O local de toda *a (in)segurança*

Privacidade e Internet são duas palavras que não combinam. A cada nova utilização, são deixadas 'pegadas' que são facilmente 'capturadas' por diversas entidades. A boa notícia é que, mesmo sendo virtualmente impossível eliminar todos os riscos, **há práticas que podem tornar a navegação *online* muito mais segura.**

por **Susana Torrão**

Um estudo da universidade de Vanderbilt revelado este ano mostra que é impossível escapar à recolha de dados pessoais por parte da Google. Segundo a investigação, um telemóvel, mesmo sem ser utilizado, envia a sua localização à empresa 240 vezes durante um período de 24 horas. De acordo com o engenheiro informático autor da pesquisa, a empresa usa várias formas de aceder e armazenar os dados, do motor de busca ao sistema operacional móvel, passando pelo Gmail ou o Youtube. Assim, movimentos *online*, viagens diárias, compras ou preferências culturais ficam armazenados, permitindo à empresa identificar os interesses do utilizador de forma eficaz. E, embora a Google tenha refutado o estudo, afirmando que parte das conclusões podem ser enganosas, a verdade é que, no passado, a empresa já assumiu que usa este tipo de informação para melhorar os serviços e tornar os resultados das pesquisas mais relevantes. Entretanto, já em setembro, veio a nu a história do *hacker* que roubou os *e-mails* secretos do Sport Lisboa e Benfica, num caso que agitou o mundo do futebol nacional. Embora de natureza diversa, estes são exemplos do quão difícil é manter a segurança *online*.

Estar online *implica o mesmo risco que passear na rua:* **por muitos cuidados que se tomem,** *por vezes, os azares acontecem*

Uso pessoal... ou nem tanto

Bruno Castro, fundador e CEO da empresa de segurança informática VisionWare, é perentório quando questionado se é possível manter a privacidade *online*. "Diria que não. Apesar de cada vez mais existir uma noção generalizada da 'insegurança' que existe no mundo cibernauta, ainda continua a haver dúvidas relativamente ao tema privacidade", afirma o especialista para quem estar *online* implica o mesmo risco que passear na rua: por muitos cuidados que se tomem, por vezes, "os azares acontecem". "Existem ferramentas e formas de aumentar o nosso nível de segurança quando estamos *online*, no entanto, a segurança ainda assim não é garantida", afirma Bruno Castro para quem este é um risco que deve ser assumido de cada vez que se navega na Internet, se publicam artigos nas redes sociais ou se realizam compras *online*.

Relato de uma vida à distância de um clique

"Se não ativarmos a navegação anónima e não tivermos o cuidado constante de limpar os *cookies*, qualquer pessoa pode fazer o *tracking* dos *sites* onde estivemos, quanto tempo estivemos, que clique fi-

GETTY IMAGES

A saber:

Alguns conceitos e ferramentas que garantem uma maior privacidade online

VPN – É o acrónimo para Rede Privada Virtual (***Virtual Private Net***), que permite a criação de um canal de comunicação seguro, em que a informação transmitida é cifrada, sendo transportada 'em cima' de uma rede pública. Ideal em situações em que o acesso é feito a partir de locais públicos.

PROXY – É uma boa solução para omitir a identidade em tarefas simples. Funciona como uma espécie de intermediário entre o computador e a Internet: todos os pedidos – páginas ou ficheiros, por exemplo, – são feitos pelo ***Proxy*** que depois os devolve ao cliente. Neste caso, o endereço IP não passa além do ***Proxy***. Mas as comunicações com o ***Proxy*** não são cifradas.

NAVEGAÇÃO ANÓNIMA – Ao utilizar um modo de navegação anónimo, o Chrome não grava o histórico da navegação, bem como os dados dos *sites* ou dados introduzidos nos formulários. Contudo, a atividade não é ocultada dos *sites* que visitar ou do fornecedor de serviços Internet. Para realizar uma navegação privada, pode usar os atalhos Ctrl + Shift + n (para Windows, Linux ou SO Chrome) ou maçã + Shift + n num Mac.

FONTE: GOOGLE SUPPORT

zemos, de onde viemos e para onde vamos", alerta Elsa Veloso, CEO da DPO Consulting, consultora especializada em proteção de dados.

A chamada 'pegada digital' pode ser seguida por quem tenha os conhecimentos necessários e usa vários instrumentos para fazer *profiling*. Este e a utilização dos *cookies* de cada sessão são, aliás, funcionalidades que, de acordo com Bruno Castro, a maioria dos *sites* tenta angariar e reutilizar em benefício próprio. "Apesar de o novo regulamento de proteção de dados vir limitar e condicionar a angariação e tratamento dos dados, ainda existe uma utilização genericamente abusiva desta informação, o que permite que os servidores (e respetivos *sites*) possam condicionar a nossa visita de acordo com a experiência passada e, teoricamente, com os nossos gostos pessoais", afirma Bruno Castro, para quem esta é uma área que requer maior exigência e controlo.

"A evolução da própria regulamentação veio permitir limitar alguma da informação angariada na maioria dos *sites* – comércio, *e-banking*, redes sociais –, contudo, existe sempre a possibilidade de angariar informação de forma ilegítima para fins maliciosos. O cuidado terá de ser sempre do lado humano", alerta Bruno Castro, que sublinha ainda que as novas tecnologias permitem minimizar o rasto que deixamos enquanto internautas. "Contudo, nada é completamente garantido no mundo da segurança cibernauta", diz.

Tendo em conta este cenário, há que pensar duas vezes antes de divulgar muita informação na Internet. "Os nossos dados pessoais são valiosos e temos de interiorizar o valor dessa informação e do risco que existe em dispersar informação desnecessária no mundo cibernauta, já que não existe garantia que seja utilizada adequadamente", alerta Bruno Castro.

E, se é verdade que o atual Regulamento de Proteção de Dados (ver caixa *Jogar com novas regras* na página 142) estabelece regras para a angariação e processamento dos dados pessoais, também é necessário ter em conta que a segurança dos mesmos depende em grande parte do conhecimento e da atenção de cada utilizador.

No mundo cibernauta, **não existe o conceito de apagamento definitivo.** *Mesmo que apague uma imagem das suas redes sociais, não sabe quem já fez* download

Isto porque, no mundo virtual, as formas de processar os dados multiplicam-se. "Entre o 'controlo', ou processamento legítimo, existem vários negócios que vivem de compra e venda de informação sobre pessoas. Portanto, o processo passa essencialmente pela segurança dos nossos dados, pela sua dispersão ou angariação proativa, na compra e venda dos referidos dados e, por fim, na reutilização dessa informação para outros fins pelos quais não era suposto serem utilizados ou sequer temos conhecimento dessa reutilização", lembra Bruno Castro.

Uma vez na Internet, para sempre na Internet

Neste contexto, a eficiência do ato de 'apagar' qualquer informação – seja uma fotografia numa rede social ou uma simples mensagem de *e-mail* – torna-se duvidosa. "É caso para reforçar a expressão de que 'uma vez na Internet, para sempre na Internet'. É especulativo dizer perentoriamente que sim ou que não, contudo, no meu entender, diria que não existe o conceito de apagamento definitivo no mundo cibernauta", diz Bruno Castro. Elsa Veloso exemplifica: "Se apagar uma imagem que esteve um dia, uma semana ou um mês *online,* isso não quer dizer que a retire de todos os sítios para onde ela já se expandiu. Quando faço eco, não posso voltar atrás com a palavra dita, da mesma forma que, com uma imagem, não posso ir ao computador de todas as pessoas que fizeram um 'gosto', copiaram ou fizeram *download* e eliminá-la", explica a CEO da DPO Consulting.

Também ao nível das mensagens, a segurança é relativa. Para Bruno Castro, tudo vai depender da plataforma de comunicação usada. No caso do correio eletrónico, entre serviços *cloud* distintos – por exemplo, Microsoft Office365 para Gmail –, o conteúdo é transmitido pela Internet entre os servidores dos respetivos *providers* (Microsoft e Google), que, na opinião do especialista "devem merecer (ou não) a nossa confiança na utilização adequada dos nossos dados". Já no caso de aplicações como o Whatsapp, *chat* do Snapchat, do Instagram ou Mes-

Regras para uma navegação mais segura

Há uma série de normas e procedimentos que devem ser adotados diariamente. Fique a conhecer alguns.

