LEI DA PROTEÇÃO DE DADOS:
COIMAS PODEM CHEGAR A 4% DO VOLUME DE NEGÓCIOS DA CLÍNICA

ANA ROCHA, ADVOGADA COM INTERESSE EM PROTEÇÃO DE DADOS
“AS COIMAS MAIS ALTAS PODEM IR DE 20 MILHÕES A 4% DO VOLUME DE NEGÓCIOS ANUAL”

O novo Regulamento Geral de Proteção de Dados (RGPD) entra em vigor em maio do próximo ano. Por esta altura, já as clínicas dentárias e os profissionais de Medicina Dentária terão de se ter adaptado às mudanças, numa preparação concedida por um período de dois anos, que cessa daqui a oito meses. Saiba o que vai mudar e antecipe incumprimentos e coimas.

Texto: Cláudia Pinto Fotos: David Oitavem

Que Regulamento é este e o que mudou em relação ao anterior?
Este Regulamento já não é novo e vai tornar-se aplicável a partir de 25 maio de 2018. Tem um âmbito muito amplo pois é aplicável ao Estado, ao setor privado e a qualquer empresa que trate de dados pessoais. Todas as empresas terão dados de trabalhadores e logo aí este regulamento aplica-se e tem um âmbito muito amplo. O impacto maior dependerá do volume de dados pessoais que serão tratados e não tanto da dimensão da própria empresa.
É um regulamento muito extenso, que não muda muita coisa naquilo que é a proteção da privacidade dos cidadãos, mas há uma mudança grande de paradigma. No anterior regime havia a obrigação de notificar e pedir autorizações à Comissão Nacional de Proteção de Dados (CNPD). Neste momento deixa de haver essa necessidade de notificarmos e a responsabilidade para o tratamento das regras passa para os próprios responsáveis pelo tratamento, ou seja, para as empresas que estão a tratar os dados. Isto não era assim…
Havia uma espécie de um controlo da CNPD através deste modelo de notificação e de autorização prévia que se tinha de seguir. Isto significa que o regulamento coloca no colo das empresas a obrigação de garantir que está tudo conforme.
São elas que têm de perceber se estão a cumprir com todos os requisitos da lei.

Porque se decidiu criar este novo Regulamento?
O que se compreendeu é que houve uma evolução tecnológica tão grande que tornou muito mais fácil de replicar, usar ou aceder indevidamente aos dados pessoais. Sabemos que a investigação clínica assenta, muitas vezes, em tratamento massivo de dados. Consegue-se hoje armazenar uma enorme quantidade de dados, devido aos avanços tecnológicos, mas isto também pode levantar muitos riscos para os direitos, liberdades e garantias, bem como no que respeita ao tratamento ilegítimo desses dados. A qualidade dos dados é relevante para verificarmos se o tratamento dos mesmos é legítimo. Esta matéria tornou-se mais sensível com as novas tecnologias tornando-se ainda mais importante aumentar a consciencialização através da CNPD e das coimas avultadas.

Esta mudança de paradigma parece simples, mas acaba por ser uma responsabilidade ainda maior…
Sim, não é nada simples. A CNPD e as congéneres europeias ficam mais livres para vigiar, controlar e aplicar sanções a quem não cumpre, o que torna o regulamento mais relevante. Por outro lado passámos de coimas de valor baixo para valores astronómicos. As coimas mais altas podem ir de 20 milhões a 4% do volume de negócios anual, a nível mundial, do grupo de empresas. Este aumento exponencial das coimas trouxe um foco grande para a necessidade de cumprimento.
Depois, especificamente no que respeita às clínicas, importa a questão da sensibilidade dos dados. Estamos a falar de dados de saúde, que vão desde exames, a meios complementares de diagnóstico, a planos de tratamento, às notas do médico… Tudo isto se enquadra numa categoria especial de dados. São dados que necessitam de uma sensibilidade maior e que requerem, por isso, garantias adicionais de segurança e até de legitimidade para o seu tratamento. Isto leva-nos a outra questão: os cidadãos estão mais exigentes e sensibilizados para estas questões. Além do peso financeiro que pode recair numa empresa em que é aplicada uma coima, há ainda a considerar o impacto a nível de reputação caso haja uma violação de dados ou um tratamento que não é entendido como legítimo. Por vezes olha-se um pouco para o regulamento como um procedimento para verificamos se as coisas estão conformes, mas para mim é muito mais uma questão de ética. Esta dinâmica está muito mais relacionada com a imagem da empresa e de quem está a tratar os dados. A primeira pergunta que temos de fazer quando estamos a tratar de dados é o que é ou não legítimo face às expetativas do titular. Neste momento, as empresas estão a recolher muitos dados para depois os usarem com finalidades que não são necessariamente antecipáveis. O motor principal será, no futuro, essa responsabilidade ética.

Isso traz outros desafios aos próprios médicos, mas também a outros profissionais das clínicas…
As questões éticas estão muito intrínsecas na atividade dos médicos, na forma como veem a profissão, mas a utilização das novas tecnologias atualmente abre outros constrangimentos. O médico pode estar perfeitamente consciente das suas obrigações de sigilo e de confidencialidade, mas os colaboradores e funcionários não abrangidos pelo mesmo dever de sigilo também acedem aos dados.

O que sugere o novo Regulamento e ao que devem estar atentos os profissionais das clínicas dentárias?
Neste caso, o Regulamento diz que tem de se garantir que, ao nível tecnológico, há que implementar anti vírus, *softwares* e criar passwords para poder controlar isto, mas também se recomenda a formação e outro tipo de políticas/acordos de confidencialidade para dotar estas pessoas de uma maior noção de responsabilização. Especificamente nas clínicas dentárias, o Regulamento exige que o responsável pelo tratamento cumpra com todas as obrigações, ao nível de segurança e legitimidade, mas do que me apercebo da forma como a atividade é prestada nas clínicas dentárias, esta noção sobre quem é que recai a responsabilidade está muitas vezes diluída. Muitas vezes é da própria clínica, mas também pode ser do próprio médico dentista, ou até se pode dar o caso de ser uma responsabilidade conjunta. Às vezes, o paciente pode ser seguido por um dentista e pode ir a várias clínicas onde o profissional dá consultas, sendo relevante do ponto de vista da responsabilidade saber se o médico pode levar consigo toda a ficha clínica do doente, os exames, o plano de tratamentos, etc. ou se essa informação fica na própria clínica, ficando a mesma responsável por garantir a confidencialidade dos dados.

Os exames são sempre do doente… Essa é uma questão também muito discutida…
Esta é uma das grandes novidades do RGPD e tem especial interesse. O Regulamento criou um novo direito: o direito de portabilidade que indica que o próprio titular dos dados, o paciente, pode pedir à clínica ou o médico, dependendo de quem tem imputada a responsabilidade, que lhe transmita num formato de relatório clínico, tudo o que seja relacionado ao seu tratamento para poder transpô-lo a um prestador de serviços concorrente ou não para ter uma segunda opinião. O paciente pode também solicitar essa informação por motivos pessoais.

O que é que os médicos dentistas terão de passar a acautelar com este novo Regulamento e que não era obrigatório antes?
Os dados pessoais são todos aqueles que direta ou indiretamente possam identificar uma pessoa singular. Neste Regulamento novo será importante que as clínicas consigam definir qual o âmbito dos dados que têm de transmitir caso seja exercido o direito da portabilidade e o direito de acesso, que já existia, e que consiste em saber exatamente quais os dados que aquela clínica tem sobre a pessoa, que podem ir desde os dados da ficha de paciente até aos exames, ao plano de tratamentos, etc.
Há um outro tema relacionado com as novas tecnologias, e que no caso das clínicas dentárias me parece muito relevante, que se prende com o facto de os médicos dentistas transportarem dados pessoais no seu telemóvel, no

seu computador, numa pen ou em máquinas fotográficas e em todos os seus equipamentos que são, à partida, mais vulneráveis e não estão muito preparados para situações em que possa haver um roubo ou até perda, com uma grande possibilidade de acesso a dados de enorme sensibilidade. O que se pode e deve fazer é criar políticas de *bring your own device*. A entidade responsável desses dados deve definir quais são as regras para antecipar todas estas situações. Em caso de uma violação de dados é difícil demonstrar que foram aplicadas todas as regras de segurança se as mesmas não forem implementadas. O que se deve fazer é tentar antecipar. O RGPD é uma tentativa de antecipar violações de dados e sugere a aplicação de medidas para o evitar. Se por acaso isso acontecer deverá ser possível demonstrar que houve diligência e o cuidado suficiente tendo em conta os dados em causa.

Os clientes têm noção destes direitos?
As pessoas começam a ter alguma noção. Começa a haver uma consciência mais geral dos seus direitos.

