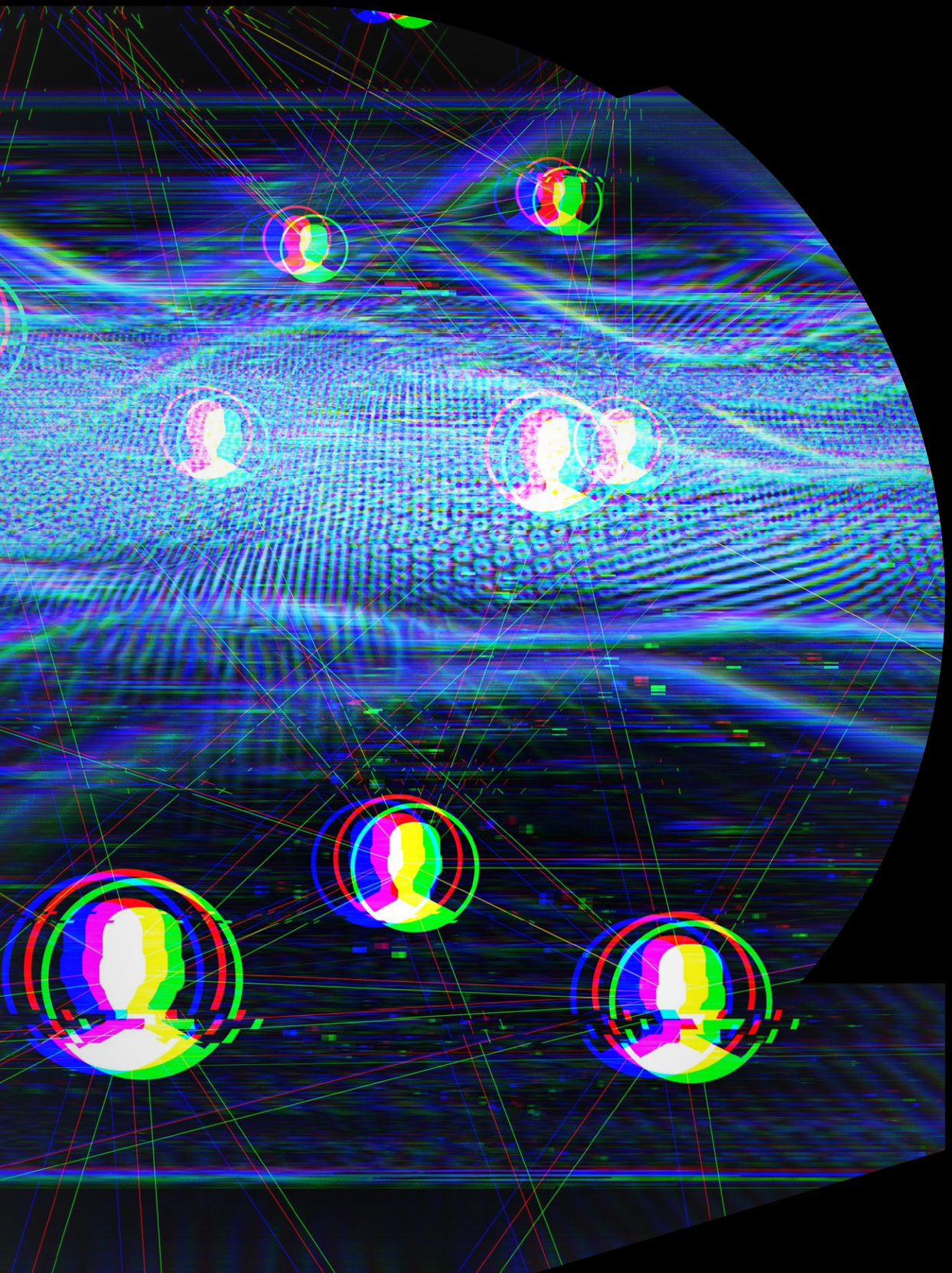
Cyber Resilience Act

Segurança Cibernética na Economia Digital

Transformative Legal Experts

PLMJ



Índice

Introdução

A crescente digitalização da economia trouxe inúmeros benefícios, mas também aumentou a exposição a riscos cibernéticos e a violações de dados pessoais na União Europeia. Para enfrentar esses desafios, a UE adotou o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho[1], relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais (doravante "*Cyber Resilience Act*" ou "Regulamento"), publicado a 20 de novembro de 2024.

Este regime representa um reforço do funcionamento do mercado interno, estabelecendo um regime jurídico uniforme para os requisitos essenciais de cibersegurança aplicáveis à colocação de produtos com elementos digitais no mercado da União.

1. Objetivos do Cyber Resilience Act

A necessidade de uma regulamentação robusta de cibersegurança tornou-se evidente com o aumento dos ataques cibernéticos, que afetam não só a economia, como também a segurança e a saúde dos consumidores.

O *Cyber Resilience Act* visa garantir a cibersegurança dos produtos com elementos digitais, estabelecendo condições-limite para o desenvolvimento de produtos com elementos digitais seguros, ao assegurar que sejam colocados no mercado produtos de *hardware* e *software* com menos vulnerabilidades e que os fabricantes encarem a segurança com seriedade ao longo de todo o ciclo de vida de um produto.

Neste contexto, pretende-se:

- **Melhorar a segurança dos produtos digitais**:
  Garantindo que os produtos sejam desenvolvidos e produzidos com um nível adequado de cibersegurança.

- **Proteger os consumidores e as empresas**:
  Reduzindo a vulnerabilidade a ataques cibernéticos e salvaguardando dados pessoais e corporativos.

- **Harmonizar o funcionamento mercado interno**:
  Estabelecendo requisitos uniformes que facilitem a livre circulação de produtos seguros dentro da UE.

- **Garantir proporcionalidade para as micro, pequenas e médias empresas**:
  Criando condições mais viáveis para os operadores económicos que desejam entrar no mercado da União.

A necessidade de uma regulamentação robusta de cibersegurança tornou-se evidente com o aumento dos ataques cibernéticos.

1 Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência)

2. Âmbito de aplicação e entrada em vigor

O *Cyber Resilience Act* abrange uma ampla gama de produtos com elementos digitais[2] comercializados na UE, desde dispositivos de IoT ("*Internet of Things*") a sistemas de *software* complexos. Todavia, não se aplicará a:

- Produtos cobertos por outros atos jurídicos da União, entre eles, Regulamento (UE) 2017/745 (Dispositivos Médicos), Regulamento (UE) 2017/746 (Dispositivos Médicos para Diagnóstico In Vitro) e Regulamento (UE) 2019/2144 (Requisitos de Homologação de Veículos);
- Produtos certificados ao abrigo do Regulamento (UE) 2018/1139;
- Equipamentos marítimos abrangidos pela Diretiva (UE) 2014/90;
- Peças sobresselentes disponibilizadas no mercado para substituir componentes idênticos em produtos com elementos digitais e fabricadas de acordo com especificações iguais às dos componentes que se destinam a substituir;
- Produtos desenvolvidos ou alterados exclusivamente para fins de defesa ou segurança nacional, ou especificamente concebidos para o tratamento de informações classificadas.

O Regulamento entrou em vigor a 10 de dezembro de 2024, e será aplicável na sua totalidade a partir de 11 de dezembro de 2027. No entanto, para assegurar uma transição suave e a garantir que os operadores económicos e as autoridades de fiscalização do mercado estarão preparados, algumas obrigações serão aplicáveis a partir de 2026, nomeadamente:

- As obrigações previstas no capítulo IV (Artigo 35.º a 51.º), relativas ao processo de notificação e implementação dos organismos de avaliação da conformidade pelos Estados-Membros, aplicáveis a partir 11 de junho de 2026,
- As obrigações previstas no artigo 14.º, referentes à comunicação, pelos fabricantes, de vulnerabilidades ativamente exploradas e incidentes graves com impacto na segurança dos produtos com elementos digitais, aplicáveis a partir de 11 de setembro de 2026.

O Cyber Resilience Act abrange uma ampla gama de produtos com elementos digitais comercializados na UE.

2 Nos termos do artigo 3.º n.º 1 do *Cyber Resilience Act*, um produto com elementos digitais corresponde a "um produto de software ou hardware e as suas soluções de tratamento remoto de dados, incluindo componentes de software ou hardware que sejam colocados no mercado separadamente".

▲ VOLTAR AO INÍCIO

3. Requisitos e obrigações a cumprir pelos operadores económicos

Nos termos do *Cyber Resilience Act*, os operadores económicos[3] a ele sujeitos devem observar um conjunto significativo de regras no que respeita aos requisitos a incorporar nos produtos com elementos digitais que pretendam comercializar no espaço da União.

3.1. REQUISITOS ESSENCIAIS DE CIBERSEGURANÇA

Relativamente aos produtos com elementos digitais, os operadores económicos devem assegurar o cumprimento dos seguintes requisitos:

- Os produtos devem ser concebidos, desenvolvidos e produzidos de modo a garantir um nível adequado de cibersegurança.
- As vulnerabilidades devem ser resolvidas através de atualizações de segurança e os produtos devem ser disponibilizados sem vulnerabilidades conhecidas.
- Os requisitos específicos devem incluir a proteção contra o acesso não autorizado, a confidencialidade e integridade dos dados, assim como a resistência contra os possíveis ataques aos serviços.

As obrigações variam em função da natureza dos operadores intervenientes na cadeia de abastecimento.

3.2. OBRIGAÇÕES DOS OPERADORES ECONÓMICOS

Os vários operadores económicos ver-se-ão sujeitos a obrigações específicas, que visam assegurar que os produtos com elementos digitais são confiáveis e cumprem as várias imposições do *Cyber Resilience Act*.

De salientar que as obrigações a observar variam em função da natureza dos operadores intervenientes na cadeia de abastecimento, conforme detalhado abaixo. Assim:

a)Fabricantes

Entre as diversas medidas que devem adotar, destacam-se a obrigação de:

i) Promover avaliações rigorosas de cada produto por forma a que se torne possível identificar e antecipar vulnerabilidades;

ii) Colocar à disposição dos utilizadores e das autoridades de fiscalização do mercado as informações e instruções previstas no Anexo II, durante, pelo menos, 10 anos após a disponibilização do produto, ou durante o período de suporte, consoante o prazo mais longo;

iii) Implementar processos que permitem identificar situações de vulnerabilidades ao longo do ciclo de vida do produto, como por exemplo, fornecer atualizações de segurança[4];

iv) Verificar que os produtos possuem a marcação CE, para garantir que um produto com elementos digitais e os processos por si aplicados estão em conformidade com os requisitos essenciais de cibersegurança constantes do Anexo I e de outra legislação de harmonização da União aplicável que preveja a sua aposição.

3 Nos termos do n.º 12 do artigo 3.º do *Cyber Resilience Act*, os operadores económicos são "o fabricante, o mandatário, o importador, o distribuidor ou outra pessoa singular ou coletiva sujeita a obrigações relacionadas com o fabrico de produtos com elementos digitais ou com a disponibilização de produtos com elementos digitais no mercado".

4 Nos termos previsto no considerando 59, "a fim de garantir a segurança dos produtos com elementos digitais após a sua colocação no mercado, os fabricantes deverão determinar o período de apoio, que deverá refletir o tempo previsto para a utilização do produto com elementos digitais. Ao determinar um período de apoio, o fabricante deverá ter em conta, em especial, as expectativas razoáveis dos utilizadores, a natureza do produto, bem como a legislação pertinente da União que determina a vida útil dos produtos com elementos digitais".

b) Importadores e Distribuidores

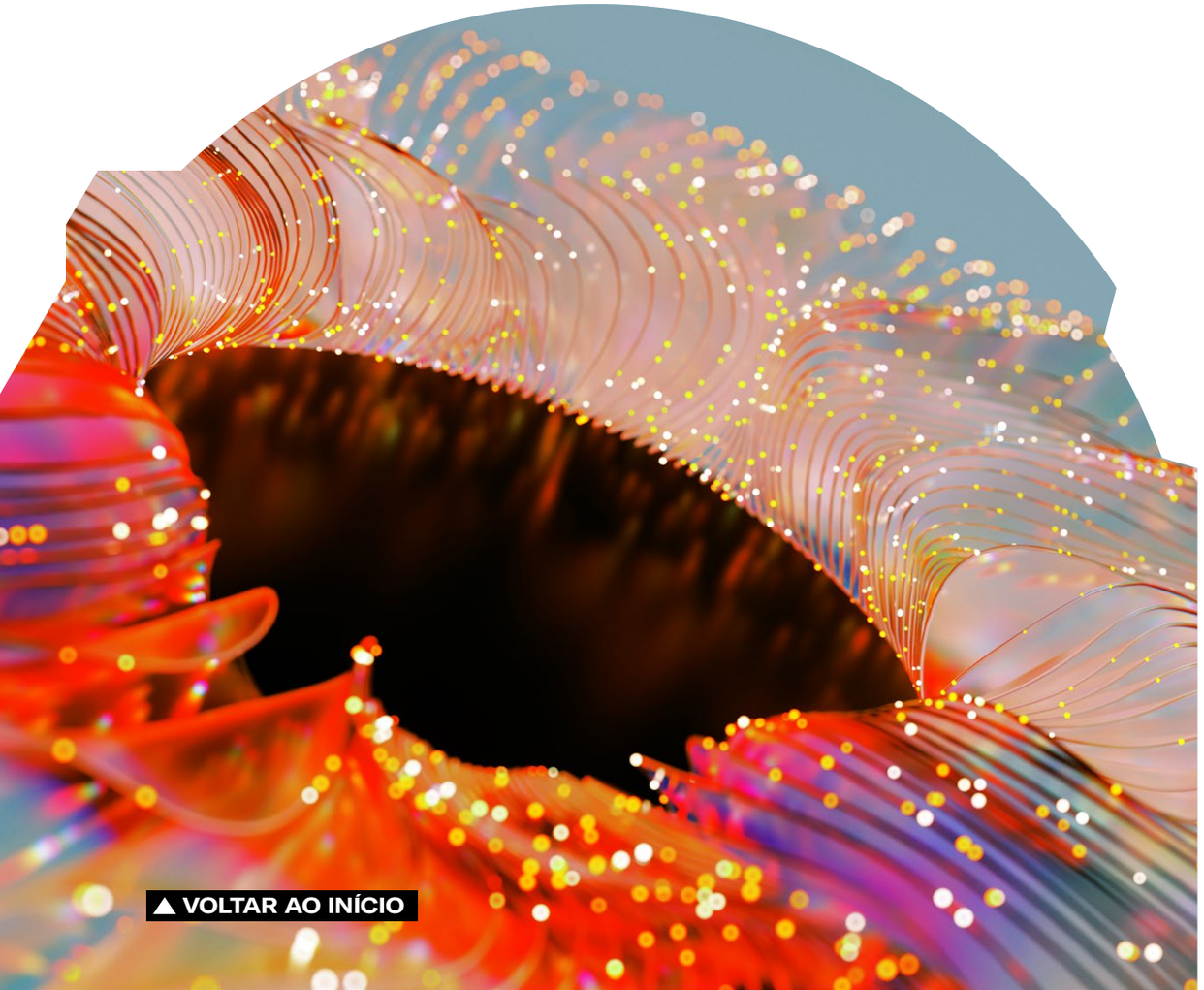
Estes operadores são essencialmente responsáveis por:

i) Garantir que os produtos que estão a ser comercializados são seguros e cumprem as regras de cibersegurança;

ii) Preservar e manter a documentação necessária para demonstrar a conformidade dos produtos ao longo do seu tempo de vida;

iii) Cooperar com as autoridades competentes em caso de investigações;

iv) Adotar medidas corretivas se identificarem produtos não conformes.



▲ VOLTAR AO INÍCIO

4. Implementação nos Estados-Membros

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

Cada Estado-Membro será responsável por designar as autoridades nacionais que irão supervisionar a aplicação dos requisitos de cibersegurança, devendo estas ser capazes de aplicar eficazmente os requisitos de cibersegurança e de realizar avaliações de conformidade.

Os Estados-Membros poderão designar autoridades pré-existentes ou constituir novas autoridades para supervisionar a aplicação do *Cyber Resilience Act*. A decisão dependerá dos recursos disponíveis e da capacidade das autoridades atuais para cumprir os novos requisitos.

Pese embora em Portugal a autoridade nacional responsável pela cibersegurança seja o Centro Nacional de Cibersegurança (CNCS), até à data os organismos governamentais portugueses ainda não definiram se será esta a entidade responsável pelo cumprimento das obrigações previstas neste Regulamento.

Cada Estado-Membro será responsável por designar as autoridades nacionais que irão supervisionar a aplicação dos requisitos de cibersegurança.

5. Incidentes e obrigações de comunicação

Todas as notificações devem ser feitas à rede de Equipas de Respostas a Incidentes de Segurança Informática ("CSIRT"), designada como coordenadora, e à ENISA, por via da plataforma única de comunicação gerida pela ENISA[5].

> Os fabricantes têm diferentes prazos de notificação consoante o tipo de vulnerabilidade e incidentes verificados.

Vulnerabilidades Ativamente Exploradas

i) **Alerta Precoce:** Notificar dentro de 24 horas após descobrir a vulnerabilidade;

ii) **Notificação de Vulnerabilidade**: Enviar detalhes dentro de 72 horas, incluindo informações sobre a vulnerabilidade e medidas corretivas;

iii) **Relatório Final**: Fornecer um relatório detalhado dentro de 14 dias após implementar uma medida corretiva.

Incidentes Graves[6]

i) **Alerta Precoce**: Notificar dentro de 24 horas após descobrir o incidente, incluindo suspeitas de atos ilícitos;

ii) **Notificação de Incidente**: Enviar detalhes dentro de 72 horas, incluindo informações sobre o incidente e medidas corretivas,

iii) **Relatório Final**: Fornecer um relatório detalhado dentro de um mês após a notificação inicial.

Estes requisitos de notificação visam garantir maior transparência, respostas mais céleres e fomentar a colaboração entre a ENISA e o CSIRT.

Para além da notificação ao CSIRT e à ENISA, os fabricantes devem informar os utilizadores afetados sobre vulnerabilidades ou incidentes graves, fornecendo pormenores necessários sobre os riscos e as medidas de atenuação adotadas.

6. Confidencialidade e sanções

6.1. CONFIDENCIALIDADE

A confidencialidade é uma preocupação central no Regulamento, na medida em que este visa garantir a proteção de informações e dados sensíveis dados obtidos no contexto da sua aplicação.

5 Ao abrigo do considerando 71, "quando os fabricantes notificam uma vulnerabilidade ativamente explorada ou um incidente grave com impacto na segurança do produto com elementos digitais, deverão indicar quão sensíveis consideram ser as informações notificadas".

6 Critérios de classificação dos Incidentes Graves: (i) afetam a capacidade de proteger dados ou funções sensíveis e, (ii) introduzem ou executam códigos maliciosos no sistema do produto com elementos digitais.

Ao abrigo do *Cyber Resilience Act*, todas as partes envolvidas devem manter a confidencialidade das informações, especialmente durante inspeções, investigações e auditorias. As informações trocadas entre as autoridades de fiscalização e a Comissão não podem ser divulgadas sem consentimento prévio.

Além disso, a Comissão e os Estados-Membros podem partilhar informações sensíveis com autoridades de outros países, desde que existam acordos de confidencialidade que garantam a proteção adequada da informação partilhada.

Estas medidas são essenciais para acautelar direitos de propriedade intelectual, segredos comerciais e a segurança pública e nacional.

6.2. SANÇÕES

O Regulamento exige que sejam os Estados-Membros a estabelecer as suas próprias regras relativas às sanções, em caso de incumprimento. O quadro sancionatório e os montantes das coimas a definir pelos Estados-Membros deverão ser efetivos, proporcionais e dissuasores. Neste contexto, os Estados-Membros devem definir um quadro que preveja:

- Incumprimento dos requisitos essenciais de cibersegurança: coimas até EUR 15 milhões ou em 2,5% do volume de negócios anual ou total a nível mundial do infrator, consoante o montante mais elevado;

- Incumprimento das obrigações gerais: coimas até EUR 10 milhões ou 2% do volume de negócios anual total a nível mundial do infrator, consoante o montante mais elevado;

- Prestação de falsas informações: coimas até EUR 5 milhões.

▲ VOLTAR AO INÍCIO

O quadro sancionatório e os montantes das coimas a definir pelos Estados-Membros deverão ser efetivos, proporcionais e dissuasores

7. Desafios e oportunidades para as empresas

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

- **Custos de conformidade:**
  Os fabricantes terão de fazer investimentos para cumprir os novos requisitos de cibersegurança, como por exemplo em processos de desenvolvimento mais seguros e em sistemas de monitorização de vulnerabilidades.

- **Complexidade técnica**:
  A produção de produtos que cumpram com os critérios de segurança implica a necessidade de criar e manter os sistemas de segurança avançados, bem como o recurso a especialistas nesta área.

No entanto, surgem oportunidades significativas:

- **Inovação**:
  Os requisitos impostos pelo Regulamento irão incentivar as empresas a inovar e a procurar desenvolver novas tecnologias e soluções de segurança.

- **Vantagem competitiva**:
  As empresas que adotem práticas robustas de cibersegurança poderão destacar-se no mercado, uma vez que produtos mais seguros aumentarão a confiança dos consumidores nos produtos digitais que utilizam.

Para facilitar a implementação do Regulamento, a Comissão irá emitir orientações[7] particularmente direcionadas às pequenas e médias empresas. Além disso, as empresas beneficiarão de um período de transição, de modo a implementarem as alterações necessárias para adaptar os produtos que já comercializam aos novos requisitos impostos pelo regulamento.

> As empresas beneficiarão de um período de transição, de modo a implementarem as alterações necessárias para adaptar os produtos que já comercializam.

Atualmente já se verifica, por parte de algumas empresas em setores altamente regulados e sensíveis à cibersegurança, a adoção proativa de medidas para garantirem que os seus produtos são seguros. Com efeito, existem empresas que já implementaram medidas que passam por atualizações de software OTA (*Over-The-Air*) e implementação de programas incentivadores de report de bugs de segurança pelos utilizadores dos produtos. Espera-se que o *Cyber Resilience Act* fomente a disseminação destas práticas por mais empresas, mas não venha colocar entraves ao desenvolvimento do mercado da UE, na medida em que o mercado só beneficia com o compromisso e preocupação contínuos dos operadores económicos com a segurança e a inovação.

7 Nos termos do considerando 53, a Comissão e as organizações europeias de normalização deverão ter em conta o Regulamento (UE) 2023/1230, "na preparação e elaboração de normas harmonizadas para facilitar a aplicação do Regulamento (UE) 2023/1230 no que diz respeito, em especial, aos aspetos de cibersegurança relacionados com a proteção contra a corrupção e a segurança e fiabilidade dos sistemas de comando estabelecidos nas secções 1.1.9 e 1.2.1 do anexo III do referido regulamento".

Sobre a PLMJ

→ Quem somos

"PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us."

CLIENT REFERENCE FROM
CHAMBERS AND PARTNERS

Sobre a área de Tecnologia, Media e Telecomunicações

→ O que fazemos

KEY CONTACTS

Pedro Lomba
Sócio

(+351) 213 197 412
pedro.lomba@plmj.pt

Nádia da Costa Ribeiro
Consultora sénior

(+351) 213 197 412
nadia.costaribeiro@plmj.pt

Rita de Sousa Costa
Associada

(+351) 213 197 560
rita.desousacosta@plmj.pt

▲ VOLTAR AO INÍCIO

Dezembro 2024

www.plmj.com