Notas Leitura / Recensão Crítica

Título: Proteção Dados Pessoais
Site: http://ec.europa.eu/justice/data-protection/
Autor da nota leitura: Henrique São Mamede, Universidade Aberta

Os dados, no geral, estão, no contexto atual, em maior risco que nunca. Todos os dias conseguimos observar notícias relativas a violações de dados - como pode ser visto a partir das estatísticas da *Open Security Foundation*[1], que mostram ter existido 1.472 violações relatadas em 2015. Tal facto demonstra o potencial de se gerar uma enormidade de situações de elevada complexidade, com identidades pessoais roubadas, empresas a terem de repensar o seu próprio negócio e a desistirem das marcas e danos à reputação, que tem sido um motivador de despedimento, até em lugares de topo em grandes organizações.

No que concerne aos encargos financeiros derivados destas violações, um relatório recente da *Grant Thornton*[2] estima o custo, em todo o mundo, em US$ 315 mil milhões. Por organização, o *Ponemon Institute*[3] estima que o custo médio de uma violação de dados terá sido de US$ 3,8 milhões em 2015. E a dimensão da organização não constitui nenhum fator de vantagem, já que organizações de qualquer dimensão podem ser afetadas. De acordo

[1] http://datalossdb.org/
[2] http://www.grantthornton.com/
[3] http://www.ponemon.org/

com a PriceWaterhouseCoopers (PwC)[4], 90% das grandes organizações experimentou uma quebra de segurança em 2015, assim como 74% das pequenas organizações. Embora muito foco seja colocado sobre ataques externos, as ameaças internas também pesam. Os utilizadores dentro do ambiente, supostamente seguro, das organizações não só têm acesso a dados sensíveis, sendo suscetíveis ao erro, como são, frequentemente, alvos de atacantes que procuram portas de entrada para acesso e roubo de informação com elevado valor.

Todos os casos que, quase numa base diária, são noticiados fazem com que exista uma maior sensibilização para o problema, com todas as pessoas a entender que estão sujeitas a vários riscos no espaço digital. Existe, também, uma preocupação em regulamentar e respeitar padrões de indústria e continuamente mostrar as melhores práticas, muitas das quais exigem controlos rigorosos aplicados a dados sensíveis. Cada organização necessita, já hoje, de cumprir leis de proteção de dados, com esta obrigação a crescer no muito curto prazo.

A Proteção de Dados na União Europeia

Os regulamentos de proteção de dados na União Europeia (UE) foram introduzidos há 20 anos, sob a forma de uma diretiva relativa à proteção de dados, que todos os Estados membros ratificaram nas suas próprias leis. Alguns Estados-Membros já tinham alguma forma de legislação nesta área, como é o caso da França. Introduzida em 1978, a sua legislação diz-se ter sido a inspiração para a diretiva relativa à proteção de dados da UE. Após a criação, foi dito que essa diretiva constituía a peça mais rigorosa de legislação de proteção de dados em todo o mundo. Em 1995, uma atualização com nova diretiva destinou-se a unificar a legislação em todo o espaço europeu e a proporcionar a igualdade de condições para as organizações que operam além-fronteiras.

Mas muita coisa mudou nos últimos 20 anos. Em 1995, a utilização massificada da Internet estava na sua infância. De acordo com a *Internet Live Statistics*[5], menos de 1% da população mundial tinha, nessa altura, uma forma de ligação à Internet; hoje, esse número cresceu para cerca de 40%. Segundo o Eurostat[6], em média, 73% das organizações que operam na UE mantêm um sítio web, subindo para 94% na Finlândia e descendo para 42% na Roménia. Na mesma fonte, é indicado que em média, 30% das organizações fazem uso de *social media*, embora isso varie muito de país para país.

A computação em nuvem é também um modelo em ascensão. De acordo com o *Cloud Industry Forum*[7], 84% das empresas no Reino Unido estão utilizando serviços em nuvem e a grande maioria pretende aumentar a sua utilização. Quando as leis de proteção de dados foram introduzidas em toda a UE, não podiam ser previstos desenvolvimentos tais como estes.

Quando a informação é arquivada num armário trancado, é relativamente fácil conseguir a segurança da mesma. À medida que mais e mais dados são transferidos em formato

[4] http://www.pwc.com/
[5] http://www.internetlivestats.com/
[6] http://ec.europa.eu/eurostat
[7] https://www.cloudindustryforum.org/

eletrónico e enviados para os serviços de Internet ou de nuvem, a segurança torna-se mais num problema. E o valor dos dados também se alterou, tornando-se mais valioso - já não é apenas de interesse para os indivíduos ou organizações privadas e os seus concorrentes, mas interessa também a uma gama muito mais ampla de atores, do crime organizado aos estados-nação, para quem esses dados podem gerar informações de enorme valor.

Outro fator que mudou o cenário da tecnologia desde 1995 foi a "consumerização" das tecnologias digitais. Nas organizações, os funcionários exigem cada vez mais terem uma palavra a dizer na escolha dos dispositivos que utilizam, não apenas para lazer, mas também para trabalho. Não só eles desejam usar seus próprios dispositivos, mas também a base de aplicativos em nuvem de sua escolha. Segundo o Eurostat, em toda a Europa, 21% dos indivíduos usam serviços em nuvem para armazenar arquivos - mas os jovens são três vezes mais propensos a usar serviços em nuvem do que aqueles com 55 anos e acima. A *Workshare*[8] concluiu recentemente que os funcionários estão utilizando regularmente aplicações de partilha de ficheiros baseadas na nuvem, mas apenas 28% tinham autorização da organização para fazê-lo. Segundo a *Symantec*[9], através do uso de serviços de partilha de ficheiros não autorizados, 83% das grandes empresas e 70% das PME têm tido informações sensíveis colocados na nuvem sem a supervisão da organização.

A Necessidade de Revisão da Legislação

A espiral ascendente que representa o número de violações de dados nos últimos 20 anos levar à introdução da legislação de notificação de violação de dados obrigatória, nos Estados Unidos da América, começando com a Califórnia em 2003. Atualmente, a maioria dos estados norte-americanos têm alguma forma obrigatória de requisitos de notificação em vigor.

Até agora, não houve uma legislação equivalente em vigor a nível europeu. Para fornecer maior proteção para dados sensíveis dentro de suas fronteiras, muitos Estados-Membros da UE seguiram o seu próprio caminho e reescreveram as suas leis de forma a serem mais abrangentes do que a diretiva da UE. Muitos, inclusivamente, previram o recurso a sanções em caso de violação de dados. Um exemplo é a Espanha, no momento considerado o mais estrito, com multas até 600.000€ impostas por incidente de violação de dados.

Esta situação resultou na existência de uma manta de retalhos de leis de proteção de dados em toda a UE, deixando num espaço cinzento a legislação aplicável a organizações ativas em mais de uma jurisdição.

Outro fator que aumentou a aposta na proteção de dados foi a revelação feita a respeito de vigilância por agências do governo, ostensivamente para fins de segurança nacional. Houve vários instrumentos criados a nível da UE para proteger a transferência de dados dos Estados-Membros da UE para as jurisdições que se considera terem níveis não comparáveis de segurança. A utilização destes instrumentos tem sido interpretada de forma diferente

[8] https://www.workshare.com/
[9] http://www.symantec.com/

pelos Estados-Membros e um dos instrumentos-chave, o uso do contrato de "Porto Seguro"[10], foi recentemente declarado inválido.

O Novo Regulamento de Proteção de Dados da UE

Todos os fatores referidos contribuíram para a perceção de que a legislação relativa a proteção de dados na UE necessitava de ser atualizada. Uma nova legislação, que se baseia na diretiva relativa à proteção de dados de 1995, em vez de reescrevê-la completamente, foi acordada em dezembro de 2015 sob a forma de regulamentação geral de proteção de dados na UE. Espera-se que venha a ser formalmente adotada pelo Parlamento Europeu e pelo Conselho no primeiro semestre de 2016, devendo entrar em vigor no início de 2018. Note-se que, sendo um regulamento ao invés de uma diretiva, os Estados-Membros são obrigados a aderir imediatamente aos requisitos aí definidos.

A intenção não é apenas para criar condições equitativas em toda a UE, mas também incrementar a garantia que as organizações cumprem com as obrigações de proteção de dados. Quando o regulamento entrar em vigor, qualquer organização que colecione, armazene, processe ou partilhe dados de residentes da UE, quer tenham ou não operações na UE, devem estar de acordo com as respetivas exigências.

A definição de dados pessoais foi sempre ampla em termos de legislação na UE, mesmo sem a inclusão da definição de dados pessoais sensíveis. O novo regulamento pretende expandir a definição ainda mais. No novo regulamento, identificadores *online*, tais como endereços IP que poderiam ser utilizados para criar perfis de indivíduos e os para identificar, estarão abrangidos. Portanto, os dados pessoais devem ser considerados como qualquer informação relativa a um indivíduo.

Um benefício para as organizações com operações transfronteiriças será não necessitarem de lidar com a agência de proteção de dados em cada Estado-Membro separadamente. Ao invés, passa a ser estabelecida a oportunidade de lidar apenas com a entidade do país onde estiverem sediados, com a exceção no que respeita a dados sobre empregados. Estima-se que esta medida permitirá economizar para o total das organizações um valor de 2,3 mil milhões de euros por ano.

Esta nova regulamentação, no entanto, impõe também alguns aspetos que podem impactar desfavoravelmente as organizações, em particular as que possuam mais de 250 empregados ou que processem informação relativa a mais de 5.000 indivíduos dentro de um período de doze meses. Estas terão, imperativamente, de nomear um *data protection officer* (DPO). Muitas terão já um *compliance officer*, mas esta nova função é diferente na medida em que o DPO será mais diretamente responsável pela segurança de dados e processos de manipulação dos mesmos.

Para situações de alto risco em relação aos direitos e liberdades dos indivíduos, as organizações terão de realizar avaliações de impacto na proteção de dados. Entre as atividades identificadas pela Comissão Europeia como de alto risco estão o processamento

[10] http://www.export.gov/safeharbor/

de dados que incluam informação sobre a saúde ou raça, a videovigilância pública em larga escala, as informações que envolvam crianças ou os dados genéticos ou biométricos.

Uma outra importante alteração está relacionada com a notificação obrigatória das violações, que muitas organizações vão encontrar como algo particularmente oneroso, já que se espera que notifiquem as autoridades no prazo máximo de 72 horas após a descoberta do problema. Nas situações em que essa violação tenha impacto nos direitos e liberdades das pessoas em causa, esses indivíduos têm de ser notificados sem qualquer demora indevida. Sanções devem também ser fixadas, em níveis elevados em caso de incumprimento, especialmente para violações repetidas. Os avisos podem ser emitidos em situações de primeira ocorrência ou não cumprimento não intencional. Mas, quando uma organização for considerada culpada, podem vir a ser aplicadas multas equivalentes a 4% do volume de negócios global ou 20 milhões de euros, o que for maior, por infrações graves, ou 2% do volume de negócios global ou 10 milhões de euros, o que for maior, por infrações mais pequenas.

A Diretiva para a Segurança de Informação e Redes

Ao mesmo tempo que se alcançava, provisoriamente, o acordo para a regulamentação geral de proteção dos dados, definia-se também a diretiva que contém as primeiras regras de sempre na EU relativas a cibersegurança, as quais vinham a ser defendidas há já algum tempo pelo Parlamento Europeu, sob a forma de diretiva de segurança de informação e de rede. As regras aplicam-se aos prestadores de serviços essenciais, tais como serviços de eletricidade, água, saúde, bancos e transporte, bem como serviços digitais, tais como motores de busca, mercados *online* e computação em nuvem.

Embora não exista ainda muito detalhe disponível acerca do que a diretiva constituirá, o período de implementação deverá cobrir os próximos dois anos. Não foram ainda disponibilizados detalhes relativos a que forma de responsabilidade será imposta a organizações que não tomarem medidas razoáveis para garantir a segurança de suas redes, embora se saiba que a obrigação de declarar violações e incidentes de segurança está incluída. Os incidentes de segurança podem incluir aqueles causados por falhas técnicas, erros involuntários, desastres naturais ou ataques maliciosos.

A Preparação para o Novo Contexto

Uma pesquisa recente realizada pela Vanson Bourne[11] em 300 organizações em França, na Alemanha e no Reino Unido concluiu que 69% dos entrevistados reconhecem que o regulamento de proteção de dados irá afetar os seus negócios, embora 18% afirmem não ter ideia do impacto, apesar do facto de os mesmos armazenam e processam dados. No total, 90% dos entrevistados afirmam que processam e armazenam dados pessoais, e 40% partilham-nos externamente utilizando meios como correio eletrónico, armazenamento portátil e sistema postal. Pouco mais de dois terços estão preocupados com os encargos que o cumprimento do regulamento irá colocar sobre eles.

O novo regulamento geral de proteção de dados especifica que as organizações devem tomar medidas tecnológicas e organizacionais adequadas para proteger os dados, incluindo colocar em vigor controles de privacidade fortes. No mesmo, afirma-se que as organizações

[11] http://www.vansonbourne.com/

devem adotar políticas internas e implementar medidas que vão de encontro aos princípios de proteção de dados por *design* e proteção de dados por defeito.

Tal significa que a proteção de dados e a privacidade devem ser consideradas desde o início do processo de planeamento de segurança. Entre as medidas a serem tomadas estão a minimização da quantidade de dados coletados, as restrições à partilha de dados e a implementação e a adesão a políticas de retenção. Salvaguardas adequadas para proteger os dados incluem criptografia e pseudónimos. O uso de criptografia evita a necessidade de notificação da violação, desde que tenha sido completamente implementada, uma vez que o recurso a este mecanismo torna os dados indecifráveis a qualquer pessoa sem autorização para aceder aos mesmos.

O regulamento introduz também o conceito de pseudónimos. "Pseudonimização" representa o ato de anonimizar o processamento de dados de tal forma que não pode ser atribuído a um indivíduo específico, sem a utilização de informação adicional. Portanto, os dados anonimizados devem ser mantidos separadamente de qualquer informação adicional de modo a garantir a não-atribuição a um indivíduo identificado ou identificável. A criptografia e a anonimização asseguram um dos princípios da proteção de dados que consiste nas proteções de privacidade seguirem os dados, independentemente de onde estes residam e através de todo o seu ciclo-de-vida. Outra garantia forte é a utilização de controlos de acesso adequados e autenticação forte.

Para garantir a segurança contínua dos dados, todos os sistemas devem ser regularmente, se não continuamente, monitorizados e deve ser posto em prática um processo para testar e avaliar a eficácia das medidas técnicas e organizacionais implementadas. Ao avaliar a segurança, as organizações devem ter em conta os riscos associados ao processamento de dados e respetivo armazenamento, incluindo a destruição acidental ou ilícita, a perda, alteração, divulgação não autorizada ou o acesso a dados pessoais.

Para além de tomar medidas como estas, a adesão aos padrões da indústria e melhores práticas irá ajudar as organizações a alcançar a conformidade com o regulamento geral de proteção de dados. Estes incluem PCI DSS, os controles de segurança crítica SANS Top 20, e as normas de segurança da informação ISO 27001 ou ISO 27002. A ISO 27001 ajuda a garantir o princípio consagrado no regulamento que devem ser tomadas medidas técnicas e organizativas adequadas contra o tratamento não autorizado ou ilegal de dados pessoais e contra a perda ou destruição acidental, ou dano de dados pessoais. Este *standard* foi projetado para organizações que desejam conseguir a acreditação para seus sistemas de gestão de segurança da informação. A ISO 27002 fornece um código de práticas em matéria de sistemas de gestão de segurança da informação, mas não fornece acreditação. Num caso de violação de dados, os tribunais provavelmente levarão em consideração a conformidade com um *standard* ISO 27001 ou ISO 27002, como um sinal de que uma organização tem implementadas as necessárias salvaguardas, quando se avalia questões de negligência.

A Utilização de Cifra

O que se pode esperar é a necessidade das organizações terem de fazer investimentos em tecnologia para reduzir o impacto da nova regulamentação de proteção de dados, em geral,

com foco na criptografia e em capacidade analítica e de produção de relatórios na área da segurança. Dado que muitas violações de dados serão motivadas pela descoberta de informações importantes, cifrar todos os dados poderá fazer todo o sentido numa organização.

Isto requer que uma organização possua um inventário das informações que produz, armazena e comunica de modo a que saiba não só o que tem, mas onde e como é armazenado, e que informações são compartilhadas com terceiros tais, como fornecedores. Ao considerar quais dados são confidenciais, uma regra de ouro é tudo o que é feito para ser interno para a organização e qualquer coisa que possa comprometer um indivíduo.

Dados para serem cifrados devem incluir informações estruturadas e não estruturadas, armazenados em bases de dados ou incluídos em folhas de cálculo, documentos de texto, apresentações e arquivos.

Tal como os referidos, também os dados devem ser cifrados quando se movem para fora da organização, seja por colocação dos mesmos na nuvem, seja armazenados e acedidos em dispositivos móveis. Para isso, é vital que as chaves criptográficas permaneçam com a organização, não sendo armazenados na nuvem. Idealmente, as chaves devem ser armazenados num dispositivo com segurança reforçada, através do qual as políticas de criptografia centralizadas podem ser impostas. Isso irá evitar qualquer acesso não autorizado por funcionários de terceiros, como é o caso dos do provedor de nuvem e também irá inviabilizar tentativas das autoridades para exigir o acesso aos dados sem uma base legal forte. Eric Schmidt, presidente da Google, disse abertamente que "a solução para a vigilância do governo é cifrar tudo". O mesmo obviamente, serve para proteger da vigilância *hacker*.

Ao escolher uma solução de criptografia, deve ter-se em consideração que existem diferentes tipos de criptografia que são adequados para diferentes fins. Dados em repouso em servidores ou qualquer tipo de sistema de armazenamento é melhor protegido com criptografia ao nível de arquivo, o que garante que os dados são inacessíveis para os administradores de sistema e que estão protegidos contra ameaças direcionadas e que o acesso de utilizadores pode ser registado e controlado. Para proteger os dados armazenados em bases de dados de acesso por administradores de sistema, devem ser empregues mecanismos criptográficos adicionais, por exemplo na forma de *tokens*, que preservam o formato da informação, mas que mascaram dados sensíveis, tais como cartão de crédito, cartão de identificação e informações sobre contas bancárias, bem como nomes de clientes. Isso vai ajudar muito no sentido de garantir o cumprimento da PCI DSS, bem como os regulamentos que exigem que os dados sensíveis sejam adequadamente protegidos. Para terminais que são facilmente perdidos ou roubados, a criptografia de disco completo está assumindo o lugar de criptografia de nível de pasta e de arquivo/ficheiro. Isso elimina a decisão do utilizador quanto ao facto de necessitar ou não de cifrar dados e não tem qualquer impacto no desempenho do dispositivo, tornando-se transparente para o utilizador. Seja qual for o tipo de criptografia utilizado, deve ser fácil de implementar, sem alterações necessárias para aplicações, e deve fornecer a capacidade de descobrir e criptografar os dados que foram deixados sem cifra.

Apenas a Cifra não Será Suficiente

A criptografia é uma tecnologia extremamente útil para proteger dados e deve ser vista como uma parte estratégica de todo o sistema de segurança implantado por qualquer organização. Esta vai diminuir certamente o impacto de qualquer incidente de segurança que ameaça os dados confidenciais, independentemente se a ameaça vem de fontes internas ou externas, mas não é em si suficiente. Em vez disso, necessita ser apoiada por controlos de acesso que auditam e reportam sobre as autorizações concedidas, e integrada com controlos que fornecem visibilidade sobre os dados sensíveis e que protejam contra as ameaças mais recentes.

Controlos criptográficos de acesso são necessários para garantir que apenas os utilizadores autorizados podem aceder a dados e para controlar o que podem fazer com os mesmos. Mesmo depois de um utilizador ver concedido o acesso a uma chave de criptografia, esse acesso é continuamente controlado, impondo controlos sobre os direitos de usuário para aceder informações, bem como outros fatores como a hora do dia. Eles podem até mesmo impedir um usuário autorizado de fornecer acesso a uma terceira pessoa. A fim de controlar eficazmente o acesso, a integração com o *Active Directory*, ou quaisquer outros diretórios LDAP utilizados pela organização, é uma obrigação.

A integração com sistemas de informações de segurança e gestão de eventos (SIEM) proporciona uma maior visibilidade sobre quem está acedendo o quê e o que estão fazendo com os dados, combinados com outras informações forenses contidas no sistema SIEM. A visibilidade é fundamental quer para garantir a segurança, quer para alcançar e permitir provar conformidade com os regulamentos, o que será especialmente importante tendo em conta as sanções que estarão disponíveis com as novas regras de proteção de dados. Os sistemas SIEM também podem fornecer mais segurança, identificando as questões emergentes em tempo real. Ajudam também na área de auditoria e relatórios de controlos de acesso por meio da correlação e análise de todos os dados de log relacionados.