CISION

advocatus

ID: 83944620

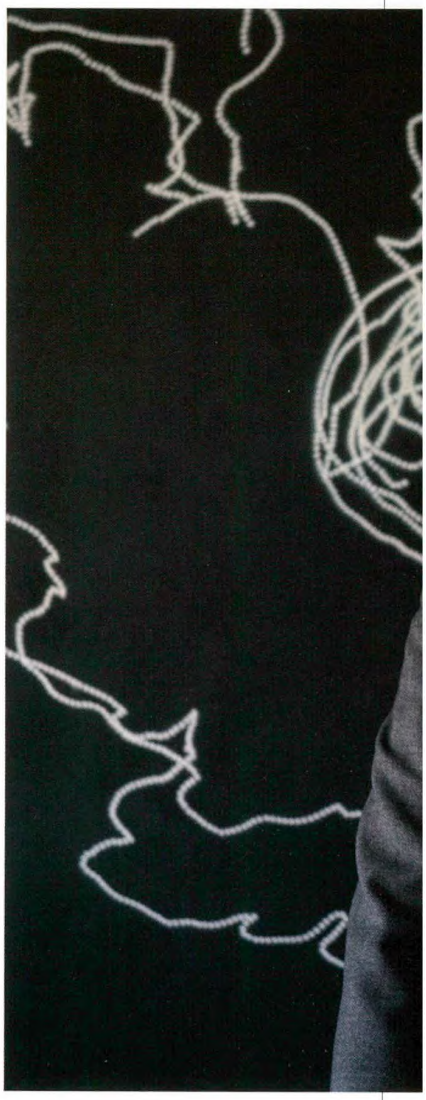
31-12-2019

Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Outros Assuntos

Pág: 34
Cores: Cor
Área: 18,00 x 22,48 cm²
Corte: 1 de 4

Luís Neto Galvão

"As empresas cumprem os mínimos olímpicos no RGPD"



Luís Neto Galvão é sócio da SRS Advogados e conta com mais de 20 anos de experiência. O advogado esteve à conversa com a *Advocatus* e explicou como tem sido a adaptação das empresas portuguesas ao Regulamento Geral de Proteção de Dados (RGPD), o papel que a Comissão Nacional de Proteção de Dados (CNPD) tem assumido e ainda comentou a Lei n.º 58/2019, de 8 de agosto.

Texto **FREDERICO PEDREIRA**
Fotos **HUGO AMARAL**

Desde 2015 que é consultor do Conselho da Europa (CE) na área da privacidade e proteção de dados. Como tem corrido este desafio ao longo dos últimos 4 anos?

É um desafio que não teve sempre a mesma intensidade. O Conselho da Europa tem um conjunto de cursos em matéria de direitos humanos sobre várias matérias, uma delas sobre a proteção de dados e privacidade, e o objetivo era criar um novo curso. Com o financiamento da União Europeia (UE), têm um conjunto de ofertas em matérias de cursos de formação online e lançaram um mini concurso para a seleção de pedidos para criarem um curso sobre proteção de dados. Nesse sentido participei nas atividades do CE nessa área. Criei um curso em 2017, mas entretanto com o RGPD houve a necessidade de o atualizar. Trabalhei nesse tema até 2019 e agora o curso já está atualizado e online. Aliás, aproveito para sugerir a todos os leitores que vão ao site do CE, ao projeto Humans Rights Education for Legal Professionals (HELP), e façam o curso online. É destinado a juristas, advogados, juízes e procuradores.

Em que consiste o aconselhamento que presta às empresas no domínio da privacidade e proteção de dados?

O nosso apoio é um pouco mais vasto do que meramente proteção de dados. Mas nessa área em específico apoiamos as empresas em tudo aquilo que necessita, face às novas obrigações e às antigas.

Em 2018 foi o início da aplicação do RGPD, mas antes disso as empresas já estavam obrigadas a cumprir um conjunto de obrigações em matéria de proteção de dados. Quem dava mais atenção a esses temas eram sobretudo empresas de certos setores, como saúde, telecomunicações, tecnológico e financeiro. Com o RGPD e com o novo paradigma que se criou, é suposto termos uma autoridade de proteção de dados, a CNPD, capacitada com um número de pessoas e de recursos que lhe permitem fazer uma fiscalização a todos os setores.

