

A person wearing a dark hoodie is shown in silhouette, looking down at a smartphone held in their hands. The background is a dark blue gradient with faint, glowing lines of digital code or data, suggesting a cyber environment. The overall mood is mysterious and tech-oriented.

A NOSSA IDENTIDADE ESTÁ À VENDA E VALE MAIS DO QUE O PETRÓLEO

SABIA QUE QUANDO CRIA UM REGISTO

NUMA REDE SOCIAL OU ABRE UMA CONTA DE E-MAIL

ESTÁ A PAGAR? NINGUÉM LHE PEDE PARA FAZER

UMA TRANSFERÊNCIA BANCÁRIA, MAS COBRAM-LHE DE OUTRA FORMA.

OS SEUS DADOS PESSOAIS SÃO A MOEDA DE TROCA

NUM NEGÓCIO QUE GERA MILHÕES DE EUROS ÀS GRANDES EMPRESAS DE TECNOLOGIA.

**HÁ QUEM JÁ AFIRME QUE OS DADOS PESSOAIS
SÃO O PETRÓLEO DE SÉCULO XXI.**

A AO PESQUISAR UM QUARTO DE HOTEL para um fim de semana em Londres – sobretudo antes que fique mais difícil entrar no Reino Unido após o divórcio da União Europeia – somos imediatamente inundados com ofertas publicitárias a anunciar restaurantes, empresas de aluguer de automóveis e passeios de barco pelo Tamisa.

Por trás desta aparente coincidência está um contrato assinado pelos utilizadores. Quando criamos uma conta de *e-mail*, fazemos um registo nas redes sociais ou instalamos uma *app* no telemóvel, estamos também a aceitar disponibilizar informações pessoais, como a data de nascimento, o número de telefone ou o próprio *e-mail*. E isso pode ter efeitos secundários que nem imaginamos.

«A generalidade das pessoas afirmam concordar com os termos dos respetivos serviços sem sequer os ler», diz Manuel Masseno, especialista em segurança informática e professor de Direito no Instituto Politécnico de Beja. «Os dados são obtidos através da disponibilização pelos respetivos titulares, isto é, por nós, em redessociais ou outras páginas e nas aplicações.»

«As empresas obtêm os dados de forma direta», acrescenta Luís Antunes, presidente do Departamento de Ciência de Computadores da Faculdade de Ciências da Universidade do Porto. «O utilizador comum tem largas dezenas de *apps* instaladas e cada uma delas recolhe quantidades maciças de dados pessoais, como a georreferenciação, os contactos e a identidade do aparelho.»

A forma como as grandes empresas tecnológicas chegam à nossa informação pessoal está bem patente na política de dados do Facebook. A rede social mais utilizada no mundo é clara neste ponto: «Recolhemos o conteúdo e outras informações que fornecemos quando utilizas os nossos serviços, incluindo quando te registas numa conta, crias ou partilhas e envias mensagens ou comunicas com outras pessoas.»

Mesmo quando não se está ligado diretamente à rede – acontece, por exemplo, quando se faz *login* numa página ou *app* com a conta do Facebook –, a rede de Zuckerberg acede à informação dos utilizadores. «Recebemos informações sobre ti e sobre as tuas atividades dentro e fora do Facebook através de parceiros, como informações de um parceiro quando oferecemos serviços em colaboração», lê-se no Facebook.

Mas a forma como os dados pessoais são disponibilizados não se resume ao que acontece na internet. O preenchimento de um cartão de cliente, introduzindo número de telefone, data de nascimento, *e-mail* e morada é uma das formas de disponibilizar informação pessoal. «Hoje é seguro assumir que todas as nossas interações em papel acabam digitalizadas. As empresas precisam de dados de forma pesquisável, editável e acessível», explica Bruno Castro, CEO da VisionWare, empresa especializada em questões de cibersegurança.

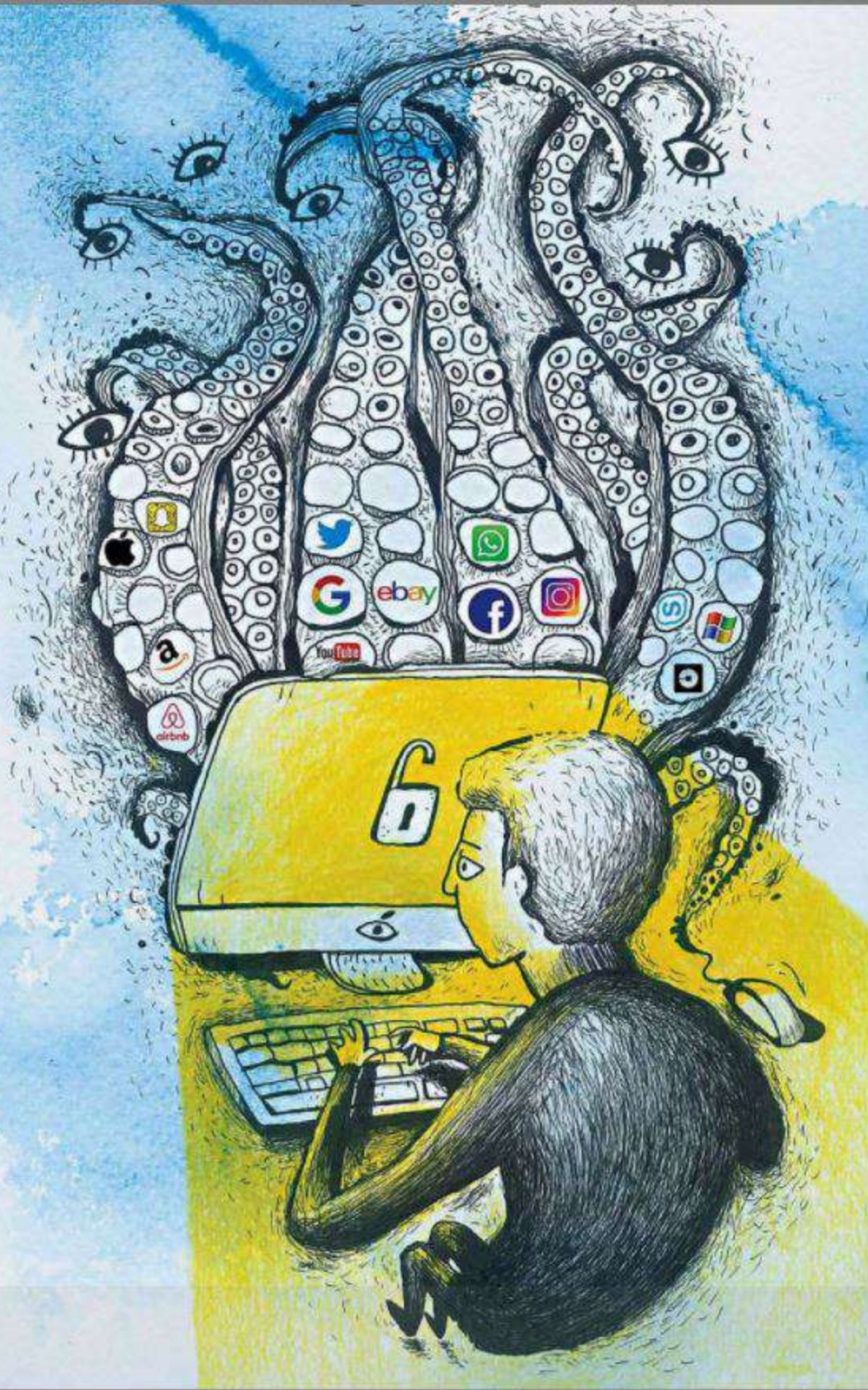
Dessa forma, aos poucos, sem darmos por isso, o volume de dados a circular na internet continua a crescer de uma forma nunca antes vista. E todos nós, utilizadores, contribuimos para isso. Foram criados mais dados nos últimos dois anos do que no resto da história da humanidade. E isto resulta daquilo a que os especialistas chamam de «efeito de rede de dados»: as grandes empresas de tecnologia usam dados para atrair mais utilizadores, que vão criar mais dados, ajudando a melhorar os serviços das companhias... que atraem mais utilizadores, que criam mais dados. Um verdadeiro efeito bola de neve que tem clara expressão nos números apresentados pela *Forbes*.

48

MIL MILHÕES

DE DADOS PESSOAIS FORAM EXPOSTOS DESDE 2013

FONTE: BUSINESS REPORTER



«O UTILIZADOR COMUM TEM DEZENAS DE APPS E CADA UMA DELAS RECOLHE QUANTIDADES MACIVAS DE DADOS PESSOAIS», DIZ LUÍS ANTUNES, PRESIDENTE DO DEPARTAMENTO DE CIÊNCIA DE COMPUTADORES DA FACULDADE DE CIÊNCIAS DA UNIVERSIDADE DO PORTO.

A revista norte-americana estima que em 2020 serão desenvolvidos cerca de 1,7 megabytes de informação por cada ser humano. A cada segundo. E a consultora norte-americana IDC, que presta serviços em inteligência de mercado, defende que em 2025 passaremos a ter cerca de 160 zettabytes de informação armazenada face aos 45 atuais. É um número tão grande que os especialistas em informática tiveram de inventar a fórmula «10 levantado a 21» para simplificar a tentativa de compreender quantos bytes tem um zettabyte: 1 000 000 000 000 000 000 000. É muita informação.

A todo o instante, a cada clique no computador ou dedilhar no *smartphone*, criamos informação. Por segundo, são feitas mais de quarenta mil buscas no Google, o que representa 3,5 milhões de pesquisas diárias. Segundo os dados mais recentes da Marktest, a empresa especializada em sondagens, 96 por cento dos portugueses possuem uma conta ativa no Facebook e cada um de nós gasta, em média, 104 minutos por dia nas redes sociais. Nestas plataformas, são feitas, em média, 2,7 publicações por dia, entre textos, fotografias e partilhas de *links*.

COM TANTA INFORMAÇÃO DISPONÍVEL, a indústria da publicidade é uma das mais ativas no que toca à exploração dos dados pessoais. «A possibilidade de partilha de gostos e hábitos permite depois haver publicidade perfeitamente dirigida ao consumidor e vai até ao ponto em que desenha padrões comportamentais», diz o CEO da VisionWare. E nem é

QUEM ME ANDA A SEGUIR?

Quando visita determinado *site* não é só esse que fica a saber que está lá. Vários *sites* são notificados da sua visita. Assim se percebe porque é que quando procura um telemóvel numa loja *online* de tecnologia é logo bombardeado com milhares de ofertas de outros *sites* sobre esse mesmo telemóvel. O Lightbeam é um *software* que ajuda a perceber quais os *sites* que estão a seguir o que faz na internet.

17
MEGABYTES
DE INFORMAÇÃO DESENVOLVIDOS POR CADA SER HUMANO EM 2020. A CADA SEGUNDO.
ESTIMATIVA FEITA PELA REVISTA FORBES

9246 QUEIXAS DE CIBERCRIMINALIDADE

REGISTADAS EM PORTUGAL EM 2016. EM 1998, OS CRIMES QUE RECORRIAM A FERRAMENTAS ELETRÓNICAS OU INFORMÁTICAS APENAS TOTALIZARAM 158 OCORRÊNCIAS.

FONTE: LUSA

preciso ser bruxo para adivinhar o que sentem as pessoas. Basta ligar uns botões. Uma equipa de cientistas da Universidade de Cambridge colocou um computador a analisar o perfil de mais de 85 mil pessoas. Só com base nos gostos do Facebook, a máquina conseguiu acertar na inclinação política de 85 por cento da amostra e no estado civil de 67 por cento. A possibilidade de traçar perfis apresenta-se como uma das finalidades dadas à informação pessoal que existe armazenada em kilobytes de dados. «Um dos melhores exemplos é o da Google, que vende publicidade direcionada para determinados perfis», diz Luís Antunes.

A SmartLinks é uma agência de *marketing* digital com sede em Lisboa. Além da criação de *sites*, faz a gestão de campanhas publicitárias em plataformas como o Google. «Os dados mais importantes são o *e-mail* e o número de telefone. O mais valioso é a forma como os utilizadores interagem com as peças de comunicação que nos permitem avançar no funil do valor de venda», diz José Peres, um dos sócios da empresa.

Com «os dados disponibilizados pelos clientes ou através de soluções de *marketing* digital», a empresa, que tem mais de oitenta clientes, entre Portugal, Angola, Brasil e França, consegue «criar publicidade que vai diretamente ao encontro dos desejos dos utilizadores».

«O investimento é menor e a eficácia é maior», concorda Tânia Morais, que faz a gestão das redes sociais para a Innov Digital, uma agência de comunicação especializada na área digital, no Porto. No uso dos nossos dados, o maior cego é o que não quer ver. «Nada é feito de forma gratuita. Há sempre uma autorização dada pelos utilizadores. Quando respondemos

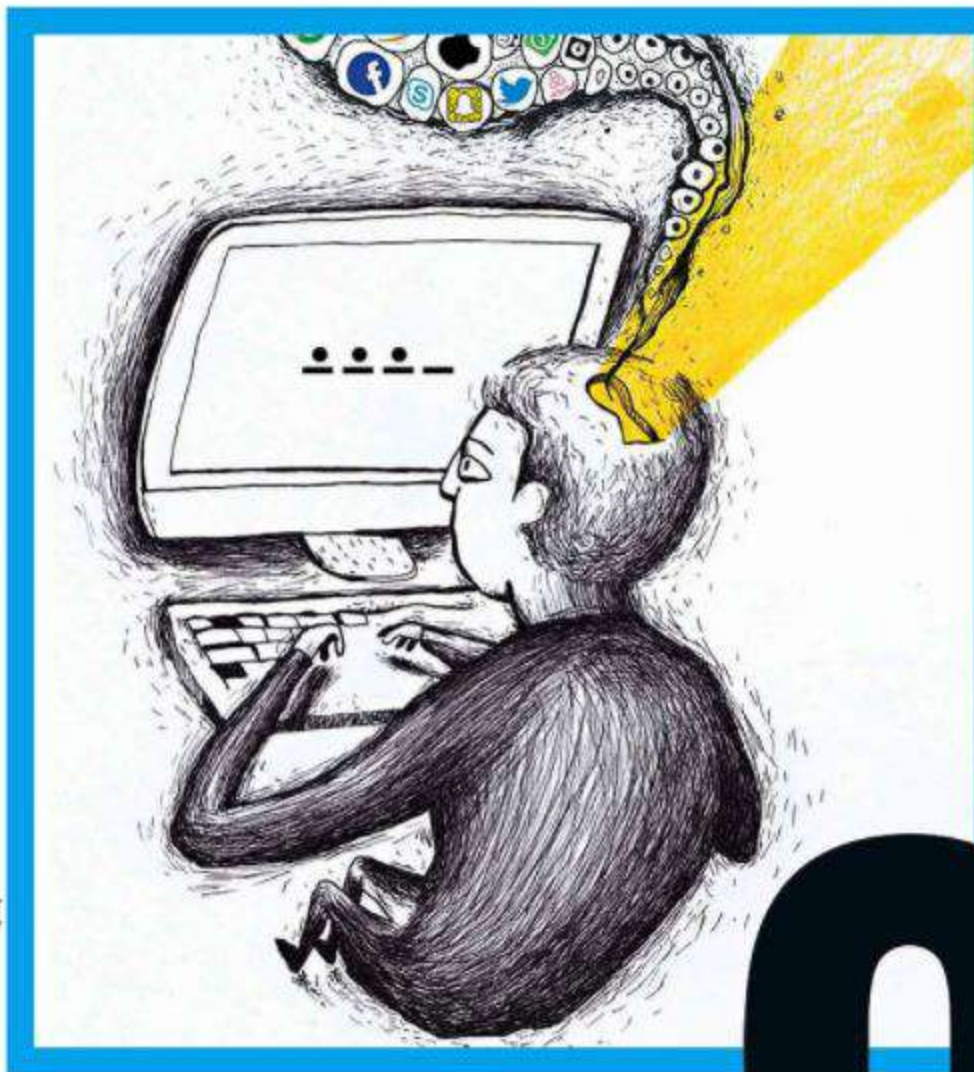
a um questionário no Facebook, ou nos inscrevemos num sorteio, há lá um conjunto de regras.»

