Update

Momentum

Financeiro e Governance

15 de abril de 2015

NOVAS ORIENTAÇÕES DA EBA SOBRE SEGURANÇA DOS PAGAMENTOS PELA *INTERNET*

Enquadramento

A *European Banking Authority* ("EBA") publicou em 19 de Dezembro de 2014 a versão final das suas *Guidelines on the Security of Internet Payments*. Em Outubro de 2014 a EBA tinha já divulgado no essencial estas orientações, através de uma consulta pública, que se destinava sobretudo a recolher a opinião da indústria quanto ao calendário da respetiva aplicação. Este processo chega agora ao seu termo, através da publicação definitiva das orientações.

A EBA publica estas Orientações ao abrigo do artigo 16.º do Regulamento (UE) N.º 1093/2010 do Parlamento Europeu e do Conselho, de 24 de Novembro de 2010 (sucessivamente alterado: de agora em diante "Regulamento EBA"). Esta norma, recorde-se, atribuiu competência à EBA para emitir orientações e recomendações dirigidas às autoridades competentes ou às instituições financeiras (n.º 1), que devem desenvolver "todos os esforços para [lhes] dar cumprimento" (n.º 3).

Embora estas Orientações não configurem normas jurídicas em sentido estrito, não deixam por isso de ter consequências jurídicas relevantes. Do ponto de vista das autoridades de supervisão, a emissão de uma Orientação da EBA - como é sabido -, gera uma obrigação de reporte: a autoridade deve confirmar se dá ou tenciona dar cumprimento à orientação, indicando as suas razões para o caso de pretender não o fazer (artigo 16.º/3, Regulamento EBA). Mas os efeitos das orientações também se fazem sentir junto das instituições financeiras: o cumprimento ou incumprimento das orientações pode ser um factor

relevante em matéria de responsabilidade civil, sobretudo numa área de prova tão difícil como a da segurança nos pagamentos pela *internet*, como abaixo será analisado em maior detalhe.

As Orientações em apreço baseiam-se em grande medida no trabalho desenvolvido até agora pelo *European Forum on the Security of Retail Payments* ("*SecuRe Pay*"). Este fórum foi constituído em 2011, e configura uma iniciativa de cooperação voluntária entre autoridades de supervisão. Em Janeiro de 2013, e no seguimento do trabalho desenvolvido pelo *SecuRe Pay*, o Banco Central Europeu ("BCE") aprovou e publicou as *Recomendações quanto à segurança dos pagamentos efetuados através da Internet*.

A conversão destas recomendações em Orientações da EBA vem conceder-lhes uma base jurídica mais sólida (entre outros, o artigo 16.º do Regulamento EBA) e assegurar assim uma harmonização das práticas de supervisão no plano europeu.

A publicação das Orientações em apreço, em Dezembro de 2014, surge no contexto mais amplo das negociações sobre a revisão da Diretiva dos Serviços de Pagamento (i.e., da Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de Novembro de 2007: "DSP" ou na abreviatura inglesa "PSD"). Como é sabido, em Julho de 2013 a Comissão apresentou um pacote legislativo que inclui uma proposta de revisão da PSD I (COM(2013) 547 final: a PSD II), mas também uma proposta de um Regulamento relativo às comissões de intercâmbio multilaterais ("CIM", ou em inglês "MIF" de *multilateral interchange fees*) e uma proposta de diretiva sobre contas de pagamento.

Em Março de 2015 foi aprovado o texto do Regulamento relativo às CIM, talvez a mais controversa das três iniciativas legislativas. Aguarda-se a qualquer momento a respetiva publicação.

Nas versões que têm sido divulgadas – a Proposta inicial da Comissão e versão resultante das alterações sugeridas pelo Parlamento Europeu - a DSP II versa também sobre regras de segurança de pagamentos através da *internet*. A EBA entendeu porém que é conveniente antecipar uma regulação mais consistente nesta matéria, atendendo aos elevados níveis de fraude que ainda se fazem sentir nos pagamentos através da internet. Assim sendo, as Orientações agora aprovadas devem ser adoptadas por todos os prestadores de serviços de pagamento ("PSP") a partir de Agosto de 2015, sendo certo que

as autoridades de supervisão devem confirmar se tencionam ou não dar-lhes cumprimento no prazo de 2 meses após a publicação das traduções da versão final, publicada em inglês, em Dezembro de 2014.

Recorde-se que a DSP I já estabelece no artigo 10.º/4 que as instituições de pagamento devem dispor "procedimentos eficazes de identificação, gestão, controlo e comunicação dos riscos a que está ou possa vir a estar exposta e mecanismos adequados de controlo interno, designadamente procedimentos administrativos e contabilísticos sólidos (...) proporcionados relativamente à natureza, escala e complexidade dos serviços de pagamento prestados".

As Orientações da EBA

As Orientações em apreço aplicam-se à prestação de serviços de pagamento através da *internet*, independentemente do dispositivo utilizado para o acesso (cartões, moeda eletrónica, *online banking*). Um dos principais aspectos consiste na obrigatoriedade de adopção e revisão periódica pelos prestadores de serviços de pagamento (PSP) de uma política explícita de segurança relativa à segurança nos serviços de pagamento prestados pela *internet*. Esta política deve constar de um documento, aprovado pela direção de topo do PSP, e deve conter os objetivos em matéria de risco, assim como atribuir competências e responsabilidades neste contexto (Título II, n.º 1).

As Orientações agora analisadas também recomendam a realização periódica de avaliações de risco pelos PSP, para aferir o risco subjacente aos sistemas e serviços que pretendem implementar, assim como para monitorizar o risco dos sistemas e serviços em funcionamento (Título II, n.º 2). Outros deveres similares são dignos de nota: (a) dever de monitorizar e reportar incidentes de segurança; (b) dever de adoptar metodologias para mitigar o risco detetado nas suas operações de *online banking*; (c) dever de assegurar a rastreabilidade das transações realizadas na *internet*.

Um dos aspectos centrais das Orientações prende-se com a autenticação dos clientes, entendida como o processo de verificação da identidade do cliente pelo PSP. A realização de pagamentos através da *internet* – assim como o acesso através da *internet* a dados sensíveis sobre pagamentos realizados - apenas deve ser desencadeada após uma autenticação robusta do cliente (*strong customer*

authentication) pelo PSP. Segundo as Orientações, uma autenticação robusta do cliente consiste num processo baseado em pelo menos dois dos seguintes elementos:

i) **[Conhecimento]** Alguma coisa que apenas o cliente conhece (ex. palavra passe, código, números de cartões de identificação);

ii) **[Posse]** Alguma coisa que apenas o cliente tem (ex. cartão de coordenadas, *smartphone*);

iii) **[Inerência]** Alguma coisa que o cliente é (ex. dados biométricos).

Para que o processo de autenticação possa ser qualificado como robusto, os elementos utilizados devem ser independentes, no sentido em que o acesso por terceiros a um deles não deve colocar em causa a confidencialidade dos demais. Por outro lado, um dos elementos de conhecimento ou posse deve ser não-reutilizável e não-replicável.

As Orientações contêm muitas outras indicações e recomendações úteis em matéria de segurança de pagamentos realizados através da *internet*. O renovado estatuto jurídico destas Orientações permite concluir que, a partir de agora, terão uma relevância também crescente na aferição do grau de cumprimento pelos PSP dos deveres gerais decorrentes da DSP, em matéria de segurança na prestação de serviços de pagamento. Esta relevância é tanto mais importante numa altura em que também cresce o número de litígios entre clientes e PSP que chegam aos tribunais portugueses, e que têm como pano de fundo uma ou mais perturbações na utilização de serviços de pagamento através da *internet*.

Francisco Mendes Correia
fco@servulo.com

Rua Garrett, n.º 64 1200-204 Lisboa - Portugal Tel: (+351) 21 093 30 00 Fax: (+351) 21 093 30 01/02
geral@servulo.com www.servulo.com