Considera que os responsáveis das clínicas dentárias estão suficientemente informados sobre as exigências deste novo Regulamento?
Julgo que algumas clínicas de pequena ou média dimensão pensam que estão um pouco abaixo do radar, mas a importância e o impacto deste Regulamento não está tão relacionado com o volume de negócios ou a dimensão das empresas, mas com o tipo de dados a tratar. No caso das clínicas, considerando que são dados de saúde, a importância deste novo Regulamento é muito relevante.
Estes projetos de implementação de RGPD são muito complexos. É necessário que todas as clínicas percam tempo a olhar para a sua casa e percebam que tipo de dados estão a ser tratados, quais são as vulnerabilidades, e todos os Departamentos da empresa estão impactados. Este não é só um projeto de compliance, jurídico, administrativo… é um projeto que abarca todas as áreas. O que me parece é que as empresas já deveriam ter começado a implementar mudanças, mas se ainda não o fizerem devem fazê-lo. Será muito importante demonstrar à Autoridade de Supervisão que há um esforço em tentar organizar "a casa" e perceber quais são os riscos maiores.
Julgo que muitas clínicas acreditam que estão fora do radar e que estas exigências não as vão atingir. Depois, o custo que tudo isto envolve é grande, seja em *softwares*, seja em formação ou outras medidas, o que pode ser um entrave. Há países, como a Alemanha e a Inglaterra, que estão muito à frente na consciencialização da importância de proteção de dados. Portugal ainda não está muito.

Qual deverá ser o papel da CNPD?
Julgo que deverá ser um papel muito mais de ajudar ao cumprimento, traduzindo o Regulamento para que possa ser aplicado na prática. Em última instância há que perceber por onde se começa. Era importante que a CNPD emitisse algumas *guidelines* e orientações muito específicas, com uma linguagem acessível e conselhos práticos que ajudassem a traduzir as exigências deste Regulamento. Neste momento está em fase de consulta pública, à população e aos *stakeholders* sobre se devem aplicar medidas mais restritivas no tratamento destes dados e possivelmente surgirá uma lei que vai concretizar alguns dos temas do Regulamento.

Por onde se começa? É difícil querer mudar tudo de uma só vez…
Diria que o primeiro trabalho a fazer é criar uma lista de prioridades, ou seja, fazer um mapeamento de todos os serviços, produtos que estão a ser desenvolvidos pela empresa, identificar os que são mais vulneráveis e começar a trabalhá-los, a criar políticas de retenção de dados… As clínicas guardam os dados ad eternum sem que haja muita razão para o fazer criando assim uma vulnerabilidade maior. Os dados só podem ser tratados para finalidades legítimas, restritas e durante um tempo determinado.

A CCA Ontier faz formação nesta área?
Os nossos projetos de implementação passam por ajudar as empresas a fazer esse mapeamento, por identificar esses gap's, fazer uma lista de prioridades e desenvolver algumas ações, como a criação de políticas de dados pessoais, políticas de controlos de acesso de emails e de internet pelos próprios trabalhadores, etc. Ajudamos as empresas com um verdadeiro projeto que tenta abranger todas as questões exigidas neste Regulamento.
O que nos apercebemos é que existem dúvidas e que as pessoas não sabem como desenvolver um projeto de proteção de dados. Desenhamos um projeto à medida das empresas e numa última fase faremos o acompanhamento daquilo que foi criado porque isto não acaba a 28 de maio de 2018. Será importante acompanhar o que foi implementado.
Ao nível da tecnologia, as clínicas até podem implementar *software*, *firewall* e outro tipo de proteção, mas depois existem armários sem chave, com arquivos dos pacientes ali mesmo à mão. Um projeto de RGPD tem de incluir a parte digital, mas também o papel. Este tem de estar seguro e há que definir quem pode ter acesso aos armários com estes arquivos. Um administrativo de uma clínica deve ter uma especial sensibilidade e uma formação particular para perceber que dados são tratados. Este Regulamento constitui um desafio enorme.
Os médicos propriamente ditos têm muita consciência e um sentido muito apurado do que é o sigilo e isso é fundamental como ponto de partida. Mas depois escapa-lhes uma grande parte porque o meio digital permite ter várias cópias diferentes. Considera-se uma quebra de segurança tanto a perda de dados, como o acesso indevido aos mesmos.

Que conselhos daria às empresas abrangidas por este Regulamento?
Diria para procurarem ajuda especializada e desenvolverem um projeto de implementação, olharem para a "sua casa" e aproveitarem para fazer esse mapeamento. Este Regulamento parece "só um peso", mas constitui uma forma de estarmos mais atentos ao que estamos a fazer, de capitalizá-lo a favor da própria atividade e de se prestar um melhor serviço.