CYBER RESILIENCE ACT: DA COOPERAÇÃO EUROPEIA AO RISCO DE EXPOSIÇÃO

Foto de edgeZodge media na Unsplash

POR RITA SOUSA E SILVA

DA COOPERAÇÃO ENTRE ESTADOS-MEMBROS AO AUMENTO DO RISCO DE EXPOSIÇÃO, O CYBER RESILIENCE ACT TEM ESTADO NO CENTRO DO DEBATE SOBRE A SEGURANÇA DIGITAL. AO MESMO TEMPO, A REGULAÇÃO RIGOROSA DA UE CONTINUA A LEVANTAR PREOCUPAÇÕES SOBRE A COMPETITIVIDADE EUROPEIA.

O Regulamento Ciber-Resiliência – em inglês, *Cyber Resilience Act* (CRA) – é uma das peças do puzzle regulatório europeu, que demonstra o esforço da União Europeia (UE) em reforçar a segurança num mundo digital em constante mudança.

No entanto, a intenção de fomentar a cooperação europeia poderá invés colocar os Estados-membros numa situação vulnerável à espionagem governamental e ao aumento do risco de exposição, com a partilha de vulnerabilidades ativamente exploradas prevista na proposta de lei.

A par disto, a mão pesada dos reguladores europeus continua a levantar preocupações sobre os custos significativos de *compliance* e possíveis perturbações na cadeia de abastecimento, bem como o forte impacto no desenvolvimento e atualização de software.

PRODUTOS DIGITAIS SEGUROS

A ciber-resiliência integra o conceito abrangente de cibersegurança e reporta-se à "capacidade de resposta e recuperação da organização em caso de ocorrência de ciberincidente", começa por enquadrar Margarida Leitão Nogueira, Sócia da DLA Piper.

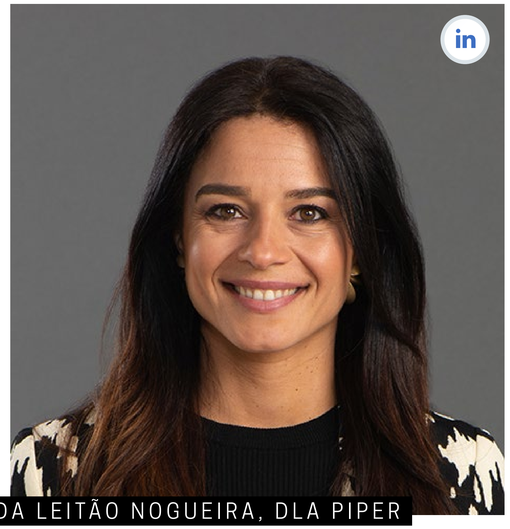
Apesar do nome atribuído, o Regulamento Ciber-Resiliência apresenta-se como uma proposta regulatória mais ampla. O projeto de lei estabelece requisitos de cibersegurança para a conceção, desenvolvimento e disponibilização no mercado de produtos com elementos digitais, procurando torná-los "menos permeáveis a ciberataques" e, ao mesmo tempo, "prestar aos consumidores informação transparente", explica a advogada.

Os últimos anos têm sido marcados por "diversas ocorrências de falhas graves na cibersegurança de soluções e produto", que "levam ao comprometimento de sistemas críticos e/ou divulgação não autorizada de dados pessoais", sublinha Pedro Rodrigues,

CISO do Banco de Portugal, referindo a existência de "casos em que vulnerabilidades de segurança deitam por terra esforços considerados na proteção de dados pessoais".

No final de novembro de 2023, o Conselho e o Parlamento Europeu chegaram a acordo sobre a proposta de lei. O texto regulatório irá aplicar-se a todos os produtos que estão "ligados direta ou indiretamente a outro dispositivo ou a uma rede", de acordo com o Conselho.

"Os produtos com elementos digitais podem representar riscos significativos para a cibersegurança, uma vez que são utilizados por todos os cidadãos da UE para realizar atividades quotidianas", afirma a Agência Europeia para a Segurança das Redes e da Informação (ENISA). "Um simples modem de Internet pode permitir que terceiros intercetem os sites que visitamos ou interrompam a nossa ligação à Internet, uma impressora Wi-Fi pode armazenar o nome dos ficheiros que imprimimos ou o nosso portátil pode usar um sensor de impressão digital



MARGARIDA LEITÃO NOGUEIRA, DLA PIPER

que possa aceitar mais impressões digitais do que as que configurámos inicialmente".

De acordo com o estudo "*NIS Investments*" de 2022 da ENISA, 69% dos operadores de serviços essenciais (OES) e prestadores de serviços digitais (DSP) na UE "indicaram que a maioria dos seus incidentes de segurança da informação são causados pela exploração de vulnerabilidades em software ou hardware produtos", revela a agência europeia.

A CIBER-RESILIÊNCIA INTEGRA O CONCEITO ABRANGENTE DE CIBERSEGURANÇA E REPORTA-SE À "CAPACIDADE DE RESPOSTA E RECUPERAÇÃO DA ORGANIZAÇÃO EM CASO DE OCORRÊNCIA DE CIBERINCIDENTE"

MARGARIDA LEITÃO NOGUEIRA, SÓCIA DA DLA PIPER

Além disto, "56% dos OES e DSP na UE concordam que requisitos comuns levariam a custos mais baixos de mitigação de riscos para os utilizadores e 61% concordam que requisitos comuns reduziriam o número de incidentes de segurança e, como resultado, o custo de gestão e recuperação de tais incidentes", acrescenta a ENISA.

Entre as várias medidas, a proposta do Regulamento Ciber-resiliência estipula a obrigação da comunicação de vulnerabilidades exploradas ativamente e a determinação da vida útil prevista do produto pelos fabricantes, sendo indicado um período de suporte de pelo menos cinco anos, à exceção dos produtos cuja utilização estará sujeita a um tempo mais curto.

COOPERAÇÃO OU RISCO DE EXPOSIÇÃO?

O artigo 11.º do CRA tem sido alvo de duras críticas por exigir aos fabricantes de software a notificação às CSIRT sobre as vulnerabilidades ativamente exploradas no prazo de 24 horas após a sua observação, estando ou não disponível uma correção. As vulnerabilidades de segurança seriam divulgadas numa base de dados da UE desenvolvida e mantida pela ENISA.

As preocupações prendem-se com o facto de "o conhecimento decorrente da divulgação de vulnerabilidades não corrigidas poder ser aproveitado por agentes com propósitos maliciosos, gerando, consequentemente, novos riscos em matéria de cibersegurança que ponham em causa a segurança dos produtos e respetivos utilizadores", aponta Margarida Leitão Nogueira.

Uma vez que 24 horas não é muito tempo para corrigir, testar e implementar *updates* de software, muitas falhas de segurança permaneceriam sem correção – ou com correções "desleixadas" – no momento da notificação. Assim, o CRA poderá criar "a possibilidade de uma base de dados de vulnerabilidades que essas autoridades podem explorar, levando ao receio de espionagem ou monitorização indevida da sua atividade", alerta Pedro Rodrigues.

Uma rápida divulgação das vulnerabilidades exploradas poderia igualmente prejudicar o trabalho dos investigadores de segurança, especialmente tendo em conta a sua coordenação com fornecedores para desenvolver *patches* de segurança. Neste contexto, é necessário "encontrar um ponto de equilíbrio entre a obrigação das organizações divulgarem vulnerabilidades nos seus sistemas, o que as força a procurar uma correção, e o tempo necessário para desenvolver a correção dessas vulnerabilidades, o que também cria pressão sobre os fornecedores para atuarem rapidamente", considera Pedro Rodrigues.

Sobre esta questão, a ENISA realça que "é importante esclarecer que o CRA se refere a notificações de vulnerabilidades exploradas ativamente. Se uma vulnerabilidade for explorada ativamente, já existem várias partes cientes dos detalhes (e das explorações), enquanto as partes menos propensas a saber são os próprios utilizadores".

Desta forma, a agência europeia acredita que esta medida "aumentará a consciencialização sobre as vulnerabilidades e permitirá que os utilizadores façam as suas próprias avaliações de risco", assegurando que, "mesmo que um patch ainda não este-


PEDRO RODRIGUES, BANCO DE PORTUGAL

ja disponível, outras ações poderão ser executadas, incluindo soluções alternativas e aplicação de controlos de compensação – até mesmo desconectando completamente a componente vulnerável".

Por sua vez, o Centro Nacional de Cibersegurança (CNCS) considera que "a partilha de informação sobre vulnerabilidades entre congéneres promove, decisivamente, a cooperação entre Estados-membros, na garantia da ciber-resiliência e permite uma ação mais rápida e eficaz por parte das Autoridades nacionais", frisando que "a notificação de vulnerabilidades não pressupõe a sua imediata publicitação pública".

Para o CISO do Banco de Portugal, "algumas das sugestões de alteração ao artigo 11º do CRA incluem a garantia de que essa informação não seria utilizada pelas autoridades ou mesmo alterar esta obrigação para que apenas cubra vulnerabilidades com correção disponível".

Ademais, a comunidade de software open-source tem-se mostrado receosa face às obrigações impostas pelo CRA aos developers de software, que deverão corrigir as falhas de segurança identificadas, implementar atualizações de software e validar dispositivos e programas de software atempadamente.

Gerardo Lisboa, Presidente da Associação de Empresas de Software Open Source Portuguesas (ESOP), destaca a "questão dos tempos de resposta que carecem de proporcionalidade face à dimensão da oferta comercial", definidos "independentemente do grau de vulnerabilidade em causa, ao arrepio das melhores práticas estabelecidas no setor

> OS ÚLTIMOS ANOS TÊM SIDO MARCADOS POR "DIVERSAS OCORRÊNCIAS DE FALHAS GRAVES NA CIBERSEGURANÇA DE SOLUÇÕES E PRODUTO", QUE "LEVAM AO COMPROMETIMENTO DE SISTEMAS CRÍTICOS E/OU DIVULGAÇÃO NÃO AUTORIZADA DE DADOS PESSOAIS"
>
> PEDRO RODRIGUES, CISO DO BANCO DE PORTUGAL

> "ESTAS MEDIDAS DE CERTIFICAÇÃO E A NECESSIDADE DE SER COMPROVADO QUE OS PRODUTOS SÃO SEGUROS PARA SEREM COLOCADOS NO MERCADO PODEM, DE FACTO, IMPACTAR A COLOCAÇÃO DESSES PRODUTOS E A INOVAÇÃO NUM PRIMEIRO MOMENTO".
>
> EDUARDO MAGRANI, CONSULTOR SÉNIOR DA ÁREA DE TECNOLOGIAS, MEDIA E TELECOMUNICAÇÕES DA CCA LAW FIRM

e definidas por normas internacionais globalmente aceites".

PERTURBAÇÃO NA *SUPPLY CHAIN*

Empresas europeias como a Ericsson e a Nokia alertaram para o impacto da nova regulação europeia na cadeia de abastecimento, considerando que a aplicação de normas comuns de cibersegurança aos dispositivos conectados poderá resultar numa forte perturbação.

Para vender um produto com elementos digitais abrangido pelo CRA, os fornecedores devem demonstrar *compliance*, pelo que é necessário algum tipo de processo de certificação. Numa carta enviada através do grupo DigitalEurope, os signatários argumentaram que a UE não dispõe atualmente da capacidade necessária para certificar produtos e componentes em tempo útil, o que poderá causar atrasos na disponibilidade para venda aos consumidores europeus.

"Dado o amplo âmbito do CRA e a falta de capacidade, enfrentamos uma situação em que os produtos seguros não podem ser colocados no mercado e serão bloqueados para clientes da UE. A Europa não pode atualmente oferecer tantas avaliações de conformidade, criando estrangulamentos, uma vez que os fabricantes devem provar a conformidade através de certificadores terceiros", escreveram os remetentes. "Corremos o risco de criar um bloqueio ao estilo da Covid nas cadeias de abastecimento europeias, perturbando o mercado único e prejudicando

EDUARDO MAGRANI, CCA LAW FIRM

a nossa competitividade".

Eduardo Magrani, Consultor Sénior da área de Tecnologias, Media e Telecomunicações da CCA Law Firm corrobora que "estas medidas de certificação e a necessidade de ser comprovado que os produtos são seguros para serem colocados no mercado podem, de facto, impactar a colocação desses produtos e a inovação num primeiro momento". No entanto, "posteriormente, o objetivo é que haja um processo já adaptado para que essa regulação não represente tantos entraves futuramente".

"O aumento de regulação tem demonstrado uma inevitável introdução de perdas de produtividade e aumento dos tempos de entrega, qualquer que seja a indústria", acrescenta Gerardo Lisboa. "Não será diferente aqui".

Além disto, sublinha-se que os utilizadores finais poderão enfrentar "preços mais elevados dos produtos com elementos digitais", diz o CNCS, com base no estudo da avaliação de impacto da proposta do CRA, elaborado pela Comissão Europeia. No entanto, "os consumidores e os cidadãos vão beneficiar, de igual modo, de uma melhor proteção dos seus direitos fundamentais, tais como a privacidade e a proteção de dados".

Para Pedro Rodrigues, "um dos maiores desafios [da implementação do Regulamento Ciber-resiliência], senão o maior, será a capacidade para gestão dos sistemas legados". O CISO do Banco de Portugal afirma que "esta é já uma realidade, mas será necessário perceber de que forma o CRA conseguirá alterar este panorama ou se se irá aplicar alguma limitação à identificação e comunicação de vulnerabilidades em produtos digitais cujo ciclo de vida já terminou".

O PREÇO DA CONFORMIDADE

A proposta do Regulamento Ciber-resiliência assenta numa mudança profunda dos processos de conceção, desenvolvimento e produção de produtos com elementos digitais, que serão marcados pela "implementação de um padrão de segurança *by design*", refere Margarida Leitão Nogueira. Consequentemente, "é expectável que a adaptação e cumprimento dos requisitos legais neste contexto

comportem custos significativos para as organizações e que parte dos mesmos possa vir a repercutir-se nos consumidores".

Os recursos humanos qualificados serão essenciais para garantir a conformidade com as novas normas regulatórias, podendo representar custos adicionais. "As organizações terão de rever os seus processos de gestão de vulnerabilidades e reforçar as suas equipas de forma a poderem não só acompanhar o ciclo de identificação e correção de vulnerabilidades, mas também desenhar e implementar requisitos de segurança mais efetivos na aquisição de produtos digitais, aumentando a sua exigência perante os fornecedores destes produtos", afirma Pedro Rodrigues.

De acordo com o Conselho Europeu, as novas medidas regulatórias serão aplicadas três anos após a entrada em vigor da lei, "o que deverá dar aos fabricantes tempo suficiente para se adaptarem aos novos requisitos".

O Conselho adianta também que "foram acordadas medidas de apoio adicionais para pequenas e microempresas, incluindo atividades específicas de sensibilização e formação, bem como apoio a procedimentos de ensaio e avaliação da compliance".

"As entidades vão ter de se preocupar de uma forma mais estrita com mitigadores de risco, relatórios de impacto, monitorização dos ciberataques e preparação de comunicação às autoridades – todas essas medidas têm custo inerente", indica Eduardo Magrani, salientando que as organizações "vão ter de dedicar um *budget* específico para esse tipo de compliance e isso exige um nível de maturidade que nem todas as empresas têm".

Segundo o estudo da avaliação de impacto do CRA, prevê-se "um aumento dos custos diretos de conformidade com os novos requisitos de cibersegurança, avaliação da conformidade, documentação e obrigações de comunicação de informações", no que diz respeito aos developers de software e fabricantes de hardware, indica o CNCS.

Contudo, "estes custos poderão ser compensados por benefícios que resultam da redução dos problemas de segurança tradicionalmente inerentes a estes produtos e serviços", refere. A par disto, o estudo em questão estima que o CRA resultará na "redução dos custos dos incidentes que afetam as empresas, em cerca de 180 a 290 mil milhões de euros por ano", para toda a UE.

As PME "vão ser, em princípio, mais afetadas do que as grandes empresas que, normalmente, têm melhores economias de escala e uma maior sensibilização para a cibersegurança", diz o CNCS. Em contraste, destaca os benefícios relacionados com "a cibersegurança integrada em produtos com elementos digitais", que "vai representar uma poupança de custos significativa para as PME, na sua qualidade de utilizadores".

Ainda assim, a conformidade poderá acarretar um preço demasiado elevado para algumas empresas. "As obrigações em termos de processo e certificação para produtos de base tecnológica não estarão ao alcance de muitas pequenas e médias organizações, que serão obrigadas a fechar portas, deixando o lugar vago para as grandes corporações", acredita Gerardo Lisboa. ◀