RGPD:
UMA REVOLUÇÃO INVISÍVEL

Afonso Araújo Neto[1]
Senior Information Security Consultant, Dognaedis LDA

EXCERTOS

"O que percebe-se agora é que a sociedade colhe as vantagens das novas tecnologias, mas tendo como custo a perda completa do controlo que as pessoas têm sobre seus próprios dados pessoais"

"No novo regulamento, os princípios de segurança *e* privacidade por defeito *são obrigatórios desde a concepção dos serviços, e em tese um serviço que faça tratamento de dados pessoais não pode nem ser oferecido caso não atenda esses requisitos"*

"O RGPD é uma revolução invisível, que se der certo trará benefícios a todos, mas não sem consequências"

"Uma solução de backup *adequada é uma que convence o titular dos dados de que ele tem o seu direito de ser esquecido preservado"*

A Regulamentação Geral sobre a Proteção de Dados (RGPD), Regulamento 2016/679 do Parlamento Europeu, arranca oficialmente a 25 de maio de 2018, e substitui a atual Diretiva de Proteção de Dados 95/46/CE. Superficialmente, tanto o RGPD quanto a diretiva são similares, e buscam os mesmos objetivos. Ainda assim, são os detalhes do RGPD que provavelmente o tornam uma novidade sem precedentes, com possibilidade de impacto ainda não visto no mundo informático e por conseguinte na sociedade. Um impacto com custos altos e mudanças de paradigma, mas que entretanto serão definitivamente benéficos aos cidadãos a longo prazo. Para compreender a natureza desses impactos, é necessário entender-se a natureza das diferenças entre o RGPD e a Diretiva, e também entre o RGPD e a segurança da informação.

Não é novidade que a Diretiva de Proteção de Dados 95/46/CE, Lei 67/98 em Portugal, embora em vigor há 19 anos, tenha impacto muito limitado no dia a dia das pessoas. Muitas nem sabem que a lei existe, ou se sabem, do que ela trata e quais os direitos e deveres ela estabelece. São diversas as razões para esta situação, e a maioria delas pode indiretamente ser atribuída à sociedade que encontrávamos nos anos 1990, quando a diretiva foi criada, e também aos legisladores que a redigiram. Um exemplo bastante simples da mentalidade dos legisladores da época pode ser deduzido do "Considerando" número 2 da própria diretiva, que declara um de seus fundamentos:

> (2) Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos;

Percebe-se pelo texto que a preocupação maior é a de que os sistemas de tratamento de dados, que em última instância serão massivamente informatizados no futuro da época, devem respeitar os "direitos fundamentais das pessoas singulares", mas devem também, antes de mais nada, contribuir para o progresso social. Os direitos

fundamentais a que o texto se refere passam necessariamente pelo artigo 8º da *Convenção Europeia dos Direitos do Homem* de 1950 (direito à privacidade) e pelos artigos 7º e 8º da *Carta dos Direitos Fundamentais da União Europeia* (direito à privacidade de à proteção de dados). De fato, esperava-se progresso, respeito e bom senso.

Os legisladores do século 21, particularmente nos últimos anos, têm outra sociedade em vista. Uma de massiva informatização e de insegurança por defeito, onde a falta de ética e respeito são regulares e esperadas. O tom do discurso passa a ser outro, e no primeiro "Considerando" o RGPD já declara o que passa a ser a linha mestra do novo regulamento:

> (1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental.

Os legisladores sabem que a informatização já foi feita e continua em franca escalada, não existe regresso. O que percebe-se agora é que a sociedade colhe as vantagens das novas tecnologias, mas tendo como custo a perda completa do controlo que as pessoas têm sobre seus próprios dados pessoais. Recuperar este controlo passa a ser o novo objetivo implícito do RGPD, e fundamenta todos os artigos da nova regulamentação. Desta forma fica bastante mais clara a intenção que tem-se quando, no RGPD,

– diminui-se a liberdade dos Estados-membros, ao desenvolver-se um regulamento ao invés de uma diretiva;

– alarga-se a definição dados pessoais, que passam a incluir dados genéticos;

– criam-se novos direitos, como o direito ao apagamento dos dados (ou direito a ser esquecido – Artigo 17), ou o direito de oposição, principalmente a decisões individuais automatizadas (artigos 21 e 22);

– exige-se segurança e privacidade por defeito na concepção de serviços que fazem tratamento de dados pessoais (artigos 25 e 32);

– fornece-se às autoridades de controlo, como a CNPD, o dever de fiscalizar e até aplicar multas às empresas e organizações que não atenderem às exigências (artigo 58).

Hoje ainda percebe-se que a relação de serviços com dados pessoais é essencialmente utilitária, algo como "dá-me isto e eu dou-te aquilo" sem a correta caracterização do escopo e limite. Por exemplo, caso a pessoa necessite algum serviço, a empresa escolhida irá solicitar dados que entender necessários para a sua execução, e o cliente pouco tem a dizer sobre isso. Quando muito, ele será obrigado a assinar um termo de consentimento para o uso de seus próprios dados, mas longe de ser uma proteção para o titular, isto é antes uma proteção para a própria empresa, algo que em última instância tornará o tratamento legal mesmo em caso de litígio. As empresas dirão que, no limite, a pessoa sempre pode recusar o serviço, mas nem sempre isso é possível ou conveniente, especialmente se a empresa possuir boa reputação. A situação é muito pior no âmbito dos serviços públicos, nos quais as pessoas não têm opção de escolha.

Os legisladores sabem que a informatização já foi feita e continua em franca escalada, não existe regresso

Com o RGPD a situação tende a inverter-se, dado que o tratamento de dados pessoais só é autorizado em condições de estrita adequação ao regulamento. No novo regulamento, os princípios de *segurança e privacidade por defeito* são obrigatórios desde a concepção dos serviços, e em tese um serviço que faça tratamento de dados pessoais não pode nem ser oferecido caso não atenda esses requisitos. Neste ponto as Autoridades de Controlo fazem o papel necessário para manter esta adequação e proteger os consumidores, mas é interessante que isto não é a única salvaguarda que o RGPD fornece-nos.

Para além de atender os princípios de segurança, o RGPD no artigo 24 exige que as organizações que façam tratamento de dados possam "*comprovar que o tratamento é realizado em conformidade com o presente regulamento*". Em outras palavras, as organizações são responsáveis por poder comprovar e *demonstrar* esta adequação. O efeito disto é que o regulamento dá o poder a todos os clientes de solicitarem que lhes sejam apresentados evidências de que os seus direitos são atendidos, o que permitiria aos clientes decidirem por outros fornecedores ou procederem a uma denúncia.

Vale ressaltar que o mesmo vale para situações de subcontratação de serviços, na medida em que o contratante passa a ser corresponsável por violações de direitos e vazamento de informações pessoais que envie para tratamento externo. Desta forma, cabe aos contratantes garantir que as subcontratadas atendam ao regulamento, sob pena de serem duplamente penalizados. As evidências de conformidade, como o Registo de Atividades de Tratamento de que fala o Artigo 30, terão papel fundamental no mundo RGPD. A construção deste aporte documental é um ponto crítico do atendimento ao novo regulamento.

O RGPD é uma revolução invisível, que se der certo trará benefícios a todos, mas não sem consequências. E a primeira mudança é na forma de se fazer segurança da informação, que com os ataques informáticos em pleno está à vista de todos como uma necessidade fundamental. Entretanto, devagar, percebe-se que a segurança como a conhecemos não será suficiente.

RGPD e segurança da informação

Pode-se imaginar que o caminho mais rápido para a adequação ao RGPD esteja na simples adequação a práticas de segurança, como por exemplo as sugeridas pela ISO 27001. É verdade que segurança da informação é um pilar fundamental da regulamentação, como já foi apresentado. Entretanto, uma análise detalhada das consequências do novo regulamento traz à tona uma verdade inescapável: muitas das técnicas mais comuns que são utilizadas no mundo da segurança da informação precisam de ajustes para o RGPD ou simplesmente são violações diretas da regulamentação. Em outros casos, a solução de segurança tradicionalmente utilizada simplesmente não é suficiente para atender o que é exigido, e questões adicionais precisam ser identificadas e adequadamente tratadas.

De forma a compreender a questão colocada, veremos como exemplo três estudos de caso onde a segurança da informação não é uma solução automática para o RGPD, e utilizaremos estes casos para discutir as estratégias adequadas.

Primeiro caso. Uma organização de investigação europeia fará uma conferência em um país europeu. Para a inscrição dos participantes será

desenvolvido um site web onde o participante fornece seus dados pessoais para tratamento e pagamento.

Seguindo os preceitos de desenvolvimento seguro e privacidade por defeito, as recomendações de segurança indicam que a comunicação com o site deve ser segura, utilizando provavelmente criptografia SSL e um certificado SSL confiável. O site possui autenticação forte com dois fatores. Os dados pessoais são criptografados antes do armazenamento dos dados. Todos os princípios de desenvolvimento seguro devem ser aplicados ao desenvolvimento do site, e a versão final pode ser testada contra intrusão, de forma manual ou automatizada. A versão final do site pode ser tão segura quanto é possível, e a equipa de segurança dá-se por satisfeita.

A análise sob ótica RGPD demanda outro tipo de avaliação. A primeira preocupação será com direitos simples dos participantes, como o de acesso e retificação, que podem ser implementados através de interfaces simples acedidas pelo próprio utilizador. O direito de ser esquecido demanda uma opção de exclusão do sistema que garantidamente exclua todas as informações pessoais do participante. Aqui, técnicas de anonimização podem ser utilizadas, caso algum resultado agregado seja necessário ser mantido.

O segundo nível de preocupação RGPD diz respeito ao artigo 12, o direito a tratamento transparente. Este item será atendido com um conjunto de preocupações: uma política de privacidade que explique quais dados são coletados e por que, e a adequabilidade e licitude do tratamento relativamente aos princípios do artigo 5, o que levará também a uma definição de por quanto tempo os dados serão armazenados. Caberá ao comité gestor do site que os dados sejam utilizados apenas da forma indicada ao titular, e que o deixe informado de quaisquer novidades no que diz respeito a novos usos que possam ser feitos dos seus dados.

O terceiro e talvez mais complexo ponto de análise do RGPD diz respeito ao capítulo V: as transferências internacionais para países terceiros. Se existe a expectativa de que investigadores de países terceiros participem da conferência (vamos utilizar China como exemplo), um efeito bastante incomum ocorre: a inscrição deste participante ocorre normalmente, porém um novo *login* e acesso aos seus próprios dados

constitui uma transferência internacional para um país terceiro (assumindo-se que ele encontra-se na China). A situação, por absurda que pareça é causada pela proibição da transferência para países que não possuem "nível de proteção adequado" (artigo 45) definido pela Comissão Europeia, situação em que a China se encontra. O RGPD apresenta diversas soluções para a situação, e a busca pela mais adequada depende de um conhecimento aprofundado do capítulo V e dos seus objetivos. Na falta de uma decisão macro para o problema, a solução final passa a ser pontual, e pode ser encontrada no artigo 49 (1)(a), sendo válida apenas se forem tomadas em consideração todas as condições do artigo 7.

Cópias de segurança têm sido fundamentais na recuperação dos ataques promovidos por *ransomwares* que assolaram a Europa e o mundo nos últimos meses

Segundo caso. Backups de sistemas informáticos que contenham informações pessoais.

Desde os primórdios da segurança da informação, a recomendação número um das equipas de segurança para atender a disponibilidade de informações é: "faça e teste regulamente as cópias de segurança de seus sistemas". De fato, cópias de segurança têm sido fundamentais na recuperação dos ataques promovidos por *ransomwares* que assolaram a Europa e o mundo nos últimos meses, como o *Petya* e o *WannaCry*. Entretanto, uma cópia de segurança é justamente isto, cópias dos dados, que, por mais seguras que estejam, dificilmente serão cópias que fazem parte natural do tratamento que o titular de dados espera receber.

A análise RGPD de um procedimento de cópia de segurança tange dois pontos. Primeiro: qual é o parâmetro que define a licitude do tratamento? Este ponto é importante de ser discutido, pois mesmo que não haja necessidade de consentimento por parte dos titulares (o que tornaria um *backup* inviável, dado que ele poderia retirar o consentimento a qualquer momento sem necessariamente desistir do serviço) é direito do titular ser informado sobre o que é feito com seus dados, e isto é inevitável. O segundo ponto é o que tecnicamente é mais complicado: como garantir a exclusão de dados

do titular no caso dele solicitar o seu direito a ser esquecido? Nesta situação, os mecanismos tradicionais de *backup* podem não ser suficientes para atender ao regulamento, dado que a remoção de um único registo de uma quantidade grande de cópias de segurança pode ser essencialmente inviável. Ao mesmo tempo, elas serão sim uma violação da regulamentação, pois serão sempre um meio a partir do qual a organização pode voltar a ter acesso aos dados, não importa as características dos sistemas informáticos envolvidos. Uma solução de *backup* adequada é uma que convence o titular dos dados de que ele tem o seu direito de ser esquecido preservado.

Terceiro caso. O RGPD exige a notificação de violações em até 72 horas caso o risco aos titulares seja alto. Uma invasão em um computador Desktop, que possui uma quantidade elevada de informações pessoais em ficheiros, exige uma perícia forense para a determinação do impacto.

Uma novidade ainda não discutida do RGPD diz respeito à obrigação de notificação à autoridade de proteção de dados em até 72 horas no caso da violação de dados pessoais, quando esta violação "*resultar num risco para os direitos e liberdades das pessoas singulares*". A determinação do grau de risco de uma invasão pode demandar um conhecimento avançado em incidentes de segurança e técnicas de investigação forense. Muitas empresas de segurança informática fornecem serviços de tratamento de incidentes de segurança que podem ser muito úteis no atendimento aos requisitos do artigo 33, e muitos ficarão satisfeitos com um serviço que inclua esta capacidade. Entretanto, como em tudo que diz respeito ao RGPD, isso não é a história toda. Nenhuma das responsabilidades, direitos e deveres são automaticamente removidos em situações de crise como a colocada. Isto significa que uma investigação forense em um Desktop com dados pessoais não deixa de ser um processo de tratamento de dados que deve ser lícito e seguro por defeito. Desta forma, os processamentos de perícia devem idealmente ser formalizados, avaliados, e os titulares devem ser avisados de que isto pode ocorrer mesmo quando seu consentimento não for solicitado.

Considerações finais

Devido à sua natureza e objetivo, o RGPD trará uma miríade de desafios e mudanças no panorama do tratamento de dados pessoais na União Europeia. Após uma longa fase de adequação, que prevemos ir muito além de maio de 2018, o cenário resultante deve ser de muito mais segurança para os titulares dos dados. Finalmente, a noção de que os dados pessoais são propriedade inalienável do seu dono mesmo quando ele os fornece a terceiros para fins de obter um serviço está prestes a tornar-se senso comum. Agora resta aguardar.

Nota

1. Afonso Araújo Neto. Senior Information Security Consultant, Dognaedis LDA.