Cerejeira Namora Marinho Falcão
an auren member firm

Privacidade, Digital e Tecnologia

Cyber Resilience Act

No passado dia 10 de Dezembro, entrou em vigor o Regulamento (EU) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de Outubro de 2024, relativo aos requisitos horizontais dos produtos com elementos digitais – *Cyber Resilience Act* (CRA).
Este instrumento legislativo altera os regulamentos (EU) n.º 168/2013 e (EU) 2019/1020 e a Diretiva (EU) 2020/1828 **e estabelece requisitos abrangentes de cibersegurança para todos os produtos de *hardware* e *software* com elementos digitais que são comercializados na União Europeia.**

Legal Update

DEZ 2024

shaping the **future**

A crescente digitalização, dependência e interconectividade dos dispositivos disponibilizados no mercado evidenciou as fragilidades da anterior legislação que não previa a obrigatoriedade de implementar medidas de segurança nos produtos com elementos digitais.

De facto, só é possível garantir a cibersegurança de toda a cadeia de fornecimento dos produtos disponíveis no mercado interno se a totalidade dos seus componentes estiver protegida contra ciberameaças.

Para atingir esse objectivo, a Comissão considerou fundamental a implementação de um *framework* susceptível de abranger a segurança em toda a cadeia de fornecimento, desde os fornecedores iniciais até ao consumidor final.

Nessa medida, todos os operadores económicos têm agora a responsabilidade de assegurar a cibersegurança dos produtos, através da fiscalização dos "blocos" que lhe precedem; isto é, cada operador económico deve verificar a conformidade dos operadores anteriores, garantindo, assim, que não se perde o rastro da conformidade (e responsabilidade) com a cibersegurança dos produtos com elementos digitais.

Foi neste contexto que surgiu o ***Cyber Resilience Act,*** prevendo:

- Os produtos devem ser concebidos, desenvolvidos e produzidos de modo a garantir um nível adequado de cibersegurança. Especificamente, devem ser concebidos de forma a reduzir o impacto de incidentes, utilizando mecanismos e técnicas de atenuação da exploração de eventuais vulnerabilidades – complementariamente, estes devem ser concebidos de forma a limitar possíveis superfícies de ataque.
- Os produtos devem ser disponibilizados no mercado sem nenhuma vulnerabilidade conhecida.
- Assegurar que as vulnerabilidades possam ser corrigidas através de atualizações de segurança.
- Assegurar, por defeito, que existem mecanismos de protecção contra o acesso não autorizado, como sistemas de autenticação, identidade ou gestão de acessos.
- Minimizar o impacto negativo pelos próprios produtos ou dispositivos conectados na disponibilidade de serviços prestados por outros dispositivos ou redes.

I. Âmbito de aplicação e principais obrigações dos operadores económicos

O *Cyber Resilience Act* aplica-se a todos os produtos com elementos digitais disponibilizados no mercado da UE, desde produtos de consumo, como dispositivos de *IoT* ("*Internet of Things*") a sistemas de *software* industriais.

Exceptuam-se do seu âmbito de aplicação os seguintes produtos:

- Produtos sujeitos a regulamentações específicas da UE, como dispositivos médicos, veículos motorizados, aviação;
- Peças de reposição;
- Produtos desenvolvidos, ou modificados, exclusivamente para fins de defesa ou segurança nacional;
- Produtos desenvolvidos especificamente para o tratamento de informações confidenciais.

O Regulamento prevê requisitos e obrigações específicas tendo em conta o tipo de produtos e o tipo de operador económico.

Tipo de produtos
Quanto aos produtos, classificam-se em:

i. Produtos importantes –os produtos são classificados como importantes, caso desempenhem funções relacionadas com a protecção de redes e sistemas, ou que possam causar danos significativos caso falhem. Esta classificação distingue-se em dois subgrupos, consoante o nível de risco:

- **Classe I –** incluem sistemas de gestão de identidade, *web browsers*, gestores de palavras-passe, sistemas operativos e *routers*.
- **Classe II –** por exemplo, *software* como *containers*, *virtual machines*, sistemas de detecção e prevenção de intrusões, microprocessadores e microcontroladores

ii. Produtos críticos – os dispostivos de *hardware* com caixas de segurança, pontos de acesso para contadores inteligente e dispositivos para fins avançados de segurança (p. ex.: o cripto processamento de ligações de dispositivos em rede).

iii. Produtos não críticos – como *softwares* de edição fotográfica, processamento de texto, videojogos.

2. Operadores económicos
Relativamente aos operadores económicos abrangidos, o CRA autonomiza três categorias, prevendo obrigações específicas para cada uma delas conforme o seu papel e função na suplly chain.

i. Fabricantes
Devido ao papel crucial dos fabricantes no design e produção de *hardware* e *software*, o *Cyber Resilience Act* impõe um conjunto alargado de obrigações que abrangem todo o ciclo de vida do produto, que se resumem nos seguintes pontos:

- Na fase de desenvolvimento do produto, assegurar que o produto é concebido e produzido em conformidade com os requisitos gerais de cibersegurança
- Efectuar uma avaliação dos riscos de cibersegurança associados a um produto com elementos digitais antes da sua introdução no mercado da UE, verificando que os requisitos estabelecidos pelo *Cyber Resilience Act* foram cumpridos;
- Criar a documentação técnica, informações e instruções para os utilizadores.
- Notificação de incidentes ("vulnerabilidades activamente exploradas" e "incidentes graves") à European Union Agency For Security (ENISA) e à Computer Security Incident Response Team (CSIRT), por meio de uma plataforma única de incidentes.

ii. Importadores
Os importadores desempenham um papel essencial no que diz respeito à introdução de produtos no mercado da UE provenientes de fabricantes estabelecidos em países terceiros.

Estes operadores são essencialmente responsáveis por:

- Garantir que os produtos que estão a ser comercializados são seguros e cumprem os requisitos de cibersegurança;
- Cooperar com as autoridades competentes em caso de investigações;
- Verificar se as exigências essenciais para os fabricantes, ao abrigo do presente Regulamento, foram cumpridas – como a realização de uma avaliação de riscos, ou a existência de documentação técnica.

iii. Distribuidores
Estes operadores económicos devem verificar se o produto com elementos digitais ostenta a marcação CE antes de o disponibilizarem no mercado da EU bem como garantir que os fabricantes e os importadores cumpriram as obrigações estabelecidas no CRA.

Fiscalização e sanções
A implementação do regulamento será supervisionada pela Agência Europeia para a Cibersegurança (ENISA), que prestará orientação e apoio aos Estados-Membros na definição e operação das autoridades nacionais.

Cada Estado-Membro será responsável pela nomeação das autoridades nacionais incumbidas de monitorizar a aplicação dos requisitos de cibersegurança, devendo estas ter a capacidade de aplicar de forma eficaz as exigências de cibersegurança e de realizar as avaliações necessárias de conformidade. A responsabilidade pela aplicação das sanções é atribuída às autoridades nacionais de fiscalização de mercado, as quais terão, adicionalmente, a competência para:

- Monitorizar o cumprimento das regras;
- Ordenar a remoção de produtos não conformes do mercado; e
- Coordenar acções com entidades europeias de fiscalização.

Embora, em Portugal, a autoridade nacional responsável pela cibersegurança seja o Centro Nacional de Cibersegurança (CNCS), até ao momento, ainda não foi determinado se esta será a entidade incumbida de assegurar o cumprimento das obrigações previstas no presente Regulamento.

No que respeita ao quadro sancionatório e ao montante das coimas, o CRA determina o seguinte:
Incumprimento dos requisitos essenciais de cibersegurança: Até 15 000 000 EUR ou, no caso de empresas, até 2,5% do volume de negócios anual total a nível mundial referente ao exercício no ano anterior, consoante o que for mais elevado;

Incumprimento ou não conformidade com os demais requisitos do *Cyber Resilience Act:* Até 10 000 000 EUR ou, no caso de empresas, até 2% do volume de negócios anual total a nível mundial referente ao exercício no ano anterior, consoante o que for mais elevado;

Prestação de informações incorrectas, incompletas, ou falsas, às autoridades de fiscalização: Até 5 000 000 EUR ou, no caso de empresas, até 1% do volume de negócios anual total a nível mundial referente ao exercício no ano anterior, consoante o que for mais elevado.

Notas finais

O Cyber *Resilience Act* entrou plenamente em vigor no passado 10 de Dezembro de 2024, contudo, a maior das disposições só será aplicável a partir de 11 de Dezembro de 2027, tendo em conta o período de adaptação que o Regulamento prevê, para que os operadores económicos se ajustem aos novos requisitos.

Assim as normas referentes às obrigações de informações dos fabricantes, são aplicáveis a partir de 11 de Setembro de 2026; e o Capítulo IV do CRA, relativo às notificações das avaliações de conformidade, será aplicável a partir de 11 de junho de 2026.

A implementação do *Cyber Resilience Act* apresenta desafios consideráveis para as empresas, especialmente para pequenas e médias empresas (PMEs).

Com o objetivo de apoiar a implementação do Regulamento, a Comissão irá emitir orientações específicas destinadas às PMEs. Ademais, conforme já referido, as empresas beneficiarão de um período de transição, permitindo-lhes realizar as adaptações necessárias para que os produtos atualmente comercializados estejam em conformidade com os novos requisitos estabelecidos pelo CRA.