



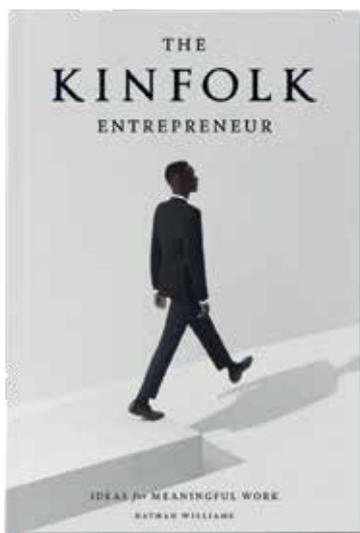
# HOW THE PRIVACY IS CHANGING?



# SUMÁRIO

## 107

Notícias



## 114

Livros

## 115

Eventos

## 108

Intro

Querido, Mudei a Privacidade!



## 110

Entrevista

Magda Cocco, sócia responsável pela área de Comunicações, Proteção de Dados & Tecnologia e Aeroespacial da Vieira de Almeida



## Cibercriminosos fazem-se passar por CEO para atacar

Há uma ameaça à segurança informática a que não podemos ficar indiferentes, alertam os investigadores da Check Point Software Technologies, fornecedor de soluções de cibersegurança.

A ameaça chama-se *Business Email Compromise* (BEC), um tipo de ataque sofisticado dirigido a empresas que realizam transferências eletrónicas. O relatório do FBI sobre delitos na Internet em 2019 afirma que os prejuízos anuais totais gerados pelo BEC atingiu os 1700 milhões de dólares, só nos EUA.

Como funciona o esquema? Aproveitando-se do sistema de teletrabalho, o cibercriminoso faz-se passar por um alto cargo da empresa, CEO ou diretor Financeiro, por exemplo, usando a aparência visual do correio eletrónico corporativo, e pedem aos empregados para usarem uma conta bancária pessoal e fazerem uma transferência de dinheiro.

Uma equipa de investigação da Check Point, que trabalha com governos e empresas a nível mundial, descobriu um grupo de hackers conhecido como The Florentine Banker que lucrou 1,3 milhões de dólares com este tipo de ataques. Durante meses estudaram os correios eletrónicos dos seus alvos, manipulando correspondência, registando domínios semelhantes e copiando a aparência visual das comunicações das vítimas.

## Vanda de Jesus é a nova diretora executiva do Portugal Digital

Conhecedora do mercado das Tecnologias de Informação e Comunicação, tanto em missões de Estado, como na perspetiva empresarial, Vanda de Jesus assume desde junho a liderança de um dos mais importantes projetos do Governo português "para transformar o País". O Portugal Digital é um plano de ação para a capacitação digital das pessoas, transformação digital das empresas e digitalização do Estado.

A executiva deixa assim a direção de Marketing da Microsoft Portugal para abraçar este desafio, semelhante ao que já teve em governos anteriores, junto do falecido Diogo Vasconcelos, quando em 2003 foi gestora de projeto e responsável pela implementação do Programa Nacional de Compras Eletrónicas.



## Cibersegurança preocupa um terço das pequenas empresas em teletrabalho



Durante a pandemia, três em cada cinco colaboradores de pequenas organizações (57%) não recebeu equipamentos das suas entidades empregadoras para trabalhar a partir de casa, segundo um estudo da consultora em cibersegurança Kaspersky, realizado em abril de 2020 em vários países europeus e do continente americano. Contudo, e apesar de muitas pequenas empresas não terem recursos para disponibilizar equipamentos, um terço dos seus colaboradores (34%) indicou que lhes foram dadas informações sobre segurança informática para trabalharem nos seus próprios equipamentos à distância. A preocupação com a segurança informática pode traduzir-se em ter instaladas soluções anti-malware, bem como usar passwords fortes e únicas em dispositivos e routers Wi-Fi.

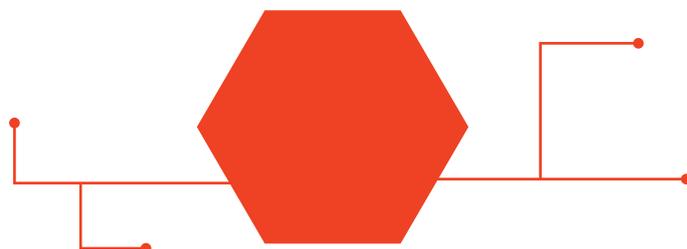
# QUERIDO, MUDEI A PRIVACIDADE!

Os reality shows de "antes e depois" são há muitos anos fenômenos de sucesso, em particular aqueles onde um decorador de interiores transforma uma ou mais divisões de uma casa e no final todos ficam surpreendidos com o resultado. Como por magia, em prazos impossíveis e com recursos limitados, os "antes" tristes e enfadonhos transformam-se em "depois" incríveis, capazes de relançar as vidas dos que lá vivem e de certa forma também dos espectadores que assistem a tais transformações. Se por momentos esquecermos o lado emocional do programa e procurarmos racionalizar um pouco o formato do programa, rapidamente percebemos que existem três fenômenos que contribuem decisivamente para o sucesso da ilusão: 1) o trabalho é realizável por um decorador de interiores por se tratar de uma renovação essencialmente estética; 2) o que é transformado é uma divisão da casa e não a casa como um todo; e 3) os resultados da renovação são apresentados como um ponto de chegada, ou seja, uma fotografia que nos faz ignorar o dia seguinte.

Estes três fenômenos resumem de uma forma geral aquilo que foram os principais desafios enfrentados por muitas Organizações no contexto dos novos requisitos de Privacidade impostos pelo Regulamento Geral de Proteção de Dados (RGPD):

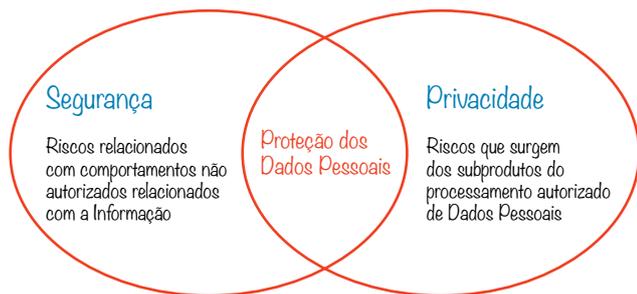
- 1) Acharam que se tratava de um desafio de renovação que poderia ser liderado por especialistas em RGPD sem o envolvimento de especialistas de áreas de privacidade, segurança, gestão, risco ou controlo de Informação e Tecnologias (para referir apenas algumas das competências envolvidas);
- 2) Pensaram que era possível lidar de forma isolada com os "Dados Pessoais", sem que fosse necessário implementar um Sistema de Informação corporativo que colocasse o ativo Informação como elemento central na criação de valor da Organização; e
- 3) Entenderam o dia 25 de maio de 2018 como a meta da corrida RGPD em vez de reconhecerem que se tratava apenas da linha da partida para implementação de uma visão integrada de governança, gestão e operação da Informação e Tecnologias.

No entanto, talvez o principal desafio das Organizações tenha sido procurarem problemas para as soluções e não soluções para os problemas. A motivação central no contexto do RGPD estava relacionado com a evolução da adoção de novas tecnologias digitais (i.e. de 3.ª plataforma e aceleradores de inovação) que potenciaram a aceleração da transformação dos negócios, num fenómeno que ficou conhecido como Transformação Digital. Ora, muitas Organizações ainda se encontram em patamares de Transformação Digital pouco avançados, o que faz com que estejam obrigadas a adotar novas abordagens de proteção de dados pessoais pensadas para a Transformação Digital em ambientes tecnológicos muito semelhantes aos existentes no final dos anos 90. Era, e continua a ser, crítico que as Organizações comecem por reconhecer a necessidade da sua Transformação Digital para que tenham realmente um problema adequado à solução, caso contrário correm o risco de fechar portas por incapacidade de competirem numa economia digital... ainda que continuem 100% em conformidade com o RGPD. Como exemplo ilustrativo veja-se a necessidade das empresas criarem experiências cada vez mais personalizadas aos seus clientes, para que possam ser competitivas numa economia digital, mas em vez disso preferirem "jogar pelo seguro" e apagarem todos os dados relacionados com os seus clientes para "não ter problemas com o RGPD". Adicionalmente, o RGPD aborda de forma integrada o tema da Proteção de Dados, relacionando as dimensões de Privacidade e Segurança da Informação, o que poderá ter gerado alguma confusão e motivado algum aproveitamento. Apesar de existirem fortes vínculos



históricos entre as iniciativas de Privacidade e Segurança da Informação (proteger a confidencialidade dos Dados Pessoais é um dos principais objetivos de ambas os tipos de iniciativas), existem objetivos em ambas as disciplinas que vão além da sua interseção. Enquanto os programas de Segurança da Informação estão sobretudo focados em responder a riscos relacionados com comportamentos não autorizados relacionados com a Informação, os programas de Privacidade estão focados em questões que surgem dos subprodutos do processamento autorizado de Dados Pessoais (Figura 1). Como exemplo, um programa de Segurança da Informação estaria preocupado com a incapacidade dos utilizadores acederem a registos médicos, no entanto essa situação não representaria uma preocupação de Privacidade. Da mesma forma, um programa de Privacidade estaria preocupado em obter o consentimento dos titulares para manter e usar os Dados Pessoais, no entanto a falta desse consentimento não representaria um problema de Segurança da Informação.

Figura 1

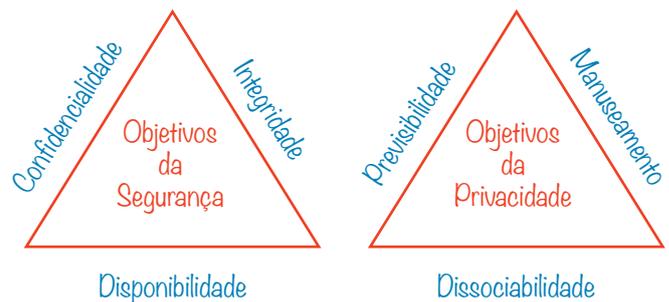


A evolução da Privacidade nas Organizações está a seguir um caminho semelhante ao seguido pela Segurança da Informação há duas décadas. Os esforços iniciais de resposta aos requisitos legais e normativos estão a dar lugar a programas estruturados que entendem os riscos de Privacidade como parte integrante dos riscos corporativos. Os programas de Segurança da Informação passaram por esse mesmo processo evolutivo e atualmente é fácil encontrar normas e boas práticas de Segurança gerais e específicas por setor, permitindo não só a operação da Segurança como a sua governança e gestão integrada num contexto mais abrangente de Informação e Tecnologias. Também na área da Privacidade têm vindo a ser desenvolvidos esforços relacionados com a definição de normas e boas práticas, permitindo cada vez mais acrescentar rigor e método aos programas de Privacidade. Neste contexto, abordagens avulsas ou projetizadas da Privacidade são cada vez menos recomendáveis, sendo necessário subir a parada e "chamar a cavalaria", e no caso concreto a cavalaria pode muito bem ser a Engenharia de Privacidade. A Engenharia de Privacidade adota uma abordagem estruturada para definir objetivos de Privacidade e para os alcançar através de requisitos "by

design" ao nível do planeamento, construção, exploração e monitorização da Informação e Tecnologias. O National Institute of Standards and Technology (NIST) lançou um conjunto de diretrizes para a Engenharia de Privacidade suportadas numa abordagem baseada em risco, propondo que as Organizações desenvolvam os seus programas de Privacidade em torno de três objetivos principais, à imagem do que é feito nos programas de Segurança da Informação com a definição dos objetivos de Confidencialidade, Integridade e Disponibilidade (Figura 2):

- Previsibilidade – Permitir suposições confiáveis das partes interessadas em relação aos Dados Pessoais e ao seu processamento por Tecnologias;
- Manuseamento – Permitir a gestão detalhada dos Dados Pessoais, incluindo alteração, eliminação e divulgação seletiva; e
- Dissociabilidade – Permitir o processamento ou outros eventos relacionados com Dados Pessoais sem associação aos indivíduos ou dispositivos, além do estritamente necessário.

Figura 2



O desenvolvimento de um programa de Engenharia de Privacidade requer uma abordagem "à prova de futuro" dos desafios da Privacidade. Em vez de entenderem a Privacidade puramente motivada por requisitos de conformidade, as Organizações que adotem uma abordagem de Engenharia de Privacidade poderão integrar os objetivos de Privacidade como parte integrante dos objetivos corporativos. ●



**Bruno Horta Soares**  
Leading Executive Advisor na IDC Portugal

# ATÉ ONDE PODEMOS IR QUANDO FALAMOS DE CONTACT TRACING APPS

**C**ontrolar a pandemia e salvaguardar a saúde das populações implica controlar um conjunto de dados que levantam questões sensíveis relacionadas com privacidade e cibersegurança. Já muitos países o fazem, e a Europa procura estar alinhada em termos de soluções a adotar pelos seus países membros. As ferramentas de contact tracing apps estão a ser implementadas, mas convém salvaguardar direitos e garantias dos cidadãos. Magda Cocco é sócia responsável pela área de comunicações, proteção de dados & tecnologia e também responsável pelo setor aeroespacial da Vieira de Almeida que considera ser um "problema para as entidades empregadoras às quais pode faltar alguma certeza jurídica na implementação dos procedimentos adequados de combate à pandemia". A *Líder* falou com Madga e esclareceu muitos dos aspetos que importa serem equacionados no âmbito desta problemática.

**Neste momento, uma questão que nos preocupa a todos é a de saber que soluções tecnológicas podemos implementar para rastrear e controlar a COVID-19?**

A privacidade, no geral, tornou-se uma questão central, no contexto do combate à pandemia, mas não apenas associada a novas soluções tecnológicas (designadamente as contact tracing apps) para rastrear e controlar a COVID-19.

Também surgiram questões no âmbito daqueles que são os limites na recolha e tratamento dos nossos dados pessoais enquanto clientes de determinados espaços (caso da medição de temperatura), enquanto trabalhadores (medição de temperatura, realização de testes ou exames), enquanto turistas (realização de testes e períodos de quarentena obrigatórios), entre outros.

O tema geral será o de perceber até onde se pode restringir a privacidade e proteção de dados com o

objetivo de limitar a propagação da doença. Não se pode afirmar que uma determinada solução tecnológica em abstrato viola as regras de proteção de dados, embora, naturalmente existam soluções tecnológicas que, pela forma como foram desenhadas permitem mais facilmente assegurar o cumprimento das regras relativas à proteção de dados.

**Essas soluções respeitam a privacidade e segurança das pessoas? Em que termos?**

As contact tracing apps (ou qualquer outra solução tecnológica) não são necessariamente compatíveis ou incompatíveis com as nossas normas de proteção de dados, dependerá sempre da sua implementação efetiva. Um dos erros que vemos muitas vezes as empresas a fazer é o de pensar que como utilizam tecnologia X ou Y estão automaticamente a respeitar as regras de proteção de dados, quando cada caso é um caso. O próprio fator humano é muito importante!

Na União Europeia, em particular, tem havido um esforço com vista a garantir que qualquer solução tecnológica é implementada de forma a respeitar a privacidade. Deste modo, já tivemos instruções de entidades como o Comité Europeu de Proteção de Dados e a Comissão Europeia sobre o desenho que deveria ser implementado para garantir, justamente, que estes tipos de soluções sejam construídas de forma a respeitar as regras de proteção de dados.

No geral, as autoridades de controlo dos Estados-membros também têm sido ativas não só ao pronunciar-se relativamente às apps de contact tracing, mas também a outras operações de tratamento de dados que têm sido implementadas no combate à pandemia.

Em Portugal, a Comissão Nacional de Proteção de Dados, apesar de ter começado um pouco mais tarde do que outras autoridades de controlo na União Europeia, já se





pronunciou sobre diversas matérias relacionadas com a pandemia como o teletrabalho, o ensino à distância, a recolha de dados de saúde dos trabalhadores ou a aplicação de controlo da lotação das praias. A Comissão Nacional de Proteção de Dados também se pronunciou sobre a aplicação de contact tracing a ser lançada em Portugal, o que indicia uma preocupação em assegurar a privacidade dos utilizadores.

No entanto, nem tudo é positivo, e na verdade há contradições nas pronúncias entre as diversas autoridades de controlo da União Europeia, e mesmo entre as autoridades de controlo e os respetivos governos dos Estados-membros. Em Portugal, a Comissão Nacional de Proteção de Dados e o Governo parecem ter posições divergentes no que concerne à medição da temperatura dos trabalhadores. Isto é um problema para as entidades empregadoras às quais pode faltar alguma certeza jurídica na implementação dos procedimentos adequados de combate à pandemia, designadamente no contexto do seu plano de contingência.

#### **Os dados recolhidos como são tratados?**

Dependerá muito da implementação específica e da operação de que estamos a falar. No entanto, podem ser tratados dados como a localização, o estado de saúde, o contacto com determinadas pessoas (incluindo infetadas), os dados relativos a deslocações, imagem e voz, entre outros. É um leque de dados amplo e que pelo nível de intrusão que pode originar na esfera dos titulares deve motivar especiais cuidados. Neste sentido, a Cibersegurança impõe-se como um requisito de primeira linha, não queremos um incidente de violação de dados pessoais que coloque

este tipo de dados nas mãos de algum ator malicioso.

#### **Que outros países estão a implementar soluções tecnológicas/digitas para ajudar no combate à pandemia? Quais e como?**

No geral, uma percentagem significativa dos países tem implementado soluções desta índole. Claro que as soluções em específico divergem de país para país (havendo, como referido, um certo fio condutor dentro da União Europeia). Existem também outras soluções tecnológicas utilizadas no combate à pandemia, como aquelas que se dedicam ao controlo efetivo do cumprimento do período de quarentena (exemplo, a Polónia).

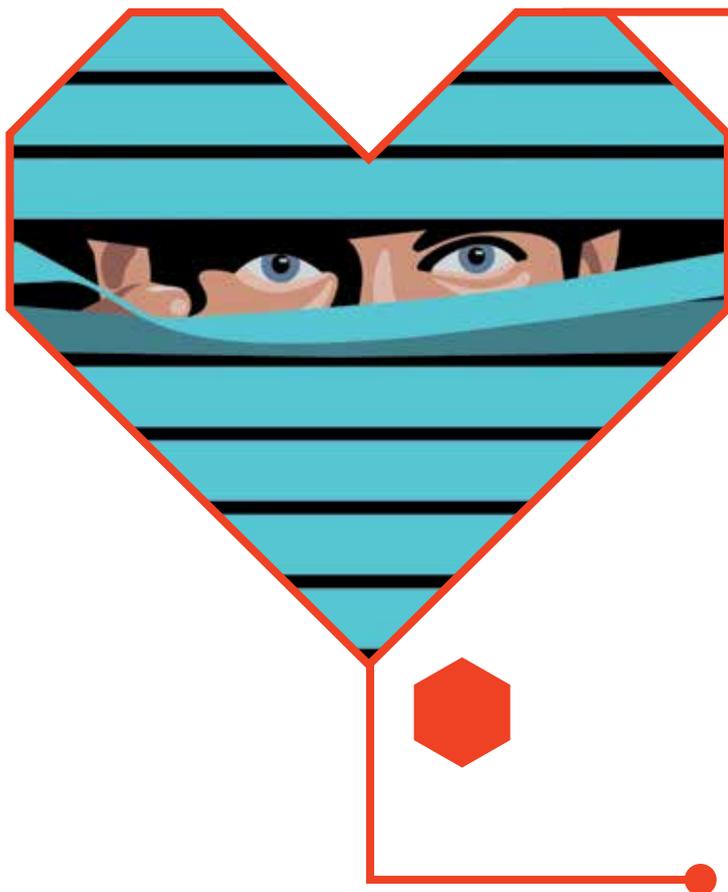
Claro que a implementação vai variar em função da jurisdição, mas há sempre soluções que serão "mais amigas da privacidade". Por exemplo, o tratamento descentralizado tenderá a ser mais aceitável de um ponto de vista da privacidade que o centralizado, a utilização de dados de proximidade (através, por exemplo, de Bluetooth Low Energy) é menos intrusiva do que a utilização de dados de localização (GPS), uma aplicação de utilização voluntária será mais privacy conscious que uma aplicação de utilização obrigatória.

Neste campo, não parece haver indícios de que a utilização de tecnologias que respeitam a privacidade tenha resultados menos eficazes que a utilização de tecnologias mais intrusivas.

#### **Temos dito muitas vezes que a transição para o digital se deu de forma repentina e avançámos em três meses quase 10 anos? Isto é mesmo assim? Já há estudos ou métricas que o confirmem?**

É indiscutível que a pandemia acelerou a transformação digital em toda a economia, num movimento sem precedentes, incluindo em indústrias tipicamente mais tradicionais.

Já foram realizados vários estudos centrados no impacto da digitalização nos países mais afetados pela pandemia: China, EUA, Itália e Espanha, e mais recentemente África. Embora não haja números específicos sobre o nível de digitalização em Portugal e na Europa, num estudo pan-europeu realizado no mês de abril sobre o impacto da COVID-19 na economia da UE e possíveis recomendações para mitigar os riscos, 90% dos inquiridos consideraram que um pacote de estímulos à transformação digital é altamente relevante para ajudar a UE a recuperar da crise. Do ponto de vista do consumidor, um estudo recente da McKinsey, referindo-se também a Portugal, mostra



que o povo português retomou durante a pandemia novas atividades digitais, incluindo videoconferência, entretenimento e bem-estar físico.

A transformação digital é um pilar fundamental da economia pós-COVID-19. O já tão falado "novo normal" do ponto de vista económico é caracterizado pela: afirmação da economia *High Tech, Low Touch*: por exemplo, as interações contactless permitem assegurar um elevado nível de automatização e uma interação pessoal baixa ou mesmo inexistente; o desenvolvimento da *Stay-at-home-economy*: à medida que passamos mais tempo em casa, o comércio eletrónico está em clara expansão, bem como a educação e o entretenimento online. Os produtos e serviços estão a ser entregues de uma forma que pode satisfazer melhor as necessidades dos consumidores em termos de conveniência, saúde e bem-estar; digital competition = digital divide: a transformação digital tem sido um motor de concorrência e inovação durante a última década. No entanto, as organizações que tinham investido antes da pandemia na sua transformação digital conseguem adaptar-se mais facilmente ao novo negócio normal.

### **A transição para o digital está a ser feita ou estimulada pelo Governo salvaguardando as questões da privacidade e segurança?**

Para uma resposta cabal a este aspeto seria necessário analisar os vários aspetos nos quais urge proteger a privacidade e segurança. Por um lado, no âmbito da atividade legislativa, seria muitas vezes adequada uma análise mais profunda e cuidada, para evitar possíveis conflitos entre a legislação de proteção de dados e outros esforços legislativos.

No entanto, há que salvaguardar que pelo menos a preocupação com a privacidade parece existir no desenvolvimento de iniciativas e políticas. Aliás, o plano de transformação digital aprovado pelo Governo contempla as questões de proteção da privacidade e da cibersegurança, por isso acredito que estes aspetos serão tidos em consideração.

### **Quais são as principais ameaças/perigos que os cidadãos e as empresas devem acautelar quando fazem, no primeiro caso, utilização do digital no seu dia-a-dia, e, no segundo, a utilização nos negócios?**

Os ciberataques são um dos principais perigos associados à digitalização da economia. Isto já era claro antes da pandemia, recorde-se que o World Economic Forum apontou os ciberataques como um dos principais riscos para este ano no *The Global Risks Report 2020*, e ficou ainda mais evidente durante a pandemia.

Ao mesmo tempo que as empresas estão a mover as suas operações online, e tendo em consideração que alguns empregados ainda estão a trabalhar remotamente, há várias frentes de cibersegurança expostas, correndo o risco de fuga de informações sensíveis e segredos comerciais.

### **E Portugal em que ponto está quando falamos de digital versus privacidade?**

No que se refere especificamente ao quadro legal, cumpre referir que, em cumprimento das obrigações legais que advêm do RGPD, o Estado português aprovou a Lei 58/2019, de 8 de agosto, necessária para a execução do RGPD em Portugal. No entanto, esta lei motivou grande controvérsia, o que levou a CNPD a publicar uma deliberação onde refere que irá desaplicar um número considerável de disposições da lei nacional, por as considerar incompatíveis com o RGPD. Esta opção da CNPD que ainda que não seja inédita é, mesmo assim, rara, pelo que se espera alguma clarificação pelos tribunais (nacionais e europeus) relativamente à aplicabilidade efetiva das normas em questão.

Do ponto de vista dos titulares dos dados, podemos ver o último relatório de atividades da CNPD, no qual esta entidade refere a existência de um aumento da consciencialização dos direitos dos titulares dos dados



por parte destes e um conseqüente aumento das situações de reporte de situações de violação da lei à CNPD.

Arriscaríamos dizer que a tendência será de crescente conhecimento e crescente utilização dos meios reativos consagrados no RGPD, pelos titulares dos dados, para fazer valer os seus direitos.

Finalmente, notamos que as empresas estão cada vez mais empenhadas em assegurar que desenham os seus produtos e serviços – e muitos deles envolvem o tratamento de dados pessoais – de forma compatível com as regras aplicáveis. As empresas portuguesas que estão mais avançadas nos processos de transformação compreendem a importância dos dados na economia digital e sabem que é fundamental desenhar os seus produtos e serviços em linha com os requisitos legais aplicáveis.

#### **E que caminho espera fazer nos próximos tempos?**

Ainda que esteja ciente que muitos desafios nos esperam devido à pandemia, penso que também há aqui algumas oportunidades que podem ser exploradas. Entre elas, uma oportunidade de agilizar a transição digital e de pensar em iniciativas inovadoras que possam contribuir para a economia. Por exemplo, já durante a pandemia foi publicada uma importante resolução do conselho de ministros relativa à promoção de Zonas Livres Tecnológicas que se espera poder contribuir para promover a implementação de diversas tecnologias importantes no nosso País (como Inteligência Artificial, DLTs e 5G). A transposição do Código Europeu das Comunicações Eletrónicas e da nova legislação europeia de proteção do consumidor também será bastante relevante.

Da União Europeia deverão vir algumas novidades tanto a nível legislativo como a nível de iniciativas económicas. Talvez tenhamos desenvolvimentos no Regulamento ePrivacy e aguardamos ansiosamente a proposta do Digital Services Act.

Espera-se que haja um acordo para um novo quadro financeiro plurianual ambicioso e que inclua uma dotação financeira adequada no suporte ao desenvolvimento tecnológico na União Europeia. Isto parece-me essencial, mas não me arrisco a prever as negociações. O certo é que a

indústria europeia precisa de algum poder económico para competir internacionalmente.

#### **As pessoas estão mais alerta para os perigos da tecnologia e da digitalização. São de facto as questões da privacidade que mais preocupam os portugueses? Que outras?**

O Regulamento Geral sobre a Proteção de Dados tem gozado de um nível de mediaticidade incomum para um ato legislativo. Naturalmente, muitas pessoas que não estavam tão sensibilizadas para a questão da privacidade tiveram curiosidade, exploraram e estão agora mais atentas aos seus direitos.

Segundo um estudo da Agência dos Direitos Fundamentais da União Europeia, 74% dos portugueses (acima da média europeia) estão cientes da existência do Regulamento Geral sobre a Proteção de Dados. Adicionalmente 68% dos nossos cidadãos conhecem a autoridade de controlo portuguesa. Naturalmente que há outras questões para além da privacidade que preocupam os portugueses, como a saúde e a economia. No entanto, os portugueses aparentam estar cientes de que a privacidade não sendo um bem absoluto também não é um valor menor e que a sua restrição se deve manter no estritamente necessário ao combate à doença.

#### **Que conselhos deixa aos nossos líderes que enfrentam este desafio da transição digital?**

A transição digital estará repleta de oportunidades para os líderes que sejam capazes de ter uma visão estratégica da transformação digital. A pandemia levou a que algumas soluções de transição digital fossem implementadas, muitas vezes, sem a ponderação que seria desejável em "tempos normais". A transformação digital é mais relevante que nunca, e todos queremos ser os primeiros. Mas não vai ser só a velocidade a distinguir os "vencedores" desta corrida, uma boa implementação tecnológica exige conformidade com a lei e uma abordagem future-proof. E não é só devido às potenciais coimas ou outro tipo de sanções que podem pesar, e muito, no bolso das empresas. É que atualmente os próprios consumidores estão mais atentos e a confiança é dos maiores ativos de uma empresa. ●

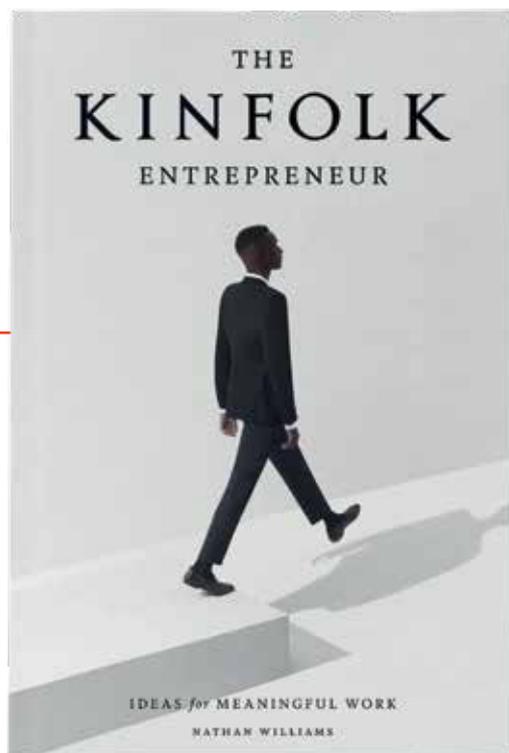


## *Phone Detox* **The School of Life**

Uma ferramenta para trazer sanidade a algum relacionamento tecnológico mais intenso e possivelmente mais perigoso.

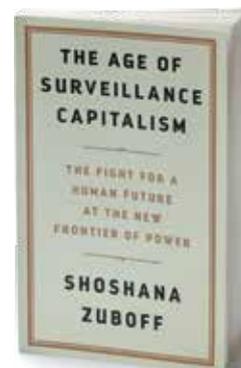
A verdade oculta é que ficou muito difícil encontrar alguém ou algo mais interessante do que o smartphone. Esta percepção desconcertante e preocupante teve para a maioria de nós enormes consequências nas nossas histórias de amor, vida familiar, trabalho, lazer e saúde.

É por isso que a School of Life criou o Phone Detox, repleto de ideias e meditações sobre o complexo relacionamento que temos com nossos telefones.



## *The Kinfolk Entrepreneur* **Nathan Williams**

Mais de 40 empreendedores criativos de todo o mundo estão a tornar os negócios pessoais. O livro explora como as ideias visionárias criam raízes e amadurecem nas carreiras, e as inúmeras maneiras pelas quais a busca pelo significado e pela paixão e as experiências de decepção e derrota podem motivar o sucesso profissional e uma qualidade de vida equilibrada. Por meio de entrevistas perspicazes com líderes nos mundos da publicação, tecnologia, arquitetura, moda, design, e além, o *The Kinfolk Entrepreneur* captura as ambições e realidades e oferece conselhos e inspiração para quem procura seguir seu próprio caminho na vida.



## *The Age Of Surveillance Capitalism* **Shoshana Zuboff**

A era do capitalismo da vigilância é um exame profundamente fundamentado da ameaça de poder sem precedentes, livre de supervisão democrática. Ao explorar o impacto deste novo capitalismo na sociedade, na política, nos negócios e na tecnologia, Shoshana Zuboff expõe as lutas que decidirão o próximo capítulo do capitalismo e o significado da civilização da informação. Mais criticamente, mostra como podemos proteger a nós próprios e às nossas comunidades e garantir que somos os mestres do digital, e não os seus escravos.

**DESTAQUE**

# EVENTOS



## Web Summit

É a maior conferência de tecnologias e empreendedorismo da Europa. O evento que no ano passado recebeu mais de 70 mil pessoas, de 163 países, em Lisboa, este ano "vai aderir aos mais rigorosos protocolos de saúde, conforme orientação do Governo de Portugal".

**02 A 04 DEZ**

Lisboa  
Online e Offline

## The Great Wave

Um festival que será online, offline, no ecrã e no mundo físico para fazer negócios de forma mais bonita. Como muitas economias estão a reabrir e estamos a voltar a uma (falsa sensação de) normalidade, não devemos deixar que esta crise, esse espaço de possibilidade, seja desperdiçada. Como queremos viver daqui para frente? Como vamos trabalhar? E que tipo de empresas desejamos? Estas serão algumas das questões centrais debatidas.

**16 E 19 OUT**

House of Beautiful  
Business



## IDC Directions 2020

Com o tema "*Changing Customer Requirements: Creating Value in the Digital Economy*", o evento da IDC debate a Economia e a Organização digitais. Para além do grande salto tecnológico, pelo menos em termos de "mindset", provocado nos últimos meses pelo COVID-19, estimamos que nos próximos cinco anos a economia irá acelerar e ganhar escala como nunca se viu antes. A IDC prevê que a economia digital venha a representar mais de 50% do PIB já em 2023. Este contexto, dominado pelo digital, exigirá uma nova espécie de organização, que obrigará a profundas alterações nos modelos de negócio, no trabalho, nas operações, na relação com clientes e consumidores, na inteligência empresarial, até na infraestrutura tecnológica.

**28, 29 E 30 SET**

**1 E 2 OUT**

Live