Tendo se alterado o paradigma, hoje em dia é suposto, pelo menos em teoria porque a CNPD ainda não começou a operar com os novos recursos que lhe foram conferidos, mas é suposto no fundo que haja uma maior atenção por parte das entidades fiscalizadoras.

Como tem sido a adaptação das empresas portuguesas ao RGPD?

Creio que tem havido uma preocupação acima do que eram as minhas expectativas. O problema começou a ser tratado bem antes de 2018. No entanto, talvez com algumas dificuldades, tendo em conta que tivemos uma transição para o RGPD que não foi muito acompanhada pelo regulador, pela CNPD. Não lhes foi possível apoiar o mercado, clarificando temas, respondendo a questões, porque o RGPD é um regulamento genérico que tem muitos princípios, muitos termos indeterminados e que necessitam de uma tradução prática. É complexo traduzirmos o que é a proteção de um direito fundamental, o direito à privacidade e à proteção de dados, traduzindo numa prática perante temas que mexem com a inteligência artificial, internet das coisas, videovigilância, com um conjunto de novos serviços que surgem a partir da cloud. As multi aplicações que surgem e que têm um conjunto de utilidades que são muitos óbvias para todos nós, mas que também lhes colocam muitas incertezas e inseguranças. Tudo isso necessita de um acompanhamento muito próximo, sobretudo quem tem a função

CISION

advocatus

ID: 83944620

31-12-2019

Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Outros Assuntos

Pág: 35
Cores: Cor
Área: 17,84 x 22,37 cm²
Corte: 2 de 4

de aplicar a lei e coimas. E isso poderia ter acontecido mais ao longo do período que levou ao início de aplicação do RGPD, 25 de maio de 2018, e depois disso também vamos chegar a um ponto de equilíbrio, creio que caminhamos para isso, já temos entretanto lei.

Do ponto de vista do legislador houve um atraso muito grande. Devíamos ter também uma lei de execução do RGPD, ou seja, havia aspetos que necessitavam de execução nacional e isso fez-se através de uma lei. Essa lei devia ter entrado em vigor em maio de 2018 e só veio a acontecer em agosto de 2019. No fundo foi muito positiva a reação das empresas. Houve dificuldades dada a falta de orientações e de legislação de execução, mas creio também que há um conjunto de temas que são muito relevantes, desde logo o facto de as PME's, nem todas as empresas têm os mesmos recursos para implementarem o RGPD. Como é óbvio, não é uma legislação que se aplique uniformemente em todos os setores e em todas empresas e deve haver um grau de adaptação, até por uma questão de política de gestão do risco. Nem todas as empresas e nem todos os setores têm o mesmo apetite ao risco e portanto dependendo do setor vamos ter um tipo de implementação e várias opções. Podemos ter vários instrumentos que ajudam a adaptar o regulamento ao setor e ao tipo de atividade, mas confesso que para as PME's vi uma dificuldade particular dada a limitação de meios que elas têm.

Depois temos também a administração pública que creio que ainda hoje existe uma necessidade especial de implementação do RGPD e, enfim, há muitos serviços que ainda não o fizeram de forma adequada.

Na sua opinião a Lei n.º 58/2019, de 8 de agosto, foi bem concebida pelos legisladores nacionais?

Nós precisávamos de uma lei e por várias razões. Uma delas tinha que ver com a falta de meios da CNPD. A lei veio permitir que a CNPD se capacitasse e que passasse a dispor de meios. Não que ela não os estivesses, mas no fundo uma grande parte da sua receita ia para segredo geral de estado. Tinha muitas limitações na contratação de pessoas, sobretudo nas com um perfil específico e especializado que necessita de ter. A lei veio resolver esse problema. Aquilo que acho que era o mais importante a lei resolver, era essa incapacidade que a CNPD tinha de responder aos desafios do RGPD.

Parece-me que idealmente devia ter sido possível ao legislador separar aquilo que é a atividade legislativa que tem que haver com a operacionalidade da CNPD, isso deveria ter sido tratado rapidamente. De todos os outros aspetos que tem que ver com a transposição para a realidade portuguesa de um conjunto normativos e princípios que constam do RGPD deveria ter sido separado um aspeto do outro e devíamos ter resolvido o problema da CNPD idealmente antes de 2018 ou no dia 25 de maio de 2018. Isso não veio a acontecer.

Por outro lado, quanto a todos os aspetos que tem que ver com a aplicação no contexto da saúde, dos dados da saúde, laboral, todos esses aspetos de especificações nacionais, o RGPD foi aprovado em 2016 e já antes de 2016 já era conhecido por todos que íamos ter uma alteração substancial do paradigma. Íamos ter um normativo muito mais exigente imposto aos estados membro. Portugal era conhecedor disso, até porque a proposta da Comissão Europeia era de 2012, tivemos um longo caminho de adoção e de 2016 para cá sabíamos que tínhamos de adotar um conjunto de medidas.

Desde logo capacitar a CNPD para lhe permitir ser um veículo de difusão, divulgação, esclarecimento de questões relacionadas com o RGPD e nada se fez. Na verdade só em abril de 2018 é que o Governo adota um projeto de regulamento

CISION

advocatus

ID: 83944620

31-12-2019

Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Outros Assuntos

Pág: 36
Cores: Cor
Área: 17,99 x 22,44 cm²
Corte: 3 de 4

e o envia à Assembleia da República (AR), pedindo à AR para o aprovar num tempo muito curto. Essa não foi a opção da AR. Entendeu que era um normativo demasiado importante e decidiu levar o tempo necessário e que foi mais de um ano. É lamentável de facto que o legislador não tenha tido outro tipo de abordagem a um normativo tão importante, sendo certo que sabíamos já desde 2016, mas até antes disso, que iríamos ter alguma atividade legislativa e isso não veio a acontecer.

Foram definidos limites máximos e mínimos para Portugal diferentes do regulamento europeu. Estamos perante uma violação do primado da UE?

Quando falamos do primado, falamos de um princípio muito antigo do Direito Europeu que determina que, em virtude de uma adaptação constitucional, este deve prevalecer sobre normativos nacionais que com eles estejam em conflito. Acredito que isso acontece no caso, por exemplo, da nossa Lei n.º 58/2019. Ou seja, de facto há um conjunto de opções em que o legislador foi muito para lá daquilo que, no meu entender, era suposto ter feito. Por exemplo ao estabelecer certas condições que devem ser cumpridas pela CNPD quando está a investigar e a reprimir um ato de atividade ilícita, uma violação da lei e do regulamento.

Tudo começou muito tarde, ou seja, não apenas a atividade parlamentar como também o projeto que foi enviado pelo Governo chegou tarde ao parlamento. Os deputados, até porque tive contacto com a comissão respetiva dos direitos humanos e com a relatora, fizeram o melhor trabalho possível. Foi uma pena não ter havido maior apoio técnico, quer do lado do Governo, quer do lado da AR. Durante aquele ano e meio poderia ter havido um trabalho legislativo de melhor qualidade.

O que entretanto veio acontecer foi que a lei entrou em vigor e a CNPD veio identificar numa deliberação um conjunto de aspetos que considera que o legislador contraria aquilo que consta do regulamento. Isso veio aumentar o clima de insegurança que já se sentia.

Estes são temas muito importantes, a CNPD identificou-os bem, fez um bom trabalho ao longo do processo de implementação e de preparação da lei. Mas adotar agora uma decisão em que ela identifica este conjunto de pontos e em que diz que "eu não vou aplicar a lei porque essas disposições específicas estão em contradição com o regulamento", creio que ela contribuiu um pouco para incerteza e insegurança jurídicas. Talvez não o tivesse feito, talvez tivesse deixado aos particulares e aos tribunais resolverem essas questões entre lei nacional e lei europeia, talvez tivesse orientado a minha orientação para aquilo que me parece prioritário que é pôr toda a máquina a funcionar. Se formos ver ao regulamento geral, há um artigo específico que estabelece as competências da CNPD em matéria da aplicação do RGPD e elas são múltiplas, são enormes. Só esse trabalho de pôr toda essa máquina em movimento consome muitos recursos e creio que é esse o papel da CNPD. No fundo deve capacitar-se e focar a sua atividade, neste momento, em executar bem aquilo que lhe foi imposto pelo regulamento, e não é pouco.

A nova lei da proteção de dados consagra ainda a responsabilidade penal das pessoas coletivas. A norma vem consagrar que se o mesmo facto for crime e contraordenação, é punido a título de crime. É caso para dizer que o crime compensa?

Espero que não seja, mas é verdade que de facto esse é um ponto que foi suscitado pela CNPD. Não é a primeira vez que temos a possibilidade de um conflito entre ilícitos criminais e ilícitos contraordenacionais, no fundo estarmos a olhar para a mesma realidade de dois pontos de vista.

No passado aquilo que é a minha experiência é que a ação da CNPD, em matéria contraordenacional, não foi impedida pelo Ministério Público e pelas autoridades de investigação criminal. Ou seja, não me recordo de no passado ter havido condenações de empresas por ilícitos criminais quando os mesmos poderiam ter sido sancionados por contraordenações, por coimas. É possível que o mesmo venha acontecer a partir daqui, mas não posso de facto fazer futurologia. Mas essa é uma questão que foi suscitada pela CNPD e creio que é uma questão muito pertinente.

A saída do Reino Unido da União Europeia vai ter alguma repercussão junto das empresas em sede de proteção de dados?

Creio que sim. Neste momento temos uma situação de grande incerteza a vários níveis, mas também no âmbito da proteção de dados. Porquê? Porque com o Reino

CISION
ID: 83944620
advocatus
31-12-2019
Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Outros Assuntos
Pág: 37
Cores: Cor
Área: 17,65 x 22,54 cm²
Corte: 4 de 4

Unido (RU) neste momento integrado na UE não existem quaisquer restrições em matéria de circulação de dados. A partir do momento em que haja o Brexit, o RU vai ficar numa situação um pouco particular, que é a de não ter um quadro que permita, por exemplo, o conhecimento pela UE que ele cumpre as regras em matéria de segurança e proteção de dados. Não vai ser um país, como são muitos outros países, por exemplo a Argentina, o Canadá, objeto de uma decisão de adequação. A Comissão Europeia tem a possibilidade de estudar os vários ordenamentos jurídicos num conjunto de países, o mais recente é o Japão, e de declarar que é um país seguro e para o qual as trocas de dados podem efetuar-se sem particulares cuidados adicionais. Isso não vai acontecer imediatamente com o RU. O ideal seria que acontecesse, que houvesse já uma decisão de adequação preparada para entrar em vigor no dia a seguir aquele em que fosse declarado efetivamente o Brexit. Isso não vai acontecer e portanto vamos ter aqui alguma necessidade de mecanismos de ajustamento.

Quais são os principais desafios atualmente das empresas, após toda a informação e preparação inicial ao RGPD?

O passo a seguir vai ser o de aprofundamento. No fundo, o tempo que mediou entre em 25 de maio e o dia de hoje, as empresas têm estado a implementar o RGPD de uma forma a cumprirem pelo menos os "mínimos olímpicos".

Dou um exemplo concreto, muitas empresas, pelo menos numa fase inicial, entenderam que o trabalho de implementação passaria em grande medida pelo próprio DPO, o encarregado de proteção de dados. Compreendo isso, é um custo, é alguém que está na empresa e a quem compete no fundo a responsabilidade do *compliance* em matéria de proteção de dados. Porém, não lhe compete, se lermos bem o RGPD, executar. É alguém que tem de garantir que os mecanismos estão em ordem, tem de ter alguma atuação em matéria de supervisão, tem de aconselhar, tem de formar, mas não lhe compete executar. É no fundo partilharmos a responsabilidade pela implementação do RGPD por toda a organização, empresa e não apenas deixá-la nas "costas" de um DPO, que deve ser independente e não tem propriamente funções que lhe permitam tomar decisões sobre a execução. Deve é garantir que aquilo que as empresas fazem cumpra o regulamento.

Os ciberataques são uma realidade em Portugal?

Nós somos um pequeno país aberto, em que os cidadãos têm particular apetência pela tecnologia, em que cresce um número de ofertas com base na internet, em que no fundo não há propriamente uma atitude muito conservadora e fechada. Por isso mesmo não estamos menos expostos a ciberataques do que qualquer outro país. Essa ameaça de ciberataques é idêntica em Portugal às que existem em qualquer outro país europeu aberto. Sobretudo, parece-me que vamos ouvir cada vez mais falar do tema. Sabemos no fundo que existem ataques a empresas na área da saúde, até em escritórios de advogados, e isso é uma realidade que passará a ser cada vez mais conhecida.

"A partir do momento em que haja o Brexit, o RU vai ficar numa situação um pouco particular, que é a de não ter um quadro que permita, por exemplo, o conhecimento pela UE que ele cumpre as regras em matéria de segurança e proteção de dados."

Como é que as empresas se protegem dos mesmos [ciberataques]?

A preparação é complexa porque desde logo é impossível evitá-las. É impossível fecharmo-nos ao mundo. Todas as empresas têm contactos com clientes através da internet, do *e-mail*, usam dispositivos de conservação de dados, e portanto as empresas em geral estão muito expostas. Como é que elas se podem proteger? Desde logo, tendo algum aconselhamento em matéria de cibersegurança. E a cibersegurança não é apenas termos umas boas *firewalls*. A cibersegurança é no fundo termos comportamento que são ciber seguros. A proteção de dados não está dissociada da cibersegurança, porque temos obrigações de segurança. Hoje em dia, para as empresas é muito difícil distinguir entre dados pessoais e não pessoais. Os dados estão muito interligados. Nessa medida, a proteção com a cibersegurança é também uma preocupação que temos em matéria de proteção de dados.

As empresas podem proteger-se desde logo, por exemplo, fazendo formação nesta matéria, obtendo aconselhamento externo e alterando o paradigma. O tema não é apenas tecnológico, é um tema de governance também. Deve haver em todas as empresas um tratamento do tema ciber pelo conselho de administração, pela gerência, por aqueles que têm como missão decidir sobre a estratégia da empresa. Desde logo é um tema não para delegar um responsável de IT, de forma cega e desinteressada, é um tema da gestão diária da empresa.

Depois o Centro Nacional de Cibersegurança tem tido um papel muito ativo em matéria de divulgação e parcerias. Hoje em dia só não está informado sobre temas de cibersegurança quem não quiser. Depois temos medidas específicas para empresas no setor financeiro, para empresas de pagamentos, para empresas na área das comunicações eletrónicas e na saúde. Existe uma melhoria de entidades que têm intervenção nas empresas e setores que estão abrangidos por obrigações em matéria de cibersegurança e entidades que têm como obrigação receber, por exemplo, notificações em matéria de segurança. Só nessa área temos o Centro Nacional de Cibersegurança, CNPD, Banco de Portugal, que por sua vez faz a ligação com o Banco Central Europeu, ANACOM, em matéria de comunicações eletrónicas e portanto o regime está a tornar-se cada vez mais complexo, está abranger cada vez mais setores. Nas PME's, que são aqui o elo mais fraco, creio que não será por falta de informação que não poderão ter proteção e uma cibersegurança assegurada.

Finalmente há ainda um quadro específico de crimes ciber. Em matéria de cibersegurança entende-se que quanto mais informação for partilhada melhor é para a comunidade e portanto há um certo favorecimento da partilha de informação. Em matéria de cibercrime temos também uma polícia bem "apetrechada" e temos um MP com unidades específicas e temos um quadro que me parece ser adequado.