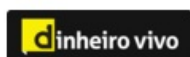


O que ainda ninguém disse sobre o RGPD

 dinheirovivo.pt/opiniao/o-que-ainda-ninguem-disse-sobre-o-rgpd-12805301.html

25 de maio de 2019



Celebra-se este mês, dia 25 de maio, um ano de Regulamento Geral de Proteção de Dados (RGPD). Um ano que fica marcado pelas primeiras coimas aplicadas por violação de dados pessoais e por muitas dificuldades de muitas entidades públicas e privadas, nacionais e estrangeiras, em pô-lo em prática. Um ano de tantas questões sobre a sua aplicação e de algumas denúncias pelo seu incumprimento.

Se, por um lado, podemos dizer que a resistência das empresas ao RGPD já foi, quase, ultrapassada, o mesmo não é verdade quanto aos cidadãos. Para muitos, o RGPD não passa de uma “coisa estranha”, pouco compreendida, que se reflete em muitos emails, ao estilo spam e acesso condicionado a sites. Mas o RGPD pode ser uma verdadeira arma, ao serviço do cidadão europeu na proteção dos seus direitos. Neste aniversário, mais do que colocarmos o enfoque nas empresas, optamos por colocá-lo nas pessoas.

Voltemos atrás no tempo.

A privacidade é um direito. Um direito previsto na nossa Constituição. Um direito reconhecido internacionalmente. Um direito que está diretamente ligado ao conceito de dados pessoais - que mais não é do que toda a informação que nos é própria como o Nome, o NIF ou a Morada.

Em abril de 2016, o Parlamento Europeu – em parte motivado por escândalos internacionais de violação daquele direito, envolvendo multinacionais ou agências estatais e cidadãos - adotou e aprovou o RGPD. Depois de um período de transição de dois anos, este entrou em força, a 25 de maio de 2018, para todos os países da União Europeia. Este

tem agora inspirado legislação por todo o mundo, do Canadá, aos EUA ou Índia. Note-se ainda que, apesar de estarmos a falar de um regulamento europeu, este não se aplica apenas às organizações residentes em estados-membros. O que está em causa é qualidade “europeia” dos dados.

O Regulamento, que prevê um conjunto de regras sobre a proteção do direito individual à privacidade, prevê ainda um conjunto de consequências, quando tal não seja feito – as polémicas coimas, que podem chegar aos milhões de euros.

Mas o que aqui está em causa não são as coimas. Aquilo para que apelamos é para as razões, por detrás da sua aplicação. As coimas são aplicadas por tratamento indevido de dados, falta de consentimento ou violação de dados. Dados de milhares de pessoas anónimas que, independentemente de quem sejam, passaram a ter os seus direitos protegidos.

É preciso tomar consciência de que o Regulamento existe para defender os cidadãos e garantir que as entidades que lidam com os seus dados o fazem de forma legítima. Aliás, como nos recorda o RGPD, *o tratamento dos dados pessoais deverá ser concebido para servir as pessoas*.

Os indivíduos precisam de estar conscientes dos perigos, mas também dos direitos que têm e que lhes permitem exigir a proteção que merecem:

Os indivíduos têm direito a saber que dados, para que fim e por quanto tempo estão a ser tratados.

Têm direito a “mudar de ideias”, retirando o seu consentimento, na mesma medida em que o deram. E mais, têm o direito a ser esquecidos.

Têm de ter a garantia de que a informação recolhida, em particular quando em causa estejam dados mais sensíveis, como os genéticos, biométricos ou relativos à saúde, não é utilizada para fins que ameacem, de alguma forma, a sua liberdade ou segurança e bem-estar.

E ainda que, se por algum motivo tiverem os seus dados violados, não só têm de ser informados como podem reagir e ser indemnizados por isso.

O acesso ilegítimo a dados pessoais pode desencadear casos de fraude, extorsão, chantagem ou *bullying* e, ainda, acabar com a reputação de qualquer indivíduo.

Do cruzamento ilegítimo de dados podem ser identificados e, posteriormente, perseguidos determinados grupos/minorias sociais ou agentes vulneráveis, com o intuito de manipulá-los, inflamar a sua opinião, ao ponto de alterar o seu sentido de voto ou incentivar à revolta ou ao crime.

Com a informação certa, pode ser ainda possível aceder a informação confidencial de qualquer tipo de empresa, destruindo negócios de raiz ou, se em causa estiver uma infraestrutura crítica, bloquear os seus serviços, podendo mesmo gerar o caos numa

cidade inteira, região ou país.

As possibilidades são tão ilimitadas quando assustadoras.

Afinal, informação é poder.

Bruno Castro é CEO da VisionWare