Há dez anos, a lista das empresas mais importantes do mundo era dominada pelas petrolíferas. Nos últimos anos, a indústria tecnológica, com a Microsoft e a Google à cabeça, intrometeu-se neste reinado, a ponto de a revista *The Economist* garantir que o recurso mais valioso do mundo já não é o petróleo, mas os dados. E toda a informação disponível em rede constitui o combustível de uma indústria que não para de crescer. «As empresas que mais dinheiro ganham hoje são as que têm os dados no centro dos negócios», diz Joaquín Muñoz Rodríguez, advogado especialista em privacidade, da Sociedade ONTIER, em Madrid.

CONSELHOS PARA UMA NAVEGAÇÃO SEGURA

- Apenas forneça dados pessoais a *sites* seguros. Só os *sites* que tenham cadeado verde são seguros para as compras.
- Limpe a cache e os *cookies* regularmente para que a informação sobre o que faz na internet seja limitada.
- Mude a password com regularidade para evitar que seja copiada e não use a mesma para tudo.
- Nas redes sociais, não exponha tudo o que faz. Dizer que vai de férias pode ser um convite para ladrões que ficam a saber que não vai estar em casa.
- Ninguém o obriga a dar os seus dados. Eles têm valor e dão a ganhar milhões a muito gente. Pense melhor se vale a pena dar o número do telefone ou o *e-mail* para entrar num daqueles sorteios que raramente dão prémios a quem quer que seja.
- Evite a publicação de fotos de menores. Poderá estar a expor os seus filhos a riscos desnecessários.

FORAM CRIADOS MAIS DADOS NOS ÚLTIMOS DOIS ANOS DO QUE NO RESTO DA HISTÓRIA DA HUMANIDADE. AS GRANDES EMPRESAS DE TECNOLOGIA USAM DADOS PARA ATRAIR MAIS UTILIZADORES, QUE VÃO CRIAR MAIS DADOS, AJUDANDO A MELHORAR OS SERVIÇOS DAS COMPANHIAS... QUE ATRAEM MAIS UTILIZADORES, QUE CRIAM MAIS DADOS.



A acumulação de informações pessoais nas mãos das empresas é apenas um dos riscos de quem vive cada vez mais rodeado de supercomputadores prontos para recolher, analisar e partilhar dados. As aplicações fazem recolhas muito mais amplas do que as necessárias para as finalidades a que se propõem e, dessa forma, «os utilizadores correm o risco de ver os dados pessoais copiados e utilizados para finalidades que não aquelas para os quais foram recolhidos», diz Isabel Baírrão, advogada especialista em proteção de dados.

Os nossos dados estão armazenados e podem ser usados pelas empresas que os recebem ou vendidos a outros interessados. Os dados informatizados, «por serem tendencialmente perpétuos e reproduzidos

infinitamente sem custos, são mais perigosos», diz Bruno Castro. Mas, para o CEO da VisionWare, os maiores perigos estão associados «aos casos de extorsão, roubo de identidade, utilização fraudulenta de dados bancários ou de cartão de crédito com objetivos ilícitos».

Com a legislação cada vez mais robusta, as técnicas dos criminosos estão mais evoluídas, sendo mais difícil monitorizar os dados obtidos de forma ilícita. «Assim, há um interesse grande do lado criminal em dados de cartões de crédito ou de identidade, que são muito valiosos», diz o CEO da empresa de cibersegurança.

A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNCT3) está ativa desde novembro de 2016 e dedica-se particularmente a estas

questões. Inspirada no modelo adotado pelo EC3 (European Cybercrime Center) da Europol, os pontos focais deste grupo da Polícia Judiciária são o abuso sexual de crianças através da internet, a fraude com os cartões e outros meios de pagamento eletrónico e virtuais, a criminalidade informática pura e a criminalidade praticada com recurso a meios informáticos. «A vida passou a estar concentrada em plataformas informáticas, sendo, assim, necessário controlar esse espaço», diz Carlos Cabreiro, diretor do UNCT3. «Os smartphones e as redes sociais, pela sua natureza ubíqua, multiplicam os riscos de crime.»

De acordo com aquele responsável, a maior parte dos problemas de segurança informática decorrem de fragilidades humanas - 65 a 70 por cento dos problemas estão relacionados com opções dos próprios utilizadores, como *passwords* pouco seguras ou fornecimento de informação não solicitada. Depois há as falhas técnicas, relacionadas com a violação de sistemas operativos e plataformas. Junta-se a negligência dos utilizadores às fragilidades técnicas e temos o cenário ideal para o cibercrime e apropriação de dados indevida.

COMO FICA A NOSSA PRIVACIDADE nestes tempos de excesso de informação a circular? Numa época em que (quase) todos querem *likes* e partilhas nas redes sociais, passar despercebido na internet é cada vez mais um luxo. Um dos pioneiros nesta luta foi o espanhol Mario Costeja Gonzáles, que entrou com um

RECORDE DE PROCESSOS

A Comissão Nacional de Proteção de Dados (CNPd) compete autorizar tratamento de dados pessoais, garantir o exercício dos direitos dos cidadãos, verificar a licitude dos tratamentos, deliberar sobre acesso a dados pessoais por terceiros e apreciar as queixas dos cidadãos. Em 2016 a CNPD emitiu 16.109 decisões (13.542 autorizações, 2.090 deliberações e 363 projetos de deliberação). E continua a bater recordes no número de processos que analisa: em 2017 foram 21.378.

recurso contra a Google no Tribunal de Justiça (TJ) da União Europeia a exigir que fosse apagada uma informação antiga relativa a um débito perante a Segurança Social do país vizinho. O TJ acabou por reconhecer o pedido do galego e na decisão final ficou estabelecida a responsabilidade da Google em relação ao tratamento de dados dos utilizadores.

Para Joaquín Muñoz Rodríguez, que acompanhou Mario na intensa batalha legal contra o gigante da internet, o caso foi um ponto de viragem. «Antes deste caso não havia qualquer controlo sobre a informação pessoal publicada na internet, mesmo quando era falsa, obsoleta ou destinada a atacar alguém.» Os motores de busca passaram a ser obrigados a colaborar com os cidadãos para remover os *links* que guiam até informações erradas ou falsas sempre que se trate de conteúdos fora da esfera do interesse público.

Ainda assim, e apesar do otimismo inerente à conquista, aquele advogado espanhol desconfia da possibilidade do esquecimento na internet. «É praticamente impossível, tendo em conta a informação que deixamos com a nossa pegada digital.»

A 25 de maio de 2018 entra em vigor em Portugal o Regulamento Geral de Proteção de Dados. As empresas que lidam com dados pessoais passam a estar obrigadas a avaliar previamente o impacto do tratamento

96% DOS PORTUGUESES POSSUEM UMA CONTA ATIVA NO FACEBOOK. CADA UTILIZADOR GASTA, EM MÉDIA, 104 MINUTOS POR DIA NAS REDES SOCIAIS

QUANTO VALEM OS NOSSOS DADOS?

2 EUROS

Um estudo levado a cabo por uma universidade italiana aponta que os utilizadores estão disponíveis para vender o resultado da monitorização do *smartphone* por dois euros.

6,5 EUROS

6,5 euros é quanto paga a Datacoup mensalmente para ter acesso às contas de *social media* de várias pessoas e um pequeno *feed* do extrato do cartão de crédito.

80 EUROS

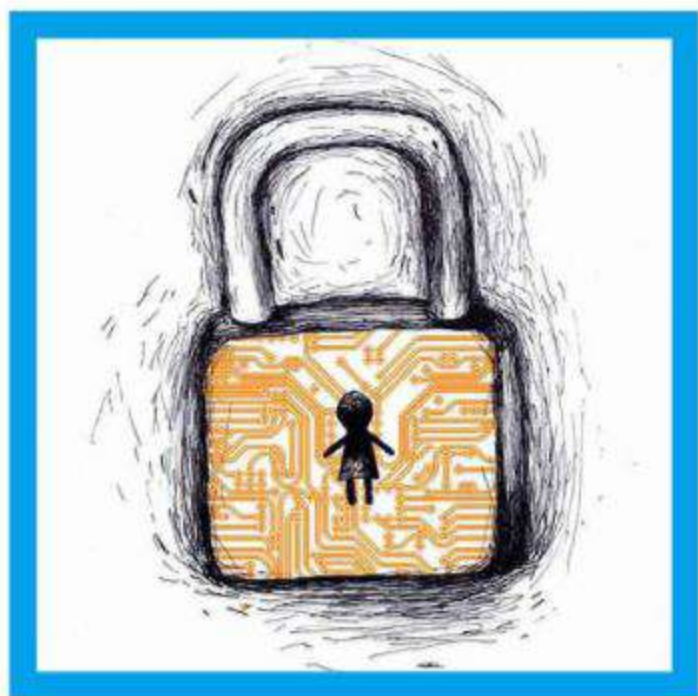
A Luth Research, uma empresa de análise de mercado, cobra 80 euros por mês a mais de 25 mil clientes para analisar a atividade de várias pessoas no *smartphone*, no *tablet* e no computador.

390 EUROS

390 euros foi por quanto Shawn Buckles, um estudante holandês, vendeu os seus dados privados ao The Next Web, que incluíam dados do *browser* e conversação de *e-mail*.

2200 EUROS

Federico Zannier, estudante da Universidade de Nova Iorque, vendeu os seus dados (movimentos do rato e atividade no ecrã) por cerca de 1,6 euros por dia ao Kickstarter, totalizando 2200 euros.



de informação suscetível de afetar o direito dos cidadãos. «São introduzidos novos direitos, como a possibilidade de se apagar dados pessoais ou a portabilidade dos mesmos», diz advogada Isabel Bairrão. Além disso, os cidadãos passam a ter o direito de saber como foi obtida a autorização para a transferência de dados. As empresas que não cumprem as novas obrigações podem incorrer em coimas que chegam aos vinte milhões de euros ou até «quatro por cento da faturação global» da companhia. Os utilizadores passarão a ter um maior controlo sobre o destino da informação pessoal. Isso é um facto. Mas será suficiente?

As empresas portuguesas já começaram a preparar-se para o novo regulamento. O Hospital de Santa Maria no Porto, que lida diariamente com dados de

centenas de utentes, já está na fase final da adaptação e, entre as novas regras, salienta o papel que o encarregado de proteção de dados, uma nova figura jurídica, teve na adaptação ao regulamento. «O facto de ser um colaborador externo garante-nos a total isenção e imparcialidade, minimizando eventuais conflitos de interesse», explica fonte do hospital.

O ENCARREGADO DE PROTEÇÃO DE DADOS é uma das figuras centrais neste novo processo. De acordo com o Regulamento Geral da Proteção de Dados, é obrigatória a figura de um encarregado em organizações que trate dados sensíveis em grande escala como atividade principal. Todos os organismos públicos, com exceção dos tribunais no exercício da sua função jurisdicional, devem ter um. Também as empresas que façam o controlo regular e sistemático dos titulares dos dados têm de criar esta nova posição. Até o Facebook está a mudar: fonte da rede social disse à France-Press que vai pedir aos utilizadores europeus para verificarem as opções de proteção da vida privada disponíveis nas páginas pessoais. No mesmo sentido, a empresa prevê centralizar até ao final do ano todas as regras respeitantes à privacidade «numa página de fácil acesso» para os utilizadores.

A nossa informação pessoal é verdadeiramente valiosa. As empresas de *marketing* estão na linha da frente porque, com dados pessoais de milhares de pessoas, conseguem fazer que as campanhas cheguem mais facilmente ao público-alvo. Os cartões de cliente foram uma das primeiras formas de ter acesso a telefones e moradas. As redes sociais, a par dos motores de busca, são o santo graal numa sociedade cada vez mais digital. E há programas que conseguem observar onde clica e como move o rato. Tudo isto ajuda a traçar um perfil de utilizador. Mas há outros interessados à espreita, com objetivos ainda menos claros e mais perigosos. Os crimes cibernéticos não param de aumentar. Dados de cartões de crédito são ouro para *hackers* que conseguem facilmente desviar dinheiro das contas bancárias. Códigos *pin* pouco seguros podem ser facilmente descobertos dando acesso a documentos privados, que podem parar na internet à vista de todos. ■