PROTEÇÃO DE DADOS

50 anos CSM Conselho Superior da Magistratura

NEWSLETTER
MAIO 2026

5

Nesta edição

Editorial

No contexto da celebração dos 50 anos da Constituição da República Portuguesa, a 5.ª edição desta newsletter é especialmente dedicada à consagração constitucional do direito à proteção de dados pessoais. Em 1976, Portugal foi pioneiro e elevou a direito fundamental a proteção de dados pessoais face à utilização da informática. Aproveita-se assim a ocasião comemorativa para revisitar meio século de história e trazer o artigo 35.º para primeiro plano, espreitando o debate parlamentar, na especialidade, na Assembleia Constituinte e acompanhando a evolução do texto constitucional ao longo do tempo.
Destaque também nesta edição para as recomendações aprovadas pelo CSM quanto ao uso de inteligência artificial pelos juízes no exercício da função jurisdicional, nas quais a proteção de dados assume papel importante.
Ainda em modo festivo, assinalam-se os 10 anos do RGPD e da Diretiva relativa aos tratamentos de dados para fins de prevenção e investigação criminal e repressão de infrações penais, e saúda-se a criação da maior área do mundo para fluxos seguros de dados transfronteiras entre a UE e o Brasil.
Prossegue-se nesta edição a rubrica "Feito por Humanos", que aborda a interessante história do primeiro *chatbot* – de ler e procurar por mais.
Para manter as Boas & Práticas, não podiam faltar as já habituais dicas de cibersegurança para que os utilizadores contribuam, com simples gestos diários, para a proteção de todos.
Por último, esta newsletter desvenda um pouco do que está para acontecer naquele que será certamente o maior evento internacional do ano em Portugal sobre tecnologia e tribunais: Judiciary Tech Summit 26, 18-20 novembro, Pavilhão de Portugal, Lisboa. Reserve já na sua agenda.

Boa leitura!
Clara Guerra

50 anos CSM Conselho Superior da Magistratura

Direito fundamental à proteção de dados tem meio século

A Constituição da República Portuguesa consagra, desde 1976, o direito fundamental à proteção de dados pessoais. Portugal foi pioneiro no mundo a conceder dignidade constitucional à proteção de dados, numa década em que surgem na Europa as primeiras leis a regular o tratamento automatizado de dados pessoais.

Sob a epígrafe "Utilização da Informática", o artigo 35.º da lei fundamental reconhecia, em três números, o direito de acesso e de retificação, a proibição de uso da informática para tratar dados referentes a convicções políticas, fé religiosa ou vida privada e a proibição da atribuição de um número único aos cidadãos.

O artigo sofreu alterações com as revisões constitucionais de 1982, de 1989 e de 1997, esta última já para acomodar as normas comunitárias da Diretiva de Proteção de Dados de 95, que previam a extensão da proteção aos dados manuais e a existência de uma autoridade nacional de controlo independente.

Apesar de a proteção de dados ser um direito fundamental, a primeira lei a regular o regime de proteção de dados só viria a ser aprovada quinze anos depois, em 1991, através da Lei n.º 10/91, de 29 de abril – Lei de Proteção de Dados Pessoais face à Informática.

Na verdade, foram feitas duas revisões ao texto constitucional na ausência de uma lei a concretizar aquele direito fundamental e a aportar experiência concreta de aplicação.

No entanto, a década de 90 do século XX veio a ser pródiga na produção legislativa nacional em matéria de proteção de dados, cumprindo-se o quadro constitucional e concretizando-se na ordem jurídica interna as normas da Convenção 108 do Conselho da Europa e da Diretiva de Proteção de Dados da Comunidade Europeia. Em 1994, era criada a autoridade nacional de controlo, à época designada por Comissão Nacional de Proteção de Dados Pessoais Informatizados.

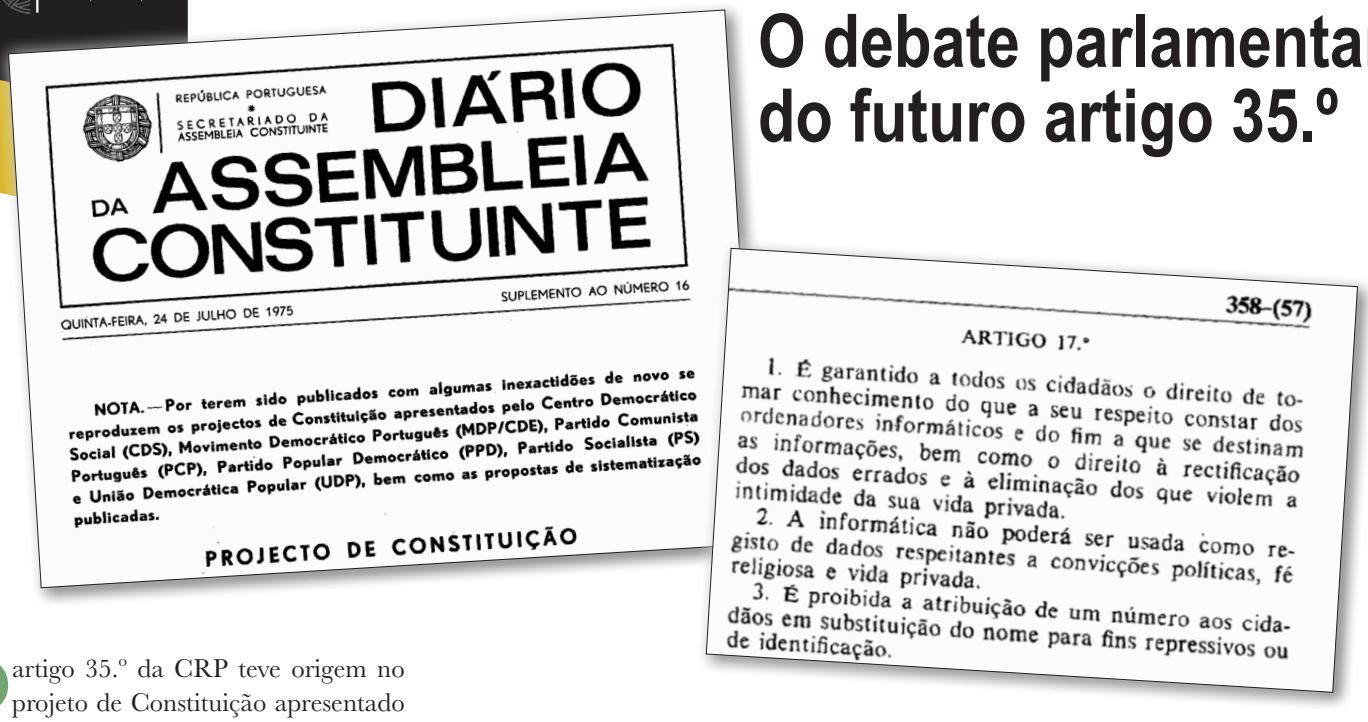
Entretanto, com o Tratado de Lisboa, a proteção de dados pessoais passou a ser, desde 2009, também um direito fundamental da União, consagrado no artigo 8.º da Carta dos Direitos Fundamentais.

Portugal foi, de facto, inovador neste domínio, certamente pelo contexto histórico nacional e pela consciência do potencial uso da informática contra os cidadãos, mas simultaneamente acompanhando os primeiros passos que eram dados em alguns países europeus e antecipando-se aos instrumentos internacionais nesta matéria: as Orientações da OCDE, em 1980, e a Convenção 108 do Conselho da Europa, em 1981.

Ao longo destes 50 anos, a epígrafe do artigo 35.º manteve-se, assim como a proibição de atribuição de um número único aos cidadãos, embora o texto constitucional tenha sido reforçado no seu todo. ■

50 anos CSM Conselho Superior da Magistratura

O debate parlamentar do futuro artigo 35.º



REPÚBLICA PORTUGUESA
SECRETARIADO DA ASSEMBLEIA CONSTITUINTE

DIÁRIO DA ASSEMBLEIA CONSTITUINTE

QUINTA-FEIRA, 24 DE JULHO DE 1975 — SUPLEMENTO AO NÚMERO 16

NOTA. — Por terem sido publicados com algumas inexactidões de novo se reproduzem os projectos de Constituição apresentados pelo Centro Democrático Social (CDS), Movimento Democrático Português (MDP/CDE), Partido Comunista Português (PCP), Partido Popular Democrático (PPD), Partido Socialista (PS) e União Democrática Popular (UDP), bem como as propostas de sistematização publicadas.

PROJECTO DE CONSTITUIÇÃO

358-(57)

ARTIGO 17.º

1. É garantido a todos os cidadãos o direito de tomar conhecimento do que a seu respeito constar dos ordenadores informáticos e do fim a que se destinam as informações, bem como o direito à rectificação dos dados errados e à eliminação dos que violem a intimidade da sua vida privada.
2. A informática não poderá ser usada como registo de dados respeitantes a convicções políticas, fé religiosa e vida privada.
3. É proibida a atribuição de um número aos cidadãos em substituição do nome para fins repressivos ou de identificação.

O artigo 35.º da CRP teve origem no projeto de Constituição apresentado à Assembleia Constituinte, em julho de 1975, pelo Partido Socialista (PS), que foi o único partido a propor a inclusão de norma constitucional que defendesse o direito à proteção de dados no contexto da utilização da informática.

Assim, no Título II daquele projeto, que acolhia os Direitos, liberdades e garantias fundamentais do cidadão, constava um **artigo 17.º**, que garantia o direito a todos os cidadãos de «tomar conhecimento» dos seus dados pessoais que constassem de «ordenadores informáticos» e dos fins a que se destinavam tais informações, bem como o direito à retificação dos «dados errados» e «à eliminação dos que violem a intimidade da sua vida privada».

Nesta proposta inicial já se consagrava que a informática não podia ser usada «como registo de dados respeitantes a convicções políticas, fé religiosa e vida privada». Por último, num n.º 3, estabelecia-se a proibição de «atribuição de um número único aos cidadãos em substituição do nome para fins repressivos ou de identificação».

Após estas normas terem descido à discussão na especialidade, na Comissão dos Direitos e Deveres Fundamentais, estava aprazada para o dia 28 de agosto de 1975 a votação do parecer da Comissão, no qual a matéria relativa à proteção de dados tinha sido renumerada para o **artigo 22.º**.

No entanto, a Mesa da Comissão parlamentar comunica que tem uma proposta de substituição de todo o artigo do PS, que é lida pela deputada socialista Emília Melo. Esta nova proposta continha alterações aos três primeiros números e aditava um n.º 4, onde se propunha que fosse criada por lei uma Comissão de Inspeção de Informática para defesa dos cidadãos contra a utilização abusiva da informática, cujas funções seriam definidas posteriormente pela Assembleia Legislativa Popular.

A deputada Emília Melo era licenciada em Ciências Matemáticas e desempenhou funções profissionais como analista de sistemas, o que lhe dava naturalmente uma perspetiva mais próxima das potenciais utilizações da informática. Daí talvez que o PS tenha apresentado alterações ao seu próprio projeto.

Uma vez que os grupos parlamentares tinham recebido cópias desta proposta de substituição, a votação do artigo prossegue número a número, a pedido do deputado do Partido Comunista Português (PