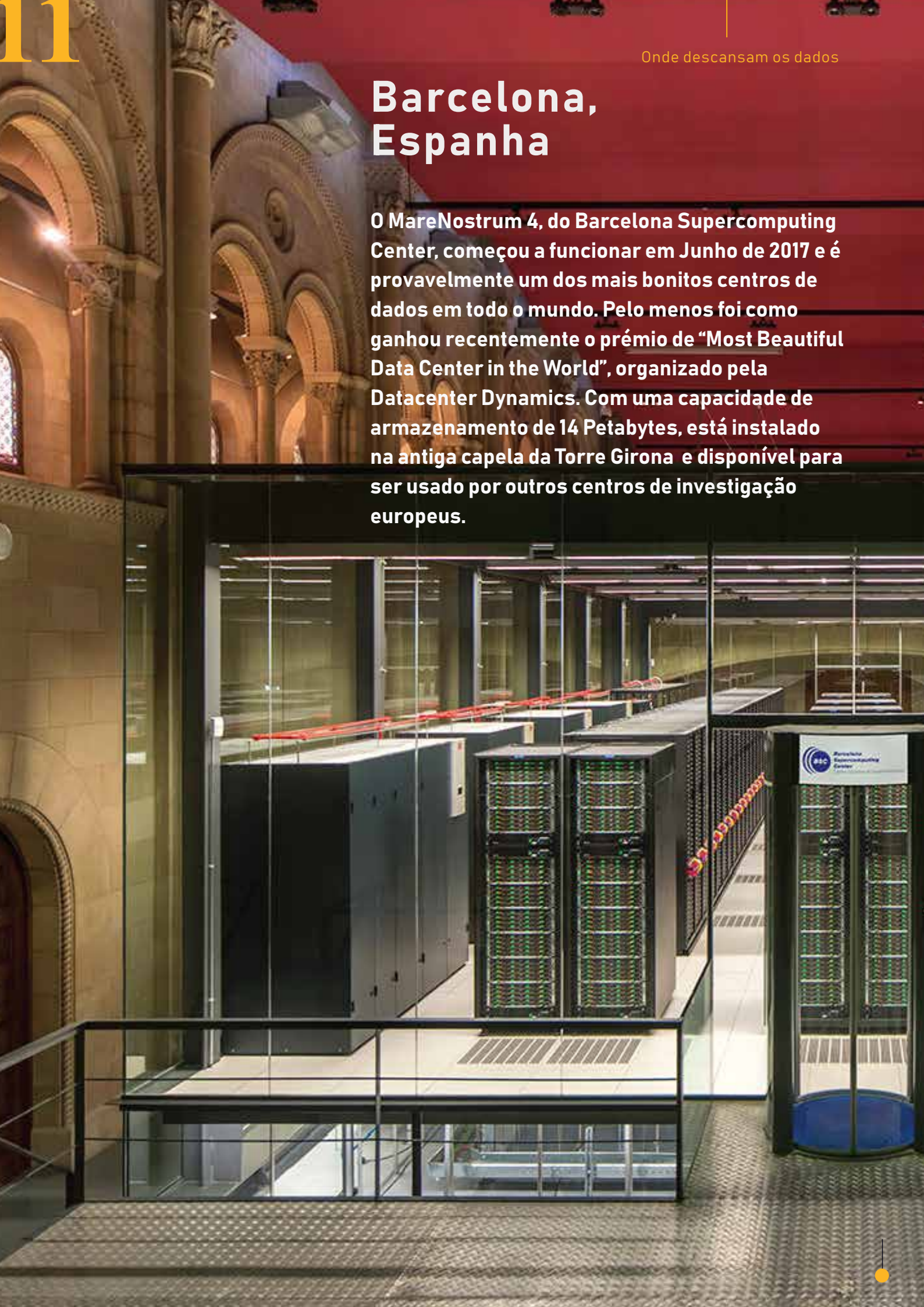
Esses dados eram depois transmitidos a outros centros de investigação e uma cópia enviada para o centro de investigação em física das partículas DESY Zeuthen, na Alemanha.

Estação Espacial Internacional

O centro de dados que mais alto se elevou foi o Spaceborne Computer, da HPE. Após 615 dias na Estação Espacial Internacional o computador regressou à Terra a 3 de Junho de 2019. O seu lançamento num foguetão da SpaceX levou-o a atingir velocidades de 30 mil quilómetros por hora. O objectivo da missão informática era investigar a supercomputação a longo prazo (o equipamento assegurou processamentos de 1 teraflop por segundo), a resiliência perante as fortes forças gravitacionais, o impacto das radiações ou o potencial para o erro humano nestas situações extremas.

Barcelona, Espanha

O MareNostrum 4, do Barcelona Supercomputing Center, começou a funcionar em Junho de 2017 e é provavelmente um dos mais bonitos centros de dados em todo o mundo. Pelo menos foi como ganhou recentemente o prémio de "Most Beautiful Data Center in the World", organizado pela Datacenter Dynamics. Com uma capacidade de armazenamento de 14 Petabytes, está instalado na antiga capela da Torre Girona e disponível para ser usado por outros centros de investigação europeus.



?

Sabia que

Facebook, Microsoft, Google e Amazon activaram 15 novos centros de dados no ano passado, estando mais de 20 preparados para funcionar nos próximos anos.

TeleGeography

Orkney, Escócia

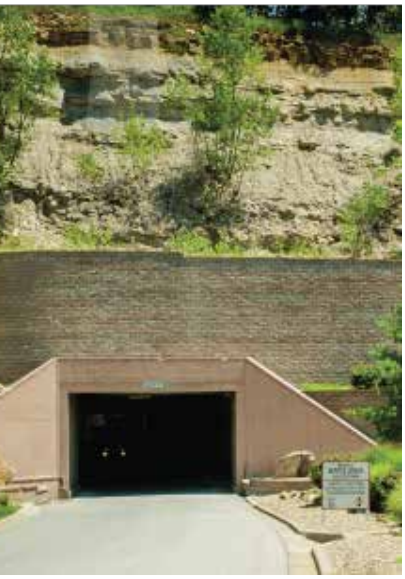
A Microsoft está a apostar em centro de dados submersos. No futuro serão assim: localizados perto da costa, para servir os utilizadores com uma menor latência no acesso e transmissão de dados, e rápidos a construir, assegura o CEO da empresa, Satya Nadella. O Project Natick foi anunciado em Julho de 2014. Um ano depois foi lançado um protótipo nas águas do Pacífico, junto à Califórnia, que serviu para demonstrar a possibilidade de desenvolvimento, incluindo a eficácia de arrefecimento da temperatura dos diferentes módulos. Ao largo da Escócia, nas ilhas Orkney, a fase 2 procura determinar a praticabilidade logística, económica e ambiental. O projecto é criticado por usar os oceanos para arrefecer a sua estrutura quando há preocupações ambientais com o aumento da temperatura do mar.

Udomlya, Rússia

Anunciado em 2015 e terminado em Julho de 2019, o fornecedor russo de serviços digitais Rostelecom aliou-se à empresa de energia nuclear Rosenergoatom para as operações comerciais do centro de dados de Udomlya, integrado nas instalações da existente central nuclear de Kalininskaya. A razão da proximidade visa garantir o fornecimento energético. Os equipamentos não vão sofrer com as radiações, garantem os responsáveis.

Moses Lake, EUA

Após serem desactivadas das suas funções, as instalações militares geram interesse para o uso civil como centros de dados. Um exemplo disso é a instalação da CenturyLink em Moses Lake, no estado de Washington (EUA), num antigo centro de comando e controlo do programa de mísseis de defesa Titan. O North American Air Defense Command Direction Center funcionou entre 1958 e 1963 e está preparado para assegurar o seu funcionamento mesmo se atingido por uma bomba de 10 megatoneladas, garante a operadora. O local tem uma reduzida actividade sísmica e 85% das suas necessidades energéticas são asseguradas pelas barragens hidro-eléctricas do pouco distante rio Columbia.



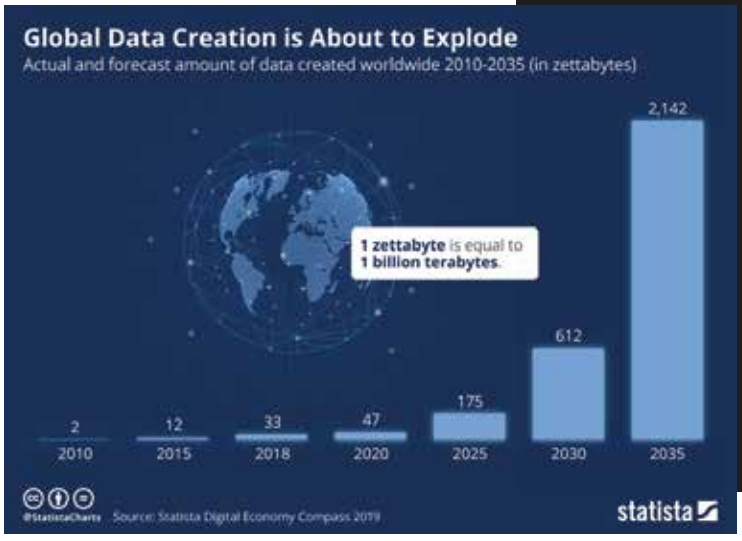
Kansas City, EUA

Instalados a 12 quilómetros de profundidade, os dados nas instalações da Cavern Technologies são provavelmente os que estão enterrados a uma maior profundidade.

Em Kansas City (EUA), enormes formações naturais de cal servem para este centro de dados ficar protegido de desastres naturais ou deliberados, enquanto a entrada humana é bastante restrita.
Outros benefícios dos centros de dados subterrâneos passam, segundo a empresa, pela garantia de maior estabilidade da temperatura e por um menor custo na construção destas instalações.

Marselha, França

O novo centro de dados da empresa holandesa Interxion será localizado como os dois anteriores junto ao porto de Marselha mas este MRS3 tem uma especificidade: está a ser instalado numa antiga base de submarinos cuja construção foi iniciada pelos alemães na II Guerra Mundial mas nunca terminada ou usada durante a ocupação da cidade, entre 1942 e 1944.
A sua localização é estratégica, com acessibilidade a cabos terrestres e submarinos que ligam a cidade francesa à Europa, Médio Oriente e Ásia.
Quatro anos após adquirir o primeiro datacenter, a empresa anunciou em Maio de 2018 o MRS2. Esta terceira será na antiga zona militar, ainda protegida e vigiada pelas autoridades.



Sabia que

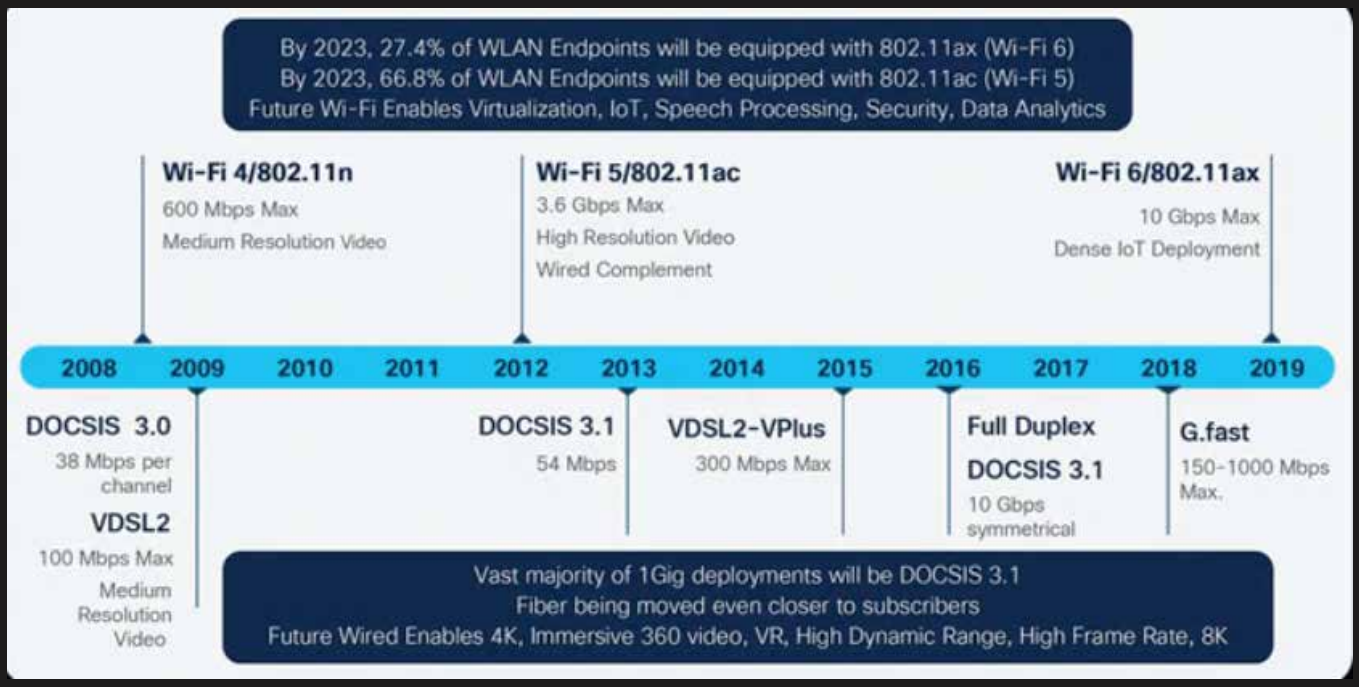
Os dados vão crescer de uma estimativa de 47 zettabytes (ZB ou Zebibyte) este ano para 2.142 ZB em 2035.

tictank.pt

?

Sabia que

Evolução histórica das tecnologias de comunicações com e sem fios



Cisco