NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UE

"NÃO É UMA REVOLUÇÃO, MAS SIM UMA EVOLUÇÃO"

O Jornal Médico quis saber o que muda com o novo Regulamento Geral de Proteção de Dados da União Europeia (UE), que todas as entidades têm a obrigatoriedade de adotar até maio do próximo ano, sob pena de incorrerem em coimas elevadas. Ana Rocha, advogada de Tecnologias, Media e *Telecomunicações & Propriedade Intelectual* (TMT & PI) e especialista nestas matérias, aponta e analisa as principais alterações decorrentes da nova legislação, esclarecendo e contextualizando conceitos como os de *data breach*, *data protection officers* ou *internet of things*.

Ana Rocha
Advogada do Departamento de TMT & PI da CCA ONTIER
Especialista em Proteção de Dados
(ar@cca-ontier.com)

JORNAL MÉDICO | O que muda – principais implicações, processos, procedimentos e regras – com o novo Regulamento Geral de Proteção de Dados da UE que todas as entidades, nomeadamente as do setor da saúde, terão de adotar até maio de 2018?

Ana Rocha (AR) | Este novo Regulamento não representa uma revolução, mas sim uma evolução. Na verdade, a maioria dos princípios e obrigações já se encontravam plasmados na atual diretiva, base das diversas legislações nacionais dos vários países membros. Ainda assim, há duas mudanças a destacar pelo seu enorme impacto para as empresas.

A primeira diz respeito ao valor das sanções, que nos casos mais graves podem ascender a 20 milhões de euros ou, no caso de uma empresa, a 4% do seu volume de negócios anual a nível mundial, consoante o montante mais elevado. A segunda grande alteração respeita à obrigação de *accountabilty* ou responsabilização que passa a impender sobre as empresas, passando a ser exigível não só o cumprimento da lei, como também a demonstração do cumprimento da lei às autoridades de controlo.

Esta última alteração representa uma mudança de paradigma, passando-se de um modelo de heterorregulação, no qual as empresas tinham a obrigação de efetuar uma notificação ou pedido de autorização à Comissão Nacional de Proteção de Dados (CNPD) antes de iniciar um tratamento de dados pessoais, para um modelo de autorregulação, em que as empresas terão de se responsabilizar por interpretar a lei e garantir que todas as obrigações são cumpridas. As empresas terão, por exemplo, de manter registos organizados das operações de tratamento que realizem, a obrigação de implementarem os princípios de *privacy by design* e *privacy by default* desde o primeiro momento de criação de um novo projeto, bem como, o dever de realizar avaliações de impacto sobre a proteção de dados em determinadas situações, imposições que implicam um esforço grande e acrescido ao nível da organização.

A necessidade de mudança dependerá do grau de maturidade de cada empresa no respeito pela privacidade. Não obstante, e mesmo considerando que haverá agentes económicos, sobretudo em alguns setores com legislação especial mais exigente nesta matéria – tais como as telecomunicações ou a banca – que estarão num estádio mais avançado de cumprimento, a implementação das novas regras do regulamento irá certamente acarretar um acréscimo aos orçamentos e aos recursos das várias equipas, devendo colocar o tema da privacidade nas mesas dos conselhos de administração de todas as empresas.

JM | As regras para obtenção do consentimento dos titulares (e a legislação sobre proteção de dados no geral) passam a ser muito mais exigentes. De onde vem esta necessidade de maior exigência e que reflexo terá no plano das instituições de Saúde?

AR | A alteração dos pressupostos para obtenção de um consentimento válido decorre de um movimento dos próprios titulares dos da-

Um *data breach* no setor da saúde tem, naturalmente, consequências mais gravosas do que noutros setores, atendendo à especial sensibilidade destes dados

dos, no sentido de se sentir uma necessidade de maior transparência, informação e controlo sobre os tratamentos dos seus dados pessoais. Na prática, apenas foram alteradas as regras para o consentimento base, tornando-o mais exigente, nomeadamente pela proibição de consentimentos implícitos, fundamentados no silêncio do titular ou em caixas *pré-tickadas*. Especificamente, no que respeita aos dados relativos à saúde e sempre que se recorra ao consentimento do titular enquanto fundamento legítimo para o tratamento de dados, mantém-se o mesmo modelo de consentimento *high standard* que se traduz na necessidade de obtenção de uma manifestação de vontade explícita. Parece-me que os próximos anos constituirão um desafio para as empresas, no sentido de que terão de conseguir comunicar e transmitir confiança, demonstrando que tratam os dados de forma justa. Serão vencedoras aquelas que melhor interiorizarem que os dados são dos seus titulares e que, como tal, o tratamento dos mesmos, em prol das organizações, apenas poderá ser realizado de forma ética e responsável.

JM | Algumas das novidades a nível organizacional contemplam a notificação obrigatória às autoridades de proteção de dados – CNPD – em caso de *data breaches* e a nomeação de *data protection officers* (DPO). Até que ponto estas alterações poderão contribuir para as boas práticas de segurança e privacidade da informação nas entidades do setor da saúde?

AR | Um *data breach* no setor da saúde tem, naturalmente, consequências mais gravosas do que noutros setores, atendendo à especial sensibilidade destes dados. A obrigação de notificação de *data breaches* às autoridades de controlo, e comunicação ao titular dos dados sempre que a violação dos dados pessoais seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas, parece-me que terá duas consequências imediatas e naturais, nomeadamente pelo facto das empresas terem necessariamente de se preparar para tentar evitar quebras de segurança, não só pelo valor das coimas associadas, mas também, e talvez sobretudo, pelo impacto a nível reputacional que um *data breach* pode representar para o bom nome e confiança dos titulares dos dados na organização. Por outro lado, a própria necessidade das empresas conseguirem identificar um *data breach* e terem processos adequados a agir de forma ágil para mitigar riscos e cumprir a lei obriga à implementação de medidas de segurança e organizacionais adequadas. Por outro lado, quanto à obrigação da nomeação de um encarregado de proteção de dados (DPO) parece-me uma mudança fundamental para garantir o respeito pela privacidade e segurança dos dados, aliás, seguindo as boas práticas já implementadas nesta área. Já havia muitas empresas que tinham um cargo desta natureza nos seus quadros. O DPO será a entidade preferencial de contacto com as autoridades de supervisão, ficando encarregue da monitorização do cumprimento das regras de privacidade, encabeçando um papel fundamental na orientação das organizações no desenvolvimento da sua atividade e de novos projetos.

JM | As entidades têm até dois anos para adotar as novas regras. Já passou um. Acredita que a maior parte dos organismos está em condições de cumprir este prazo legal?

AR | Dependendo do estado de maturidade das empresas, haverá algumas que estarão em melhores condições de cumprir. Parece-me, no entanto que em Portugal não temos ainda enraizada uma cultura de respeito pela privacidade nas organizações, em comparação com países como o Reino Unido, França ou Alemanha. Nesta medida, o esforço terá de ser maior. Até porque o cumprimento das novas regras representa não só a implementação de procedimentos e processos novos, mas também um assimilar destes novos conceitos e direitos de privacidade, consubstanciada numa necessidade de repensar e compreender também do ponto de vista ético qual o papel das empresas.

JM | Tendo em conta as várias entidades do setor da saúde – hospitais, companhias farmacêuticas, farmácias, PME, *startups* – quais, a seu ver, poderão ter maior dificuldade na adoção (adequada e atempada) das novas regras? E em termos de setor público *versus* setor privado, espera-se alguma discrepância?

AR | A transformação digital, as tecnologias da sociedade de informação, são realidades incontornáveis nos vários setores da economia e, claro, na sociedade em geral. O setor da saúde não é exceção e são enormes os desafios que se avizinham. Os avanços ao nível da inteligência artificial ou da realidade aumentada já não são apenas "ficção científica" levantando inúmeras questões em matéria de proteção de dados.

Quer ao nível da prestação de cuidados de saúde, organização interna, investigação ou da *internet of things* (IoT), sendo extremamente valiosos os recursos a *profiling* e *big data* e envolvendo todos os agentes da cadeia de produção – nomeadamente hospitais, farmacêuticas, laboratórios, *startups* e PME – que tenham atividade na prestação de serviços às entidades de saúde ou criação de tecnologias que tratem dados de saúde. Por outro lado, no setor público, e pela abrangência do seu universo alvo, a necessidade de desmaterialização dos processos e do acesso à informação e a introdução de novas tecnologias associadas à prestação de cuidados médicos representam maiores dificuldades no cumprimento das novas regras face ao setor privado.

JM | As coimas previstas no caso de incumprimento da legislação são elevadas. Quem terá a cargo a fiscalização deste processo e a instauração das mesmas?

AR | Atendendo ao novo sistema de balcão único, determina-se que a autoridade de controlo do estabelecimento principal do responsável pelo tratamento terá um papel mais proeminente, embora não exclusivo, no controlo e supervisão da aplicação do regulamento. Em Portugal, a CNPD será a autoridade de referência. Nesta sede, o papel das autoridades de controlo deveria não só constituir-se numa ótica única sancionatória, mas sobretudo formadora, educativa e "tradutora" dos conceitos e obrigações impostos pelas novas regras, devendo estar próxima dos cidadãos e das empresas. Este novo regulamento representará também um desafio para as autoridades de supervisão, na forma como vão encarar o seu novo papel.

Em Portugal não temos ainda enraizada uma cultura de respeito pela privacidade nas organizações, em comparação com países como o Reino Unido, França ou Alemanha