- **Ter a certeza de que navega de modo anónimo.**
- **Ter antivírus no computador.**
- **Proceder à atualização regular de sistemas e aplicações.**
- **Mudar regularmente a *password* sem a partilhar. Garantir ainda que aquela tem uma complexidade de pelo menos 13 caracteres com alfanuméricos e caracteres especiais.**
- **Não deixar o computador aberto em espaços públicos ou no local de trabalho, mesmo durante pequenas ausências.**
- **Usar navegadores *Web* como o Firefox ou o Google Chrome, que começou a bloquear certos anúncios e *cookies*.**
- **Evitar *sites* inseguros.**
- **Desativar a localização nas opções do *browser* do seu computador.**
- **Usar *plugins* para bloquear *trackers*, impedindo que os *cookies* funcionem quando visitar um *site*.**
- **Usar VPN, que possibilita a criação de um canal de comunicação seguro.**

FONTE: BRUNO CASTRO, CEO DA VISIONWARE, E ELSA VELOSOM, CEO DA DPO CONSULTING

senger do Facebook, não existe ligação entre servidores de diferentes *providers*, mas uma conexão direta dos dispositivos finais (*smartphone* ou computador) ao servidor do provedor do serviço. "No caso do Whatsapp, que utiliza um modelo de criptografia bastante avançado, possui a chamada *end to end encryption,* o que faz com que exista uma pseudogarantia de confidencialidade do conteúdo das mensagens trocadas por essa plataforma às quais nem a própria empresa conseguiria aceder. Inclusive, este nível de segurança já colocou a plataforma de *chat* debaixo de fogo em alguns Estados", explica Bruno Castro.

Já Elsa Veloso é mais crítica em relação a este tema. "Só há uma forma de fazer mensagens completamente seguras, que são as mensagens encriptadas com *one time password*, com o tamanho do texto e que só é usada uma vez", diz a responsável da DPO Consulting, para quem todas as outras mensagens são suscetíveis de ser truncadas, intercetadas ou adulteradas. Contudo, na prática, usam-se comunicações encriptadas. "A encriptação pode ser simétrica ou assimétrica. Se for simétrica, o emissor e o recetor têm a mesma *password*; se for assimétrica, as *passwords* são diferentes", explica Elsa Veloso, que alerta para os riscos que, mesmo assim, existem. "Não posso garantir que um telefonema não está a ser escutado, que a infraestrutura não foi corrompida, que não entrou um *hacker* no meu computador e acedeu às mensagens. No fundo, só pequenas coisas podem ser garantidas", diz a especialista.

Como explica Elsa Veloso, a segurança da informação é uma questão de resiliência. Os sistemas de segurança de informação *standard* são baseados no modelo CIA (*Confidentiality, Integrity, Avalability*), que garante a confidencialidade, integridade e disponibilidade da informação. "Quando temos de construir um sistema de resiliência – que tem de garantir a resiliência das infraestruturas, dos *softwares* e dos sistemas, e assegurar que as pessoas envolvidas têm todos os conhecimentos necessários –, temos também de garantir que todo este sistema é resiliente e é resistente. E isso vai depender do grau de maturidade da organização, para

O Whatsapp utiliza um modelo de criptografia avançado, que faz com que exista uma pseudo garantia de confidencialidade

GETTY IMAGES

o que está preparada, o que quer fazer e quais os níveis que quer atingir", afirma a especialista em proteção de dados.

Nas nuvens...

Hoje, muita da informação de particulares e empresas está armazenada em *clouds*, supostamente para uma maior segurança. Contudo, também este sistema tem falhas. "As nuvens não existem – este é apenas um nome bonito dado a infraestruturas físicas redundantes", afirma Elsa Veloso. O Regulamento Geral de Proteção de Dados obriga a que esta redundância seja feita dentro da Europa, ou seja, a mesma informação está duplicada em infraestruturas em Portugal, na Holanda e na Alemanha, por exemplo. Mas, além de redundante, o armazenamento na *cloud* tem de ser resiliente, característica que lhe é dada pelos *backups*, *firewalls*, antivírus e sistemas de autonomia energética utilizados. "As *clouds* são infraestruturas físicas e terrenas que dão a garantia de que a informação que lá está armazenada é protegida. Mas se a NATO e o sistema Visa podem ser atacados, nada impede que uma *cloud* não o seja. Tudo é atacável. O tempo que o sistema resiste vai depender do nível de resiliência", sublinha Elsa Veloso.

Também Bruno Castro aponta o facto de as *clouds* continuarem a ser "servidores clássicos que disponibilizam espaço para alojamento e tratamento de ficheiros a utilizadores remotamente". "Apesar de ainda não existir essa impressão generalizada, a segurança das *clouds* – independentemente do *provider* – depende exclusivamente do proprietário da *cloud*. Assumir que o serviço de *cloud* é seguro é estar a assumir que o nível de segurança dos *providers* de *clouds* cumprem os níveis adequados de segurança", afirma.

"As clouds são estruturas físicas que dão a garantia que a informação que lá está é protegida. **Mas se a NATO e o sistema Visa podem ser atacados,** *nada impede que uma cloud não o seja"*

Higiene e segurança na Internet

Ainda assim, há uma série de boas práticas que devem ser seguidas para garantir uma maior segurança *online*. "Tem antivírus? O antivírus é bom? Faz *updates* dos seus sistemas e das suas aplicações com regularidade? Muda a *password* e garante a sua confidencialidade? Deixa o seu computador aberto no local de trabalho quando vai tomar café ou realizar outras atividades?" Estas perguntas são lançadas por Elsa Veloso e refletem alguns dos principais cuidados a ter para garantir um uso mais seguro da Internet. "Há uma série de coisas que são primárias, mas que se forem feitas todos os dias ou com regularidade garantem alguma segurança da informação", afirma a CEO da DPO Consulting.

Para Bruno Castro, a salvaguarda da privacidade *online* deve ser feita do mesmo modo que o é no mundo real. "A maioria dos conceitos de segurança que aplicamos no dia a dia podem replicar-se para o mundo da Internet e, portanto, com alguma inteligência e precaução, devemos seguir os comportamentos de proteção que aplicamos no nosso quotidiano", diz. Ou seja, se nas ruas o bom senso dita que se evitem locais inseguros e não se forneça informação excessiva a um total desconhecido, o mesmo deve ser feito *online*. Regras básicas a que se devem juntar outras, como a de desativar a localização nas opções do *browser*, recorrer a uma ligação VPN (*Virtual Private Net*) ou recorrer a *plugins* para desativar *trackers*. Deste modo, embora continue a ser impossível garantir uma privacidade total, os níveis de segurança aumentam de forma substancial.

JOGAR COM NOVAS REGRAS

Em maio passado, entrou em vigor o novo Regulamento de Proteção de Dados Pessoais. As principais mudanças propostas pela nova lei podem resumir-se em sete pontos: a autorização de transmissão de dados tem de ser inequívoca (até aqui era tácita); a idade mínima para que os menores passam autorizar o tratamento dos seus dados pessoais *online* ficou fixada entre os 13 e os 16 anos, cabendo a cada país definir a idade; qualquer pessoa pode pedir – a qualquer momento – que os dados pessoais recolhidos possam ser apagados pela empresa que os recolheu; o titular dos dados tem o direito de os receber; os sistemas de videovigilância foram limitados e já não podem ser usados na via pública, em zonas de digitação de caixas multibanco e terminais ATM e no interior de áreas reservadas a utentes como casas de banho ou provadores de roupa; a conservação de dados pessoais passa a estar limitada no tempo e, por último, as imagens ou dados pessoais registados no âmbito das relações laborais através de sistemas de vigilância só podem ser usadas no âmbito de um processo penal. Para Bruno Castro, o novo regulamento é "provavelmente, a lei com maior impacto de sempre na indústria digital". "O regulamento veio tornar mais claro e desenvolver melhor o que é necessário desenvolver na proteção de dados pessoais e veio trazer valor a essa mesma proteção. Variáveis como o Encarregado pela Proteção de Dados, o valor elevado das coimas e os registos obrigatórios vieram valorizar a importância dos dados pessoais: Não só para o seu 'dono', mas especialmente para as entidades e empresas que angariam e processos os referidos dados", afirma o CEO da VisionWare, para quem a maior consciencialização dos utilizadores levou a uma maior consciencialização e controlo por parte do público cibernauta em geral. "É óbvio que o regulamento por si só não vai mudar as consciências como uma vacina mágica, mas estou convicto de que irá certamente começar o processo da mudança...", diz.