ASSEMBLEIA DA REPÚBLICA

2021PORTUGAL.EU
Dimensão Parlamentar

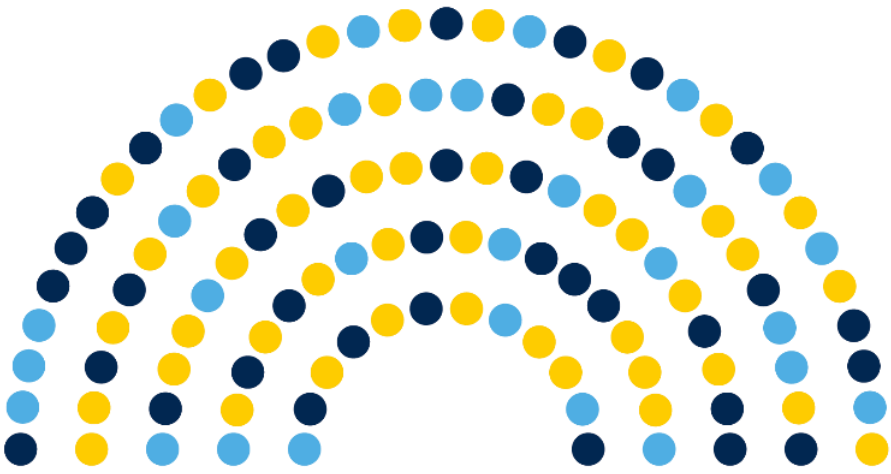
Nota de Enquadramento

Cibercriminalidade e resiliência digital

8.ª Reunião do Grupo Especializado de Controlo Parlamentar Conjunto da Agência da União Europeia para a Cooperação Policial (Europol)

1-2 de fevereiro de 2021

Portugal



NOTA DE ENQUADRAMENTO

Cibercriminalidade e resiliência digital

- **Cibersegurança**

Numa Europa digital e conectada, a cibersegurança é uma das principais prioridades da Comissão[1]. Em 16 de dezembro de 2020, a Comissão apresentou a nova Estratégia da UE para a Cibersegurança, componente fundamental da Comunicação Construir o futuro digital da Europa, do Plano de Recuperação para a Europa e da Estratégia da UE para a União da Segurança, cujo objetivo é reforçar a resiliência coletiva da Europa contra as ciberameaças e ajudar a garantir que todos os cidadãos e as empresas possam beneficiar plenamente de serviços e ferramentas digitais seguros e fiáveis[2], mantendo o ciberespaço aberto estável e seguro.

A nova **Estratégia para a Cibersegurança** permite igualmente à União Europeia (EU) reforçar o seu papel de liderança em matéria de regras e normas internacionais no domínio do ciberespaço, apresentando propostas concretas de iniciativas de regulamentação, de investimento e de ação em três domínios de intervenção da UE: (1) **Resiliência, soberania tecnológica e liderança**, designadamente prevendo o lançamento, a nível da UE, de uma rede de centros de operações de segurança baseados na inteligência artificial (IA), que constituirá um verdadeiro «escudo para a cibersegurança» a nível europeu, capaz de detetar sinais de um ciberataque com antecedência suficiente e de permitir uma ação proativa; (2) **Reforço da capacidade operacional para prevenir, dissuadir e reagir,** através da preparação de uma nova ciberunidade conjunta (Joint Cyber Unit) a fim de reforçar a cooperação entre os organismos da UE e as autoridades nacionais responsáveis pela prevenção, dissuasão e resposta a ciberataques, nomeadamente as comunidades civis, policiais, diplomáticas e de ciberdefesa; (3) e **promoção de um ciberespaço à escala mundial aberto graças a uma maior cooperação,** intensificando a colaboração com os parceiros internacionais com vista a reforçar a ordem internacional assente em regras, promover a segurança e a estabilidade internacionais no ciberespaço.

[1] A cibersegurança é uma prioridade que também se reflete no próximo orçamento de longo prazo da União Europeia (2021-2027). Além de que os Estados-Membros são incentivados a utilizar plenamente o Mecanismo de Recuperação e Resiliência da UE para impulsionar a cibersegurança.

[2] Mais informações no comunicado de imprensa e no documento com perguntas e respostas.

Ao mesmo tempo, apresentou propostas para abordar a ciber-resiliência e a resiliência física das redes e das entidades críticas, com uma proposta de diretiva relativa às medidas destinadas a assegurar um elevado nível comum de cibersegurança em toda a União (Diretiva SRI revista) e uma nova diretiva relativa à resiliência das entidades críticas[1].

Os Estados-Membros são, ainda, incentivados a concluir a aplicação do conjunto de instrumentos da UE para a cibersegurança das redes 5G (riscos para a segurança das redes 5G e das gerações de redes futuras).

- **Combate ao cibercrime**

Especificamente, em matéria de **combate ao cibercrime**, que afeta cidadãos, negócios e organizações por toda a UE, o papel da Agência da União Europeia para a Cooperação Policial **(Europol)** é fundamental na oferta de soluções inovadoras e apoio eficaz e abrangente às investigações[2].

A Europol criou o **Centro Europeu da Cibercriminalidade (EC3)** em 2013 para fortalecer a resposta da aplicação da lei ao cibercrime na UE e, assim, ajudar a proteger cidadãos, empresas e governos europeus de crimes *online*, crimes que, pela sua própria natureza, não têm fronteiras nem jurisdições. Esta unidade foi concebida para fornecer essa especialização enquanto centro agregador de conhecimentos e informação, nomeadamente para apoio operacional e de peritagem forense no quadro de investigações penais, bem como através da sua capacidade para mobilizar todos os recursos relevantes nos Estados-Membros visando mitigar, reduzir a ameaça dos criminosos informáticos, independentemente do local onde se encontrem, e promover soluções à escala da UE.

[1] Ficha informativa: Diretiva revista relativa à segurança das redes e da informação (SRI2).
[2] O Europol Review [Relatório Geral sobre as Atividades da Europol], de periodicidade anual, que dá conta dos resultados e contém informações específicas sobre os tipos de funcionalidades e de sistemas à disposição da Europol, a partir dos quais presta um apoio coordenado às operações policiais em toda a Europa e, por vezes, em territórios mais longínquos.

A ação do EC3 incide, no essencial, sobre atividades em linha ilegais exercidas por grupos de criminalidade organizada, especialmente os ataques dirigidos contra operações bancárias em linha e outras atividades financeiras em linha, a exploração sexual de menores na *Internet* e os crimes que afetam as infraestruturas críticas e os sistema de informação na UE.

Todos os anos, o EC3 publica a Avaliação de Ameaças ao Crime Organizado na Internet - *Internet* Organised Crime Threat Assessment **(IOCTA)** -, o seu principal relatório estratégico sobre as principais descobertas e ameaças emergentes e desenvolvimentos em crimes cibernéticos, estabelecendo prioridades para o Plano de Ação Operacional da **EMPACT**[1] (European Multidisciplinary Platform Against Criminal Threats**)** nas áreas de cibercrimes, que são o foco para esse ano. O IOCTA demonstra o quão amplo e variado é o cibercrime e como o EC3 é uma parte fundamental da resposta da Europol e da UE.

O EC3 adota uma abordagem de três ângulos para o combate ao cibercrime: forense, estratégia e operações. Também faz parte do EC3 o Joint Cybercrime Action Taskforce **(J-CAT)**, cuja missão é conduzir ações coordenadas e lideradas pela intelligence-led contra as principais ameaças de cibercimes através de investigações e operações transfronteiriças.

De referir que o Relatório anual sobre a Ameaça de Crime Organizado na Internet (5 de outubro de 2020) veio confirmar que a Covid-19, que obrigou a que o mundo se adaptasse a uma nova realidade, um novo normal que se viu mais focado na *Internet*, impulsionou o crescimento de problemas ligados ao cibercrime por toda a Europa, designadamente através de esquemas *online*, "phishing" (fraude eletrónica de obtenção de senhas e dados financeiros e pessoais), da disseminação de "*fake news*" e de crimes de alta tecnologia (programas malignos: *malware*, ou s*oftware* malicioso que se infiltra e ganha controlo sobre um sistema de computador ou um dispositivo móvel para roubar

[1] O cibercrime é uma prioridade do EMPACT para o ciclo de políticas de 2018 a 2021: o objetivo é combater o cibercrime, interrompendo (1) as atividades criminosas relacionadas a ataques contra sistemas de informação, particularmente aqueles que seguem um modelo de negócio crime como serviço e trabalham como facilitadores para crimes online, (2) combatendo o abuso sexual infantil e a exploração sexual infantil, incluindo a produção e disseminação de material de abuso infantil, e por (3) direcionar criminosos envolvidos em fraude e falsificação de meios de pagamento não monetários, incluindo fraudes em cartões de pagamento em larga escala (especialmente fraude não presente), ameaças emergentes a outros meios de pagamento que não em dinheiro

informações valiosas ou danificar dados; existem muitos tipos de *malware* que se podem complementar ao realizar um ataque).

Por sua vez, a encriptação de dados impõe uma dificuldade acrescida para as forças policiais que atuam neste ramo, pelo facto de ser complicado aceder a dados relevantes para constituir investigações criminais.

Os ataques de "*ransomware*" tornaram-se mais sofisticados, visando organizações específicas nos setores público e privado por meio do reconhecimento de vítimas. ("ransomware" é um tipo de *malware* que restringe o acesso ao sistema infetado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido).

A transmissão *online* ao vivo de abuso infantil continuou a aumentar, tornando-se ainda mais popular durante a crise da Covid-19, quando as restrições de viagens impediram os infratores de atuarem fisicamente.

A troca de cartões SIM, que permite que criminosos acedam a contas privadas, é uma das novas tendências incluídas no relatório deste ano da Europol.

Também no relatório da Europol – How COVID-19 related crime infected Europe during 2020 (11 de novembro de 2020) - é feita a análise da relação da progressão da pandemia com a evolução da criminalidade. O relatório foca a distribuição (***online*** e ***offline***) de materiais de proteção e produtos médicos e farmacêuticos falsificados e o aumento potencial da solicitação de material relacionado com o abuso sexual de crianças, entre outros fenómenos. Sublinha o incremento de fenómenos de cibercrime (campanhas de ***phishing***, ***ransomware***, ***malware*** e ***business email compromise***) e também de desinformação, ou ***fake news***.

A resposta coordenada a ciberataques em larga escala continua a ser um desafio fundamental para uma cooperação internacional eficaz no ecossistema de cibersegurança. O desenvolvimento do protocolo de resposta a emergências da UE melhorou significativamente a preparação da ciber-resiliência, afastando-se de medidas incongruentes de resposta reativa, orientado a incidentes e agindo como facilitadores críticos de recursos de resposta rápida que suportam a resiliência digital.

Só com um esforço conjunto, em colaboração com os seus parceiros a nível bilateral, regional e internacional, será possível colocar a UE na linha da frente da resiliência digital e da luta contra a cibercriminalidade. E é, por isso, essencial sincronizar parceiros e recursos globais na procura e adoção das melhores práticas de prevenção e mitigação do cibercrime internacional e outras ameaças de segurança mais abrangentes.