BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

MARÇO 2023 | nº 1/2023

DESTAQUES

Desinformação

O termo “desinformação”, no contexto da identificação de uma ameaça, refere-se a “toda a informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público” (ERC). A sua associação à expressão “notícias falsas” ocorre quando essa desinformação procura simular notícias.

Cibersegurança

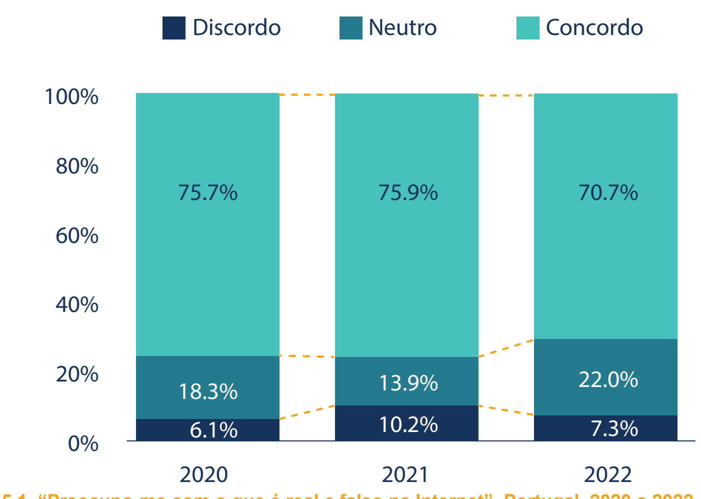
O problema da desinformação não é apenas do âmbito do jornalismo ou dos *media*. É também um problema de cibersegurança, sobretudo porque os meios digitais proporcionam a disseminação de desinformação e automatismos informáticos para simular conteúdos e ações fidedignos: por exemplo, as campanhas que usam *botnets* para manipular as redes sociais, a produção de *deepfakes*, a criação de contas falsas ou o furto de identidade *online*.

Desinformação avançada

Os desenvolvimentos mais recentes nas tecnologias digitais, como seja no campo da Inteligência Artificial (IA), trouxeram maior sofisticação à desinformação e capacidade de simular imagens, vozes e textos. Além disso, o contexto geopolítico criou condições para o uso sistemático deste instrumento como arma nas redes sociais para a desestabilização política por parte de oponentes estatais ou paraestatais (Singer e Brooking, 2018).

PANORÂMICA

- De acordo com o *Digital News Report Portugal 2022*, existe uma preocupação com o que é “real e falso” na Internet para 7 em cada 10 pessoas em Portugal em 2022, menos 5 pp do que em 2021. Por sua vez, há mais pessoas a ter uma posição neutra a este respeito.
- As pessoas em Portugal afirmam ter encontrado informação falsa sobretudo em relação à Covid-19 (42%* das pessoas), a política (34%) e a produtos e serviços (22%). Os dados indiciam ainda que quanto mais se desconfia das notícias, mais se crê identificar notícias falsas.
- Em termos de consumo de notícias através das redes socais, este estudo mostra que o Facebook é a plataforma mais usada (49% das pessoas), mas que perdeu 18 pp desde 2015. No WhatsApp e no Instagram, ao contrário, este tipo de consumo aumentou.



5.1. “Preocupo-me com o que é real e falso na Internet”, Portugal, 2020 a 2022

Fonte: RDNR 2020 a 2022. Edição: OberCom. n2020=2012; n2021=2101; n2022=2011 (utilizadores de Internet).

*Os valores apresentados são arredondados. (Obercom-RISJ)

- Não obstante, em Portugal, a fonte principal de notícias em 2022 foi a televisão (54% das pessoas), seguindo-se as redes sociais (20%), a Internet (excluindo as redes sociais) (17%), a rádio (7%) e a imprensa (3%).
- Existem discrepâncias significativas entre idades a este respeito: as pessoas mais velhas tendem a ter na televisão a sua fonte principal de notícias, enquanto as mais jovens encontram nas redes sociais um peso idêntico à televisão como fonte principal de notícias.

PERSPETIVA

1 O uso da desinformação como instrumento de propaganda não é uma novidade na História. A desinformação, neste sentido, diz respeito a campanhas que procuram polarizar, confundir e condicionar um público através da criação de perceções erróneas ou descontextualizadas sobre uma realidade, conduzindo esse público a ações que prejudiquem o próprio e um adversário. Por exemplo, o público poderá ser um eleitor e o adversário um político em eleições.

2 A desinformação também é utilizada como instrumento para a obtenção de ganhos económicos. Neste caso, em geral, ocorre uma ação sobre um público com o objetivo de o condicionar a ter comportamentos que favorecem economicamente o agente que lança o conteúdo de desinformação. Por exemplo, quando uma ação de *phishing* é acompanhada por conteúdos de desinformação que promovem falsamente um produto ou serviço.

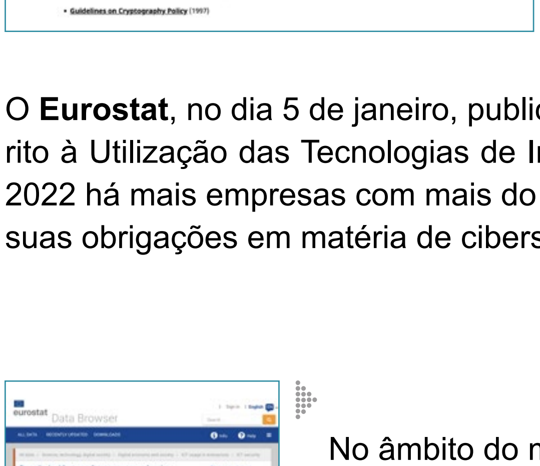
3 Existem ainda processos que se confundem com desinformação e que, embora intencionais, podem não corresponder a ações com objetivos maliciosos, embora tenham consequências negativas. Por exemplo, alguns conteúdos falsos que desacreditam a ciência ou elaboram “teorias da conspiração” podem ser desenvolvidos com base em crenças honestas. No entanto, por vezes, estes casos são instrumentalizados por campanhas de desinformação efetivas.

4 Algumas tecnologias emergentes, como a IA, têm trazido desenvolvimentos facilmente apropriáveis como instrumentos de desinformação. O incremento da capacidade de simular uma realidade através de imagens, vozes e textos promovido pela IA favorece uma desinformação que é tanto mais eficaz quanto melhor conseguir produzir simulações verosímeis. Além disso, a IA permite a automação dos processos de disseminação da desinformação.

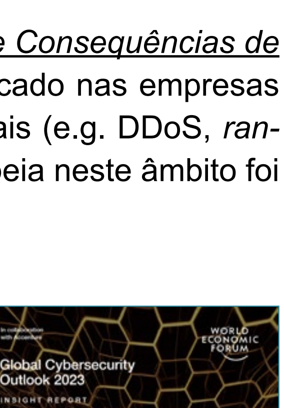
5 A criação de ambientes digitais imersivos, como o metaverso, resulta em contextos particularmente desafiantes no que diz respeito à desinformação. Este tipo de ambiente tende, mais do que a simular uma realidade existente, a construir uma realidade alternativa, ainda que eventualmente em conexão com a realidade existente. Este efeito incide muito diretamente sobre o quadro de perceções dos indivíduos, o alvo-chave da desinformação.

6 As redes sociais têm tido um papel muito importante na disseminação da desinformação digital. A conversão dos leitores de notícias em potenciais produtores de notícias e vetores de partilha de conteúdos distribuiu a criação de informação por uma massa de perfis *online* apropriáveis ou influenciáveis por agentes maliciosos. O caráter aberto das redes sociais expõe de uma forma ímpar o espaço público à influência de campanhas de desinformação.

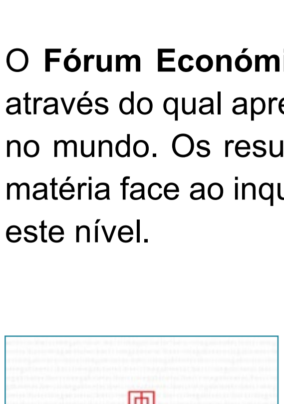
PUBLICAÇÕES E NOTÍCIAS



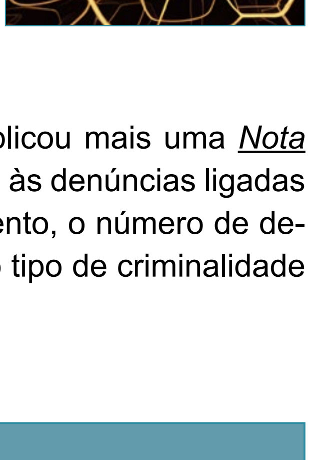
A **OCDE** - Organização para a Cooperação e Desenvolvimento Económico, no dia 14 de dezembro, produziu um conjunto de recomendações relevantes para a cibersegurança, nomeadamente sobre gestão do risco da segurança digital, estratégias nacionais para a segurança digital, segurança digital de produto e serviços e tratamento das vulnerabilidades da segurança digital.



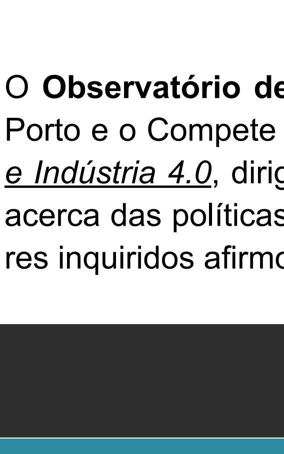
O **Eurostat**, no dia 5 de janeiro, publicou os resultados referentes às *Políticas de Segurança*, no âmbito do Inquérito à Utilização das Tecnologias de Informação e Comunicação nas Empresas. Entre 2019 (inquérito anterior) e 2022 há mais empresas com mais do que 10 empregados em Portugal a sensibilizar os seus funcionários para as suas obrigações em matéria de cibersegurança, um crescimento de 9 pp, de 54,3% para 63,3% das empresas.



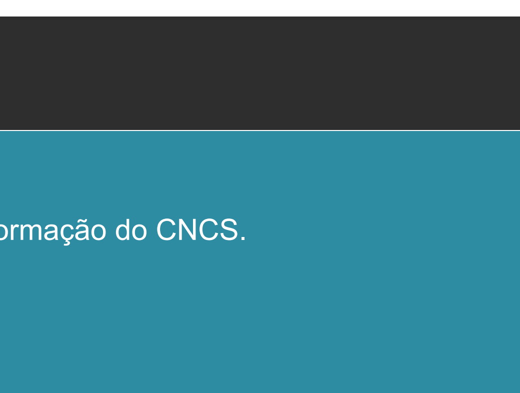
No âmbito do mesmo inquérito, foram partilhados pelo **Eurostat** dados relativos a *Incidentes e Consequências de Segurança*. O tipo de consequência resultante de incidentes de cibersegurança mais identificado nas empresas com mais de 10 empregados em Portugal, em 2022, foi a indisponibilidade de serviços digitais (e.g. DDoS, *ransomware*, falhas de *hardware* ou *software*), para 9,7% das empresas. A média da União Europeia neste âmbito foi de 20,1%.



O **Fórum Económico Mundial**, no dia 18 de janeiro, publicou o *Global Cybersecurity Outlook Report 2023*, através do qual apresentou os resultados de um inquérito sobre cibersegurança realizado a líderes empresariais no mundo. Os resultados mostram que há mais consciência sobre a cibersegurança e vontade de agir nessa matéria face ao inquérito anterior. Contudo, existem dificuldades na comunicação entre parceiros empresariais a este nível.



O **Gabinete Cibercrime** da Procuradoria-Geral da República, no dia 14 de fevereiro, publicou mais uma *Nota Informativa Cibercrime: Denúncias Recebidas 2022*, na qual apresenta os números relativos às denúncias ligadas ao cibercrime recebidas por este organismo durante o ano de 2022. Segundo este documento, o número de denúncias aumentou 83%, de 1160 para 2124, em 2022 face ao ano anterior. O *phishing* foi o tipo de criminalidade mais denunciado.



O **Observatório de Cibersegurança** do CNCS, em colaboração com o Instituto Politécnico do Porto e o Compete 2020, no dia 7 de março, publicou os resultados do Inquérito *Cibersegurança e Indústria 4.0*, dirigido aos técnicos operacionais e trabalhadores de entidades da Indústria 4.0, acerca das políticas e práticas de cibersegurança implementadas. Somente 26% dos trabalhadores inquiridos afirmou ter recebido da sua empresa sensibilização em cibersegurança em 2021.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança