newsletter

cyber&data protection IP

Politécnico de Viseu · Politécnico da Guarda · ipvc Instituto Politécnico de Viana do Castelo

PROTEÇÃO DE DADOS

O QUE FOI 2021 E O QUE ESPERAR DE 2022?

Opinião
Elsa Veloso
(Advogada Especialista em Privacidade e Proteção de dados)

Quando pensei em escrever sobre o que podemos esperar de 2022, logo me ocorreu a ideia de que tal raciocínio apenas poderia ser feito mediante uma análise e um balanço contundente sobre o que foi a agenda da privacidade, da proteção de dados e da segurança da informação durante o ano 2021.

Fazendo uma retrospetiva global ao nível destas matérias de crescente importância no dia a dia de cada um de nós, destaco oito acontecimentos que marcaram o ano:

1. Em 2021, foi atingido o valor mais alto de coimas aplicadas por força da violação dos dados: 1 bilião de euros de coimas aplicadas pelas autoridades de controlo. Os três primeiros lugares do pódio foram ocupados pelas coimas de € 746.000.000, € 225.000.00 e € 50.000.000 à Amazon, Whatsapp e Google

2. A aprovação da Digital Market Act (Lei dos Mercados Digitais), direcionada para a regulação e proibição de certas práticas desleais dos gigantes da tecnologia, garantindo posições equitativas no mercado da concorrência livre e saudável no espaço europeu, oferecendo uma liberdade de inovação nos produtos digitais, preços mais justos, qualidade e capacidade de escolha pelo consumidor, abrindo o mercado e a economia a todos os que dela queiram fazer parte;

3. Foi aprovada a Digital Services Act (Lei dos Serviços Digitais), destinada a assegurar uma melhor proteção dos consumidores, o respeito pelos direitos fundamentais em linha, a implementação de um quadro claro e eficaz em matéria de transparência e responsabilidades das plataformas online garantindo a liberdade e escolha de preços mais baixos, menor exposição a conteúdos ilegais e sobretudo, uma atenuação dos riscos sistemáticos tais como a manipulação ou a desinformação;

4. Por cá, Portugal esteve no epicentro da agenda política da temática da proteção de dados(e não pelas melhores razões). Relembremos o caso Russiagate, relativo à partilha pela Câmara Municipal de Lisboa dos dados pessoais (e sensíveis) dos promotores de manifestações com as embaixadas em Portugal, nomeadamente a embaixada russa, por ocasião de um protesto organizado contra Putin. A CML acabou por ser acusada de mais 100 infrações consubstanciando-se na violação dos princípios e regras do tratamento de dados previstos no RGPD, levando à queda do executivo nas eleições autárquicas;

5. 2021 foi também o ano em que (afinal) os cookies dos sítios webs dos organismos ligados ao Estado estavam em desconformidade com a decisão do Tribunal de Justiça da União Europeia (Acórdão Planet 49), indo contra as regras do consentimento na recolha de cookies pelos responsáveis pelo

tratamento e por entidades terceiras com quem os dados eram partilhados.

6. 2021 foi também o ano em que nos apercebemos que os dados pessoais dos representantes legais e contratantes singulares nos contratos celebrados com as entidades públicas estavam expostos no portal BASE, de forma excessiva e desproporcional, em perfeita contradição com o princípio da minimização dos dados pessoais e da necessidade, distorcidos das exigências dos fundamentos de licitude (execução contratual, interesse legítimo e interesse público);

7. Não podemos ainda esquecer o reembolso do IVA através do programa IVAUCHER, o qual indicou como responsáveis pelo tratamento dos dados duas entidades denominadas de SALTPAY (uma inclusive com sede na Islândia), ao invés do Estado, levando uma vez mais, à entrada em campo da autoridade de controlo (a CNPD);

8. Por último, 2021 foi o ano da sentença e da morte da app stayway covid por inaplicabilidade, mas sobretudo pelas diversas falhas de segurança demonstradas, ao mesmo tempo que era apelidada antiética, antidemocrática e até inconstitucional por força da sua hipotética obrigatoriedade.

Com isto, concluímos que em 2021 o Estado (ainda) não está em conformidade com o Regulamento Geral sobre a Proteção de Dados. Não podemos aceitar que o maior beneficiário da bazuca europeia, com fundos e ordens para aplicação na transição e transformação digital ainda se escude na ignorância e desconhecimento das regras, princípios e das medidas técnicas e organizativas impostas pelo RGPD, em vigor há seis anos e aplicável há três.

Os organismos públicos, assim como as empresas privadas, devem nomear Encarregados da Proteção de Dados dotados de competência, conhecimento, sensibilidade e formação na área de modo a zelar, acompanhar, sensibilizar e agir de acordo com as suas funções de garantes do cumprimento da legislação nesta matéria. Devem ainda, se necessário, recorrer a consultoria externa para colaboração e cooperação nas questões mais complexas ou nas dúvidas sem respostas. Contudo, deverá a Comissão Nacional da Proteção de Dados, lançando mão dos parcos recursos e meios que pode e tem, ir fiscalizando e agindo sobre o Estado e as entidades particulares na garantia dessa conformidade. Não podemos deixar que a proteção dos dados e a segurança da informação caiam e sejam geridas por um certo amadorismo, curiosidade e gosto elementar na matéria.

Face a isto, as empresas podem esperar um ano 2022 igualmente interventivo em matéria de regulação do tratamento dos dados pessoais e da segurança da informação, com o foco na prevenção e reação à violação dos dados no seguimento do que foi 2021. As autoridades de controlo continuarão no encalço do desrespeito pelas regras e princípios previstos no RGPD, sobretudo no escrutínio das plataformas e tecnologias com sistemas biométricos, definição de perfis e uso de algoritmos que impactem seriamente os direitos fundamentais dos titulares dos dados.

Assim, faço votos que em 2022:

· As empresas e o próprio Estado continuem e encetem os esforços necessários para a assunção dos compromissos em matéria de respeito pela privacidade, proteção de dados e segurança da informação, seja através da formação e sensibilização dos seus funcionários e das partes envolvidas, seja através do reforço e pedidos de consultoria junto de empresas que ajudem e colaborem na árdua tarefa de colocar o aparelho estadual no campo de visão do RGPD.

· Seja aplicado mais privacy by design, mais respeito pelo princípio da minimização dos dados, pelo princípio finalístico, acesso e transparência sobre quem, quando e como, os dados serão e são tratados;

· Sejam feitas mais avaliações de impacto sobre as novas formas (tecnológicas) e plataformas de tratamento de dados pessoais, de forma a avaliar mitigar, eliminar ou transferir os riscos dos tratamentos sobre os dados.

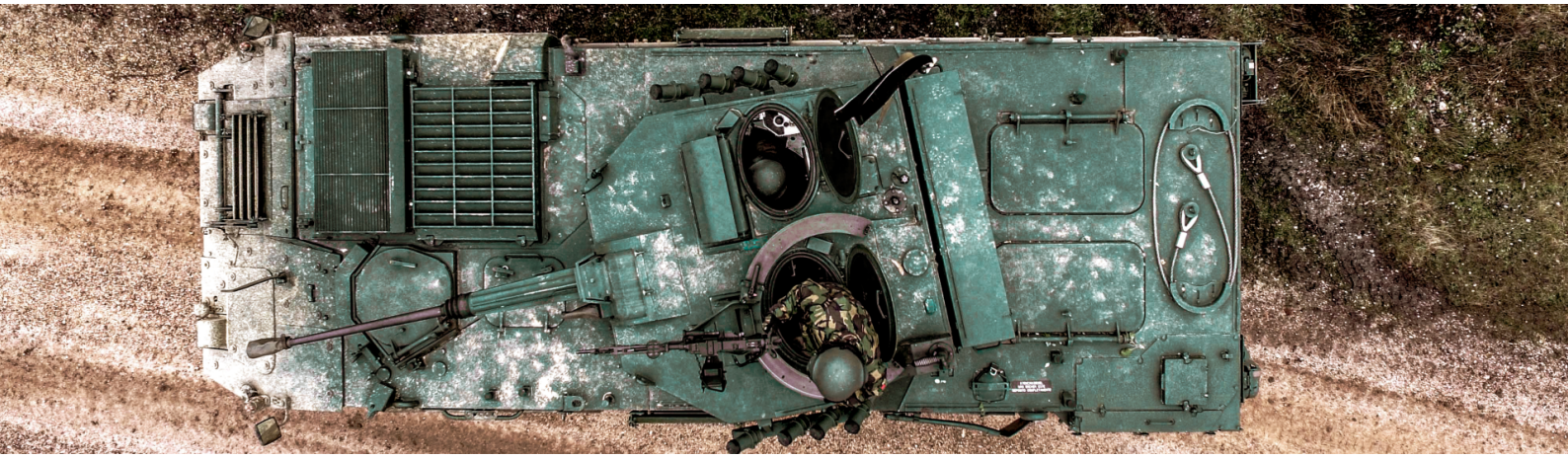
Em resumo, espero que 2022 continue a dar seguimento ao controlo do tratamento dos dados.

No novo ano, os dados continuarão a ser o "novo petróleo" para as empresas e para o próprio Estado e cabe a cada um a responsabilidade da sua exploração, tendo em conta que a mesma tem regras e que, à mínima falha, o preço a pagar poder ser demasiado alto.

Fonte **ECO**

PORTAL BASE CONTINUA A PUBLICAR DADOS PESSOAIS DE CIDADÃOS. **CONTRATOS DO EXÉRCITO ENTRE OS MAIS DESPROTEGIDOS**

Tiago Soares
(Jornalista)



Problema foi noticiado em outubro e demorou dois meses a ser corrigido após Governo ter tomado conhecimento, mas várias entidades públicas continuam a divulgar informações sigilosas de empresários que fizeram contratos com o Estado em 2022 — incluindo números de telefone, moradas, números de cartão de cidadão e de contribuinte. Exército é dos organismos com menor proteção de dados pessoais, mas há muitos casos em organismos do SNS, universidades, e autarquias - incluindo a Câmara Municipal de Lisboa.

O Portal Base, o site onde são disponibilizados todos os contratos públicos, continua a publicar dados pessoais de cidadãos portugueses: moradas, números de telefone, números de cartão de cidadão e de contribuinte. A entidade do Estado está assim em violação do Regulamento Geral de Proteção de Dados (RGPD), a lei europeia cujo objetivo é proteger a privacidade das pessoas e que entrou em vigor em 2016.

Entre as entidades públicas que colocaram contratos na plataforma em violação da lei estão os três ramos das Forças Armadas, associações de comércio regionais, organismos do SNS (como centros hospitalares), universidades, e autarquias - incluindo a Câmara Municipal de Lisboa, que já foi multada em 1,2 milhões de euros na sequência do caso 'Russiagate', em que dados pessoais de ativistas foram enviados a países estrangeiros.

O Base é gerido pelo Instituto dos Mercados Públicos, do Imobiliário e da Construção (IMPIC), que está sob a tutela do Ministério das Infraestruturas e da Habitação. "O IMPIC vai fazer nova notificação a todas entidades para que sejam corrigidas as irregularidades que forem detectadas no que diz respeito à proteção de dados", disse fonte oficial do instituto ao Expresso. O jornal também contactou a Comissão Nacional de Proteção de Dados (CNPD) e aguarda respostas às questões colocadas.

O incumprimento do RGPD por parte do Estado não é novo: em outubro, o Expresso noticiou que o Base estava a expor moradas, números de telefone e números de cartão de cidadão

e de contribuinte de cidadãos. Na altura, alertado pelo jornal, o Governo mandou bloquear o acesso aos contratos públicos até as irregularidades serem corrigidas.

Seguiu-se um trabalho que durou cerca de dois meses: o IMPIC contactou as entidades públicas para estas reverem os contratos e rasurarem os dados pessoais, tendo reforçado por escrito a necessidade de cumprimento do RGPD. Além disso, o IMPIC foi obrigado a reportar os casos à CNPD e aos próprios cidadãos cujos dados tinham sido expostos.

Apesar destas medidas, os problemas mantêm-se: o Expresso consultou centenas de contratos de várias entidades públicas celebrados já em 2022 e constatou que muitos organismos

continuam sem rasurar dados pessoais ou fazem-no de forma deficiente — por exemplo, inserindo uma 'barra preta' por cima da informação sigilosa.

Problema: qualquer pessoa com um conhecimento mínimo de informática é capaz de abrir o documento num leitor de ficheiros 'pdf' e retirar a barra preta, ou até mesmo copiar a informação escondida por baixo da barra e colá-la para um novo documento (copy paste) para a poder consultar. No entanto, os funcionários públicos responsáveis por rasurar os dados pessoais e fazer o upload dos contratos para o Base não conheciam ou não acautelaram esta simples possibilidade técnica.

A julgar pelos contratos celebrados em 2022, uma das entidades públicas que mais vezes comete esta falha é o Estado Maior do Exército. Exemplo: o terceiro maior contrato celebrado este ano, no valor de quase 580 mil euros, expõe sem grande resistência o número de cartão de cidadão do representante da empresa que chegou a acordo com o Exército, sob a tutela do Ministério da Defesa.

Outro ficheiro, referente a um contrato celebrado no início deste mês entre o Exército e uma empresa portuguesa, deixa a descoberto dados pessoais sobre o empresário em questão — incluindo número de contribuinte e morada.

"O Estado Maior do Exército trata de informações confidenciais e tem acesso a informações críticas, por isso deveria ter formas mais sofisticadas de proteger os seus dados. É uma situação inenarrável", considera um especialista em proteção de dados, que pediu para manter o anonimato. "Sendo um ramo das Forças Armadas, deviam ter ao seu dispor instrumentos confiáveis para proteger estas informações", acrescenta.

Esta deficiência repete-se com outros contratos, apesar de nem todos os documentos estarem mal rasurados. O mesmo se pode dizer dos ficheiros anexados ao Base pela Marinha e pela Força Aérea: há ficheiros mal rasurados e que expõem informação confidencial, mas também há ficheiros em que o trabalho informático foi feito de forma eficaz. Aliás, comparando os três ramos das Forças Armadas, conclui-se que a Marinha e a Força Aérea são mais eficientes a cumprir o RGPD do que o Exército — e quando deixam informação desprotegida, o processo para obtê-la é mais difícil do que simplesmente fazer um 'copy paste', algo que é frequente no caso do Exército.

"O Estado tem de dar o exemplo", começa por opinar Elsa Veloso, jurista e especialista no regime que rege a proteção de dados. "Se o IMPIC sabe que houve fugas de dados através do Base e tomou medidas para resolver o problema, tem a obrigação legal de validar essas medidas", acrescenta. Para a jurista, bastava que o IMPIC "disponibilizasse um pequeno tutorial ou uma ferramenta simples" que permitisse às entidades públicas limpar os dados pessoais de forma eficaz e submeter os dados pessoais de forma segura no Base. "Não é bom sinal que o Estado esteja a apostar na transição digital e não crie algo tão simples, sobretudo num portal que já deu tantos problemas", considera.

UNIVERSIDADES E AUTARQUIAS EM FALHA (INCLUINDO LISBOA)

De certa forma, o caso do Exército indica a falta de compreensão do RGPD por parte de alguns organismos estatais: em alguns contratos recentes, é rasurada informação que não deve ser rasurada — como o nome das empresas e respetivos números de contribuintes. "O RGPD não se aplica a nomes empresariais e pessoas coletivas, e esconder essa informação viola a lei da contratação pública e o princípio da transparência, cujo cumprimento é a principal função do portal Base", explica Elsa Veloso.

Outra instituição que apresenta falhas no tratamento dos dados pessoais é a Câmara Municipal de Lisboa: o Expresso encontrou pelo menos um contrato celebrado em 2022 em que era possível obter o número de cartão de cidadão e de contribuinte do empresário que chegou a acordo com a autarquia. No entanto, a esmagadora maioria dos ficheiros referentes à autarquia da capital que foram consultados estavam rasurados de forma segura.

Assim, tal como na situação noticiada em outubro, o Base está a disponibilizar de forma ilícita dados que não deviam ser disponibilizados, "o que constitui um crime de violação de dados", aponta Elsa Veloso. Está em causa a violação de três princípios do RGPD: o princípio da legalidade, porque não há base legal para o tratamento dos dados pessoais; o princípio da minimização de dados, porque só podem ser usados os dados estritamente necessários para determinado fim, que neste caso é a transparência da Administração Pública; e o princípio da finalidade, que diz que os dados só podem ser usados para as finalidades para os quais foram recolhidos.

Várias instituições do Ensino Superior também estão a publicar contratos sem protegerem os dados pessoais das outras partes. É o caso do Instituto Superior Técnico, por exemplo, cujo maior contrato celebrado este ano permite consultar o número do cartão de cidadão do representante da empresa (neste caso, de segurança privada). A Universidade Nova de Lisboa também incorre no mesmo erro mais do que uma vez.

Há ainda entidades do universo da saúde - o Centro Hospitalar de Lisboa Norte e o Centro Hospitalar de Coimbra, por exemplo - que também fizeram upload de informação sigilosa para a plataforma pública, tal como pelo menos duas autarquias. Em contrapartida, os ficheiros disponibilizados por GNR e PSP, por exemplo, cumprem as regras da proteção de dados, estando rasurados de forma eficaz e segura.

Em junho do ano passado, o Expresso noticiou que o RGPD foi violado pela Câmara de Lisboa, que de forma reiterada divulgou informações pessoais de ativistas a vários países, incluindo a Rússia. A CNPD detectou 225 infrações e multou a autarquia da capital em 1,2 milhões de euros.

Fonte **EXPRESSO**
Fotos **EXÉRCITO PORTUGUÊS, FREEPIK**

CIBERSEGURANÇA

RECOMENDAÇÕES DE CIBERSEGURANÇA PARA AS EMPRESAS EM TEMPOS DE GUERRA

Empresa global de cibersegurança recorda vários ciberataques de que a Ucrânia foi alvo recentemente e diz que não se pode "ignorar a possibilidade de que os ataques se possam propagar a mais geografias".

Num contexto de Guerra na Ucrânia, a empresa global de cibersegurança Cipher recorda os vários ataques informáticos de que a Ucrânia foi alvo recentemente e diz que não se pode "ignorar a possibilidade de que os ataques que inicialmente têm como alvo um país, se possam propagar a mais geografias".

Perante este clima de incerteza, a Cipher apresentou, através de um comunicado às redações, sete recomendações de cibersegurança para as empresas:

"1. Desenvolver e planificar um plano de resposta a incidentes.

2. Verificar o acesso que os colaboradores têm dentro da organização e as permissões que podem representar um risco para a empresa, o que inclui ativar a autenticação de dois fatores.

3. Manter o software atualizado com as últimas atualizações de segurança consideradas, dando prioridade às novas vulnerabilidades identificadas.

4. Verificar se os mecanismos de backup e restauração estão a funcionar corretamente.

5. Os profissionais dentro da empresa dedicados à proteção dos bens devem ser formados na identificação de eventuais ameaças ou comportamentos anormais na rede.

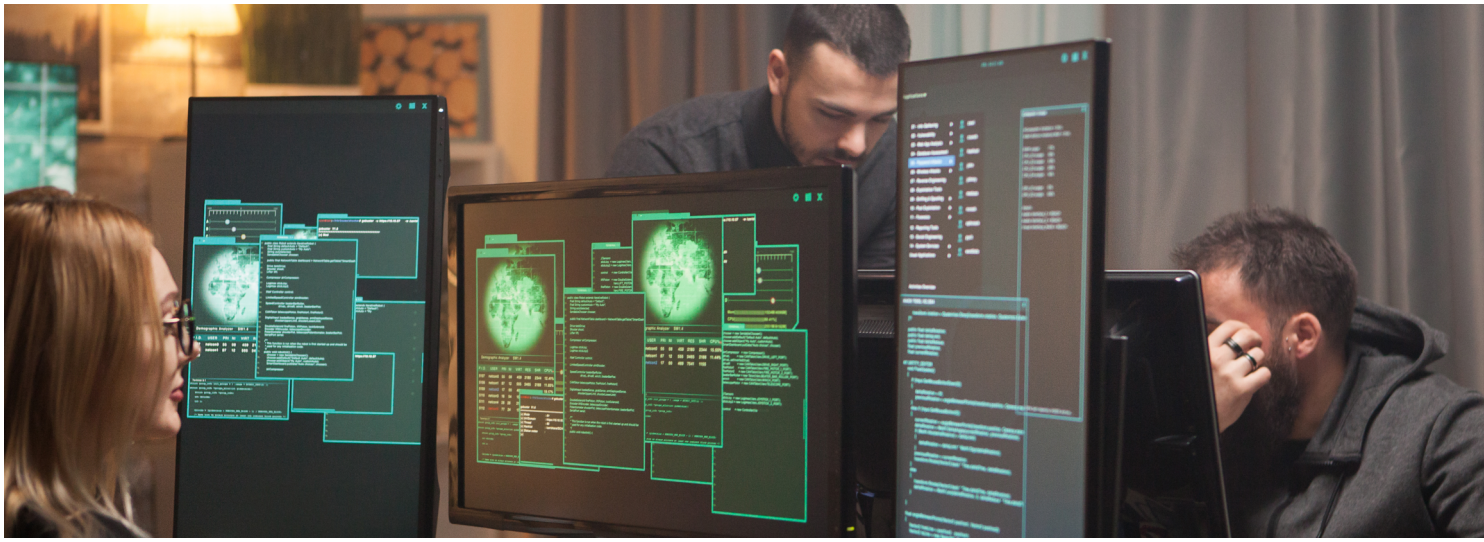
6. No caso de trabalhar com organizações ucranianas, recomenda-se a monitorização e inspeção do tráfego da rede dessas organizações e dos controlos de acesso às mesmas.

7. É recomendável que se mantenha a par das recentes ameaças que estão a ser levadas a cabo."

A Cipher lembra que o Ministério da Defesa ucraniano e vários bancos estatais (Privatbank e Oschadbank) sofreram ataques que resultaram na interrupção das suas operações a 15 de fevereiro e que vários sistemas e bancos governamentais ucranianos foram novamente perturbados por outro ataque oito dias depois.

"Na sequência destes incidentes e da escalada do conflito após o início da invasão russa, as ações ofensivas cibernéticas têm consistido principalmente em takedown de websites e ataques DDoS dirigidos ao governo ucraniano, a meios de comunicação social, a infraestruturas da Internet e a serviços eletrónicos utilizados por cidadãos ucranianos, tais como a banca digital. Estes ciberataques têm provavelmente como objetivo causar confusão, dificultar as comunicações, enfraquecer uma resposta militar ucraniana e desmoralizar a população do país. Embora o alvo neste momento seja a Ucrânia e a Rússia, não podemos ignorar a possibilidade de que os ataques que inicialmente têm como alvo um país, se possam propagar a mais geografias", pode ler-se no comunicado.

Fonte **DN**
Fotos **FREEPIK**



CIBERSEGURANÇA

CONSÓRCIO EM GOUVEIA DESENVOLVE CIBERSEGURANÇA PARA MUNICÍPIOS

"Para dar resposta à crescente necessidade de segurança da informação e para responder às exigências legais do Decreto-Lei 65/2021, que obriga a Administração Pública a procedimentos de segurança de informação e de infraestruturas informáticas, o projeto 'The Rock' desenvolveu um conjunto de serviços que disponibiliza à Administração Local, que é o 'Secure County'", referiram os promotores em comunicado enviado à agência Lusa.

O 'Secure County' é um conceito "que foi especialmente desenvolvido para garantir a segurança da informação, detetando vulnerabilidades, prevenindo intrusões e recuperando incidentes que eventualmente venham a acontecer, numa perspetiva holística de melhoria contínua que permite assegurar tranquilidade e segurança em todos os sistemas dos Municípios Portugueses".

O serviço será oferecido em três patamares, "adaptando-se às especificidades de cada município, oferecendo serviços desde Gestão de Vulnerabilidades, Gestão de Risco, Conformidade Processual até à monitorização de Cibersegurança e de resposta a incidentes 24/7".

"Este serviço foi desenvolvido por um consórcio de empresas recentemente instaladas em Gouveia e liderado pelo 'The Rock', combinando as mais recentes tecnologias de líderes mundiais, com uma equipa de profissionais altamente qualificados na área da Engenharia Informática e da Cibersegurança", explicaram os promotores.

O consórcio "encontra-se neste momento a apresentar a solução à generalidade dos Municípios Portugueses, assim como a outras entidades da Administração Local".

O projeto empresarial "The Rock" foi apresentado publicamente em julho de 2021, numa sessão realizada no edifício dos Paços do Concelho de Gouveia.

Como os promotores referiram na ocasião, o projeto iria "criar e desenvolver um ecossistema digital e de tecnologias de informação a partir de Gouveia".

Nuno Ramos, responsável financeiro do projeto, adiantou à Lusa que estimava realizar um investimento "superior a dois milhões de euros e a criação de mais de 50 postos de trabalho", num horizonte de cinco anos.

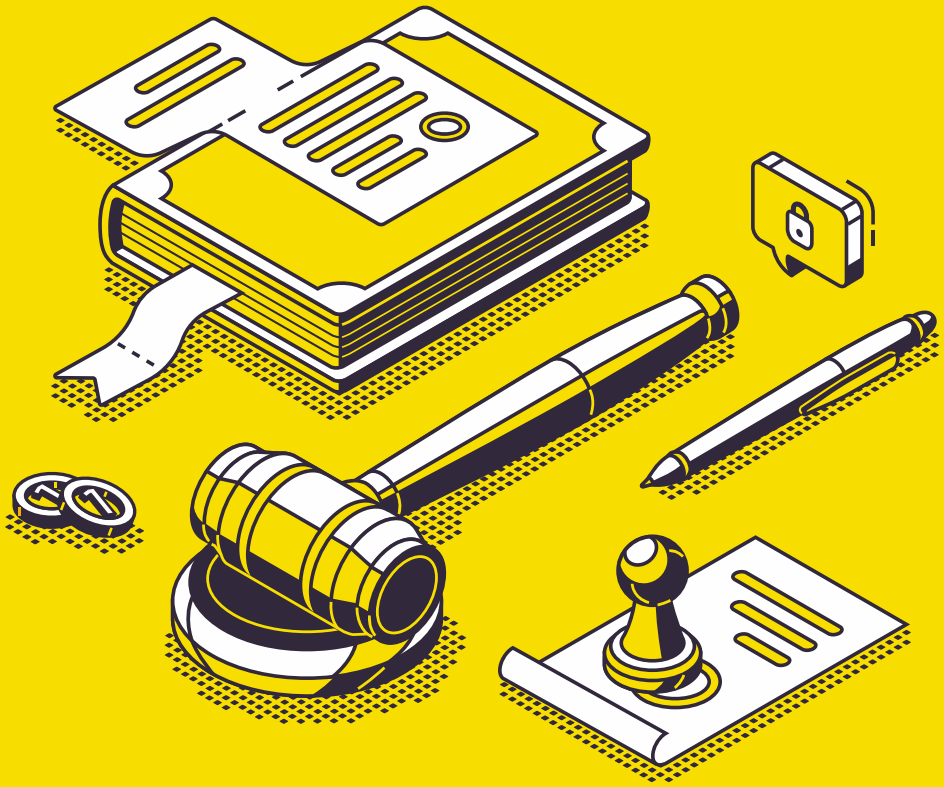
O projeto "The Rock" "pretende aproveitar uma série de fatores que são muito construtivos a partir de Gouveia, nomeadamente as questões geográficas, que permitem transmitir uma maior sensação de segurança e, a partir do município, prestar serviços na área da cibersegurança para empresas e instituições públicas", declarou.

No dia 01 de fevereiro, no âmbito das comemorações da elevação de Gouveia a cidade, o município inaugurou uma Incubadora de Negócios, que resultou da obra de reconversão do espaço da antiga fábrica têxtil Belino & Belino, destinada a acolher o projeto "The Rock", segundo a autarquia.

Fonte **LUSA / NOTÍCIAS AO MINUTO**
Fotos **LINKEDIN**

CIBERSEGURANÇA

DAS LEIS ÀS OBRIGAÇÕES DAS ORGANIZAÇÕES



Várias são as leis que abrangem as matérias da cibersegurança, sendo uma das mais operacionais a Lei n.° 109/2009, de 15 de setembro, "Lei do Cibercrime". Para além desta, existem dois diplomas: a Lei n.° 46/2018, de 13 de agosto que transpõe para o ordenamento jurídico português a Diretiva (UE) 2016/1148 e o Decreto-Lei n.° 65/2021, de 30 de julho que regula o primeiro diploma.

Neles, são estabelecidos os requisitos de segurança e as obrigações de notificação de incidentes que as entidades da Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais, os prestadores de serviços digitais terão de cumprir, bem como os procedimentos de notificação voluntária de incidentes a todas as entidades que utilizem redes e sistemas de informação.

Já a Lei do Cibercrime (Lei n.° 109/2009, de 15 de setembro), estabelece as disposições penais materiais e processuais relativas a ataques contra sistemas de informação, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

O legislador europeu está consciente de que as redes e os sistemas e serviços de informação desempenham um papel vital na sociedade e de que a sua fiabilidade e segurança são essenciais para as atividades económicas e sociais e, em especial, para o funcionamento do mercado interno.

Quando os ataques afetem dados pessoais ou hajam suspeitas de que podem ter sido afetados, impõe-se a aplicação do Regulamento (EU) 2016/679, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ("RGPD") e a Lei n.° 58/2019, de 8 de agosto, a Lei de Proteção de Dados Pessoais ("LPDP").

Politécnico de Viseu
POLITÉCNICO GUARDA
ipvc Instituto Politécnico de Viana do Castelo
Cofinanciado por: COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu