Qual a importância do Regulamento eIDAS na mitigação do ciber-risco?

Nas últimas décadas, temos vindo a testemunhar uma evolução tecnológica constante, influenciando as mais diversas esferas da sociedade, designadamente a nossa forma de comunicar, de trabalhar, de aprender ou de pensar.

Hoje em dia, as organizações procuram acelerar a sua transformação digital, através de tecnologias disruptivas que oferecem diversas vantagens competitivas, para além de se apresentarem também como soluções que reduzem o impacto ambiental das diversas atividades económicas.

Apesar da transformação digital se apresentar como algo fundamental para a evolução de qualquer organização, esta também traz consigo novos desafios, nomeadamente o inevitável incremento do ciber-risco. É neste contexto que pretendemos explorar o papel que o Regulamento eIDAS pode desempenhar como ferramenta regulatória para a mitigação do ciber-risco. Pese embora tal diploma já se encontre em vigor há alguns anos, verifica-se a existência de um grande desconhecimento sobre os instrumentos que foram introduzidos por este. Mas comecemos pelo início.

O Regulamento n.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014, comummente conhecido como Regulamento eIDAS, entrou em vigor com o intuito de criar um quadro jurídico comum a toda a União Europeia, permitindo reforçar a confiança nas transações eletrónicas no mercado interno, através da criação das condições necessárias para o reconhecimento mútuo de tecnologias facilitadoras. Tal como preconiza o Decreto-Lei n.º 12/2021, que assegura a execução na ordem jurídica interna do Regulamento eIDAS: "*A adoção do Regulamento teve como objetivo aumentar a confiança e segurança das transações online na União Europeia*". Esta clareza regulatória - bem como o estabelecimento de normas técnicas exigentes para as comunicações eletrónicas no mercado único europeu -, apresenta-se como fundamental para a mitigação do ciber-risco.

Para este efeito, o Regulamento eIDAS apresentou três elementos essenciais:

- Introdução dos **Prestadores Qualificados de Serviços de Confiança** – como é o caso da **DigitalSign**;
- **Uniformização das assinaturas eletrónicas qualificadas e selos eletrónicos qualificados** no mercado interno;
- Introdução do **serviço qualificado de validação de assinaturas eletrónicas qualificadas**.

Os **Prestadores Qualificados de Serviços de Confiança** são devidamente credenciados pelas entidades supervisoras, sendo obrigados a cumprir os requisitos estabelecidos pelo Regulamento eIDAS, de modo a fornecerem serviços qualificados, tal como a emissão de assinaturas eletrónicas qualificadas ou o fornecimento de um serviço qualificado de validação de assinaturas eletrónicas qualificadas. Por esta razão, são fundamentais para criar e reforçar a confiança nas transações eletrónicas em todos os Estados-Membros.

Ademais, o Regulamento eIDAS veio estabelecer os pressupostos para a emissão de assinaturas eletrónicas qualificadas, bem como selos eletrónicos qualificados, permitindo a uniformização das mesmas no espaço da União Europeia. Destarte, uma assinatura eletrónica qualificada emitida num determinado Estado-Membro terá de ser reconhecida em todos os outros Estados-Membros, com um efeito equivalente ao de uma assinatura manuscrita, tal como preconiza o número 3, do artigo 25.º do Regulamento eIDAS. Da mesma forma, se um selo eletrónico qualificado for emitido por um determinado Estado-Membro, terá de ser reconhecido por todos os outros como tal, conforme resulta do número 3 do artigo 35.º do referido Regulamento.

Deste modo, conclui-se que apenas é possível emitir uma determinada assinatura eletrónica qualificada em conformidade quando esta respeite os requisitos previstos pelo Regulamento eIDAS. Perante tudo isto, é fundamental dispor de ferramentas capazes de demonstrar se uma determinada assinatura eletrónica qualificada é válida ou não. Devido à tecnologia adjacente à criação e aposição das assinaturas eletrónicas qualificadas, a verificação da validade de uma assinatura eletrónica qualificada difere, naturalmente, do modo de verificação da validade de uma assinatura manuscrita.

Por esta razão, o Regulamento eIDAS introduziu – através do seu artigo 33.º - o **serviço qualificado de validação de assinaturas eletrónicas qualificadas**. Este serviço procede à validação de assinaturas eletrónicas qualificadas ou selos eletrónicos qualificados, ou seja, permite verificar se uma determinada assinatura eletrónica qualificada foi emitida de acordo com os requisitos estabelecidos no Regulamento eIDAS, tal como consagra o artigo 32.º do mesmo Regulamento.

A DigitalSign, enquanto Prestador Qualificado de Serviços de Confiança, criou o DS Verify, – **um serviço qualificado de validação de assinaturas eletrónicas qualificas ou selos eletrónicos qualificados** – que, tal como mencionado *supra*, permite verificar se uma determinada assinatura eletrónica qualificada cumpre efetivamente os requisitos aplicáveis à validade das assinaturas eletrónicas qualificadas.

A conjugação destes três elementos introduzidos pelo Regulamento eIDAS é fundamental para a mitigação do ciber-risco, uma vez que os Prestadores Qualificados de Serviços de Confiança atuam como terceira parte de confiança, através da emissão de assinaturas eletrónicas qualificadas e selos eletrónicos qualificados aos diversos agentes do mercado e, para além disso, fornecem ainda serviços qualificados de validação de assinaturas eletrónicas qualificadas, que permitem a esses agentes verificarem a autenticidade de um determinado documento eletrónico, através da validação das assinaturas eletrónicas qualificadas que lhe são apostas.

Podemos então concluir que a mitigação do ciber-risco apenas será possível caso se verifique o recurso a ambos os instrumentos:

- Aposição de uma assinatura eletrónica qualificada ou selo eletrónico qualificado a um determinado documento eletrónico;
- Recurso a um serviço qualificado de validação de assinaturas eletrónicas qualificadas.

Em suma, é consabido que a desmaterialização dos processos físicos permite que as organizações operem de uma forma mais célere, ágil, económica e sustentável. **Todavia, é fulcral que a transformação digital seja realizada de modo eficiente e, acima de tudo, de forma segura.** Tal como se deixou claro na presente exposição, o recurso às ferramentas previstas no Regulamento eIDAS permite o estabelecimento de controlos de gestão de todo o tipo de documentos eletrónicos recebidos por parte de uma determinada organização, nomeadamente através da definição de quais os tipos de assinaturas eletrónicas que devem ser utilizadas/aceites em cada um dos processos desmaterializados. Para além disso, o recurso a serviços qualificados de validação possibilita aferir se uma assinatura eletrónica aposta a um determinado documento eletrónico é, ou não, qualificada, o que, por sua vez, permite às organizações assegurarem a autenticidade dos documentos eletrónicos por si recebidos, sendo este um processo essencial para todas as organizações no que diz respeito à Cibersegurança.

Exemplo da Faturação Eletrónica

A faturação eletrónica é um caso paradigmático nas comunicações eletrónicas, onde a garantia da autenticidade da mesma, através da aposição de um certificado digital qualificado, e a sua consequente validação, apresentam-se como fundamentais para mitigar o ciber-risco de qualquer organização.

Em abril de 2023, era publicada a notícia de que o FC Porto e o Anderlecht, dois clubes conhecidos do panorama europeu, tinham sido alvos de uma burla informática, em cerca de 90 mil euros e 500 mil euros respetivamente. De acordo com esta notícia, o ataque informático realizou-se através de um "*man-in-the-middle*", que consiste na interceção das comunicações eletrónicas entre as partes e na posterior alteração das mesmas pelo atacante, sem que os alvos da interceção se apercebam. Ora, foi exatamente isto que aconteceu no caso em concreto: os atacantes obtiveram acesso a faturas eletrónicas que se encontravam ainda por pagar, alteraram os dados das mesmas e, por fim, receberam o pagamento indevido por parte dos dois clubes.

Esta ocorrência teria sido evitada caso estas organizações tivessem implementado processos de controlo de gestão de documentos eletrónicos. Perante os factos acima descritos, nenhuma das

organizações verificou se a fatura eletrónica rececionada era, de facto, autêntica. **Por outras palavras, nenhuma das organizações supramencionadas recorreu a um serviço qualificado de validação de assinaturas eletrónicas qualificadas para verificar se o documento eletrónico - no caso, a fatura eletrónica - se encontrava devidamente assinado por uma assinatura eletrónica qualificada ou selo eletrónico qualificado, garantindo assim a autenticidade da origem e a integridade do conteúdo da fatura eletrónica.**

Apesar de a obrigatoriedade da aposição de um certificado digital qualificado à emissão de faturas eletrónicas apenas entrar em vigor em janeiro de 2024, fruto dos constantes adiamentos efetuados pelo Governo português, **é fundamental que se garanta a autenticidade da fatura eletrónica emitida, bem como a posterior verificação da autenticidade da origem e a integridade da referida fatura eletrónica por parte do destinatário.**