

## Revolução nos dados pessoais

EXAME | 09.08.2019 às 12h41



As regras do jogo mudam já este mês, com a entrada em vigor, em toda a União Europeia, do Regulamento Geral da Proteção de Dados (RGPD), o documento que mais irá revolucionar a forma como as empresas tratam os dados pessoais dos seus clientes ou utilizadores. **Este artigo foi originalmente publicado na edição de maio de 2018 da revista EXAME.**



PAULO M. SANTOS

O regulamento foi publicado em 2016, com um prazo de adaptação de dois anos, para que o tecido empresarial tivesse tempo suficiente para adotar as novas regras. Escreveram-se milhares de artigos sobre o tema, realizaram-se centenas de debates e de sessões de esclarecimento. Com um prazo tão alargado, seria de esperar que toda a gente estivesse mais do que preparada para as mudanças que aí vêm... mas não. Muito pelo contrário. Segundo uma sondagem recente realizada pela IDC, apenas 2,5% dos gestores portugueses admitiram que a sua empresa está preparada para lidar com a nova lei de proteção de dados.

Preocupado? Deveria estar, mas, a avaliar pelos inquéritos semelhantes realizados noutros países, os resultados não são tão desanimadores. Na Alemanha, por exemplo, país que por norma mais se prepara para este tipo de mudanças, uma sondagem da Computerwoche garantia que apenas 2% das empresas estavam realmente preparadas para as alterações. E metade delas mostrava-se preocupada se conseguiria ou não cumprir todos os requisitos exigidos dentro do prazo. No Reino Unido, 89% dos gestores admitiram que ainda estão confusos com as alterações que a lei irá trazer. Em França, na Irlanda e na Holanda, o panorama não é substancialmente diferente.

Este grau de impreparação do tecido empresarial para o novo regulamento levanta muitas dúvidas quanto à sua entrada em vigor no próximo dia 25 de

PUBLICIDADE



SAIBA MAIS



levanta muitas dúvidas quanto à sua entrada em vigor no próximo dia 25 de maio. Mas não só. Há outros receios por parte dos empresários. José Eduardo Carvalho, presidente da AIP, diz à EXAME:

“As principais preocupações das empresas nesta matéria centram-se nos custos de implementação, no prazo de aplicabilidade e nas coimas em caso de infração.”

A implementação de medidas que satisfaçam os requisitos do RGPD requer investimento e nem toda a gente tem capacidade financeira para o fazer, tal como defende Ana Jacinto, presidente da AHRESP, associação que representa a restauração e a hotelaria. Este é um processo de adaptação “oneroso e complexo, incomportável e injustificado para muitas delas, em especial no que diz respeito às micro e às PME”, que representam 99% do tecido empresarial português.

As várias consultoras e escritórios de advogados, contactados pela EXAME sobre o processo de adaptação a este novo regulamento, admitem que muitas empresas, sobretudo as de pequena e média dimensão, ainda não estão preparadas. Reconhecem que, à medida que o prazo aperta, a procura de ajuda por parte de empresários, nomeadamente PME, aumenta exponencialmente.

Magda Cocco, senior partner do escritório de advogados Vieira de Almeida, VdA, diz que existe já um grande nível de cumprimento das regras por parte de grandes empresas, sobretudo em setores regulados, como a saúde, a banca e os seguros. “Tivemos empresas que começaram a trabalhar nas mudanças para este regulamento no dia seguinte à sua publicação, em 2016”, salienta. Mas casos como este são a exceção. A maioria das empresas está longe de assegurar uma transição atempada. É por isso que José Eduardo Carvalho defende “uma prorrogação do prazo para a implementação do RGPD por mais 24 meses”.

E, se para as empresas mais comuns o processo é difícil, fomos perguntar às grandes operadoras de telecomunicações que lidam com milhões de dados, e muitos deles interligados entre si, como é que está a ser a adaptação à lei. “É um desafio brutal. De facto, é violento para quem gere uma multiplicidade de dados como nós fazemos”, disse Alexandre Fonseca, presidente-executivo da Altice Portugal. Apesar das dificuldades, o gestor garante que a sua empresa “irá cumprir” o regulamento, mas aproveita para apelar ao regulador “que tenha o cuidado de perceber o balanço entre o cumprimento escrupuloso, ou até por vezes com excesso de zelo, da legislação e um tratamento no espírito da lei, mas não necessariamente só na letra da lei”. Alexandre Fonseca considera que, pelo menos numa primeira fase, as empresas “terão de ter alguma flexibilidade para, por um lado, garantir a privacidade dos cidadãos”, e, por outro, também manter “o desenvolvimento de projetos. Caso contrário não é gerível”, realça.

Filipa Carvalho, diretora jurídica e de regulação da NOS, admite que “o novo regulamento traz enormes desafios e orientações bastante exigentes”, razão pela qual defende que, “dada a complexidade das novas regras, parece-nos natural que venha a existir um período de adaptação”.



SAIBA MAIS

#### DESTAQUES



EXAME: Há 30 anos a contar a economia



Um dia de história e de futuro: veja o vídeo da conferência da EXAME

#### ÚLTIMAS LUSA

**há 9 minutos** Moçambique/Dividas ocultas: Tribunal sul-africano adia audiência sobre extradição de Chang

**há 17 minutos** Eleições/Madeira: Cabeça de lista do PS diz estar “preparado” para ser presidente do Governo Regional

**há 22 minutos** Motoristas: Abastecimento no aeroporto de Lisboa “em níveis bastante abaixo do estipulado” -- ANA

**há 29 minutos** Incêndios: Pouca experiência de piloto e técnica de pilotagem originaram acidente no Algarve

**há 38 minutos** PSI20 encerra no 'vermelho' com BCP a perder 5,22%

### O que aí vem

Mas, afinal, o que assusta tanto os gestores e os empresários? Vamos por partes. O RGPD foi desenvolvido a pensar na harmonização da legislação europeia em matéria de dados e traz inúmeras mudanças, quer para as pessoas quer para as empresas ou outras entidades que lidam com informações pessoais. Protege os direitos do utilizador em praticamente todas as formas concebíveis e entende que a recolha e o manuseamento de dados deverão estar sempre protegidos em todas as fases do processo. Mais: os consumidores podem saber, sempre, o que as empresas estão a fazer com eles.

O RGPD consagra direitos que, apesar de já estarem definidos na lei que se encontra em vigor desde 1995, não eram respeitados, como, por exemplo, a alteração do consentimento e o direito ao esquecimento. No primeiro caso, sempre que uma pessoa disponibiliza os dados num determinado serviço, este pede-nos que aceitemos algumas regras. Esse acordo ficava em vigor e era muito difícil de mudar. Agora, as empresas são obrigadas a ter um sistema que permite ao utilizador alterar o seu consentimento sempre que o queira.

No segundo caso, o utilizador pode, em qualquer altura, pedir que os seus registos na base de dados sejam apagados, o chamado direito a ser esquecido. Para as empresas, este é um dos casos mais complicados de resolver, porque muitos dos sistemas que processam estes dados estão replicados. Por exemplo, a quem nunca lhe aconteceu pedir que apaguem o nome de uma base de dados para efeitos de marketing, mas, passado um mês ou dois, estão a ligar outra vez porque o nome estava noutra base de dados da empresa? Com o RGPD, esta situação terá de mudar. O pedido de esquecimento obriga a que tudo seja apagado.

### Agora é a doer

Apesar de todas as alterações que irão ocorrer, as multas elevadas são a grande preocupação da comunidade empresarial. Estas podem chegar aos 20 milhões de euros ou a 4% da faturação de uma empresa, consoante o valor mais elevado. Este é o montante máximo das coimas, mas cada Estado-membro pode fazer uma graduação dos valores em função do tipo de incumprimento. Por exemplo, o Governo português já definiu os valores mínimos das coimas a aplicar em Portugal. Para pessoas individuais, o valor será 500 euros para as contraordenações graves, e mil euros para as muito graves. Para as pequenas e médias empresas, as coimas serão mil e dois mil euros, respetivamente, e, para as grandes, os valores sobem para 2 500 e 5 000 euros. O Estado fica, para já, isento de multas, mesmo em caso de infrações. José Eduardo Carvalho não concorda e defende “a redução significativa das coimas”, censurando “a sua não aplicabilidade às entidades públicas”.

Antes, as multas funcionavam quase exclusivamente por denúncia. Uma das contraordenações típicas era a do cliente que se queixava por ter sido contactado por uma determinada empresa, após já lhe ter dito que não queria ser incomodado com ofertas de serviços. Outra era a das

videovigilâncias não assinaladas. Poucas mais havia. Agora o caso é sério e, além das denúncias, o regulador terá uma maior capacidade de fiscalização das atividades de cada entidade.

Para lá das multas, a outra grande mexida na lei assenta na necessidade de notificação do regulador sempre que haja uma falha na segurança das bases de dados. Entende-se como falha de segurança a destruição, perda, alteração, divulgação não autorizada ou acesso a dados pessoais – ataque de um hacker, roubo de um computador ou de uma pen com informações, entre outras. Sempre que tal aconteça, a empresa é obrigada a reportar o sucedido à Comissão Nacional de Proteção de Dados e, em caso de ser uma situação grave, terá de fazê-lo também aos seus titulares.

Outra das maiores mudanças trazidas pelo RGPD é a forma como se inicia um procedimento que envolva o tratamento de dados. Até agora, a lei previa que, antes de começar a recolha ou o processamento de dados, a entidade tinha de pedir autorização ou notificar a Comissão Nacional de Proteção de Dados (CNPd). Por exemplo, tinha de se pedir autorização antes de se instalar câmaras de videovigilância ou quando se fazia bases de dados que definiam características ou padrões de comportamento (profiling) dos clientes, etc. Esta necessidade de autorização desaparece. Cada empresa pode, pura e simplesmente, começar a fazê-lo sem necessitar de autorização – mas não para todos os tipos de dados. Está ainda por publicar uma lista de quais os dados mais sensíveis que obrigam a um pedido de autorização à CNPD para fazer o seu processamento.

O regulador dá mais liberdade mas impõe multas elevadas que servem de fator de dissuasão perante o incumprimento e que aumentam a capacidade de fiscalização.

Neste âmbito, o regulamento obriga as empresas a munirem-se de uma série de medidas e de um conjunto de procedimentos para verificarem se o regulamento é ou não cumprido. Uma delas é o Privacy by Design, que significa que todos os sistemas informáticos desenhados para o processamento de dados terão de ser concebidos já com estes novos procedimentos previstos no RGPD. Além disso, as empresas terão de criar um sistema de autoavaliação permanente da proteção das bases de dados (Privacy Impact Assessment) que estão na sua posse, bem como arquivar todos os procedimentos feitos com esses dados, incluindo a tipologia, o tempo durante o qual estiveram na sua posse e se foram exportados para países fora a União Europeia.

Apesar de ser um regulamento comunitário, este abrange empresas estrangeiras em duas situações: quando há controlo online de dados de cidadãos europeus (redes sociais) e quando existe uma oferta online de produtos e de serviços na União Europeia (sites de vendas). O regulamento obriga a que essas empresas tenham um representante estabelecido na Europa.

Por último, o RGPD cria uma nova figura para os quadros das empresas que lidem com dados: o encarregado de Proteção de Dados, do inglês Data

Protection Officer (DPO).

### Um novo gestor

Não basta uma empresa ter uma base de dados para ser obrigada a ter um DPO: Apenas se a sua atividade implicar um controlo sistemático do comportamento dos titulares dos dados ou se Esta tratar, em grande escala, de categorias especiais de informações (saúde, financeiras, criminais, entre outras).

Mas a lei ainda não é clara sobre a definição de grande escala, pois varia de país para país. Certo é que os bancos, as seguradoras, os hospitais, etc., terão de criar esta nova figura nos seus quadros.

Existem ainda outras lacunas na lei. Por exemplo, esta não é explícita se um conglomerado económico necessita de apenas um DPO para todo o grupo ou se terá de ter um em cada empresa. Além disso ainda não está determinado que lugar este novo cargo irá ocupar na estrutura de governação da entidade empresarial. Mais uma vez, a lei é pouco clara, e apenas diz que tem de reportar à administração ao mais alto nível. Ou seja: o CEO não tem desculpa para não estar informado sobre o tema.

O setor público também será obrigado a ter um DPO, mas ainda está em discussão na Assembleia da República se este será comum para todos os serviços ou se cada um deles terá o seu próprio encarregado de proteção de dados. A lei aponta no sentido da segunda versão, mas ainda não está fechada.

Segundo Magda Cocco, existe neste momento alguma dificuldade de as empresas identificarem e contratarem gestores para este cargo. “Não há no mercado pessoas com o know-how necessário para esse tipo de função”, salienta.

### Cuidados a ter

O marketing é o caso que tem gerado mais contraordenações em termos de violação do uso de dados e, segundo os especialistas contactados pela EXAME, deverá ser o setor em que poderá haver mais problemas nesta fase inicial, devido aos processos automáticos de recolha e de tratamento já existentes. Por exemplo, uma empresa que faça profiling automatizado, apesar de ser uma prática legítima, necessita da autorização da pessoa a quem esses dados pertencem para os poder analisar. Quando compramos um produto e nos pedem uma série de dados, essa empresa não necessita deles para aquela transação. Deseja-os para fins de marketing pessoal. A utilização indevida dessa informação é uma típica situação de incumprimento.

Além disso, com a aplicação do RGPD, “as pessoas ficarão mais conscientes e alertas para o tema e irão contactar mais as empresas para saberem que tipo de dados é que estes têm sobre si e, consoante as respostas, as empresas poderão ter problemas”, diz Magda Cocco.

### Uma nova era

E se tudo isto já gera muita confusão, então prepare-se para o que aí vem. É que o tema não vai ficar fechado no dia 25 de maio. Ainda falta vir a lume uma série de orientações da autoridade nacional, como os tratamentos de dados que estão sujeitos a autorização prévia, os que não estão sujeitos ao Privacy Impact Assessment, etc. Além disso, há outro regulamento comunitário que ainda está em discussão e que irá entrar em vigor mais tarde, o ePrivacy, que definirá as regras aplicáveis ao tratamento dos dados dos operadores de telecomunicações, bem como os dos over the top (skype, WhatsApp) e a qualquer setor que comunique através de meios digitais. O documento já vai na quinta redação e ainda não está fechado. Se o RGPD teve mais de quatro mil emendas desde que começou a ser discutido, este teve ainda mais.

Terá também um período de adaptação, apesar de ainda não se saber de quanto tempo.

A Europa está inundada de incertezas em relação à proteção de dados pessoais. Mas uma coisa é certa. A primeira empresa a ter um problema de violação da lei após o dia 25 de maio irá abrir as manchetes em todo o mundo. Falta saber o valor das primeiras multas. Estas poderão determinar se os reguladores terão ou não mão pesada para os prevaricadores. No mundo digital há o antes e o depois do RGPD. E a proteção de dados nunca mais será a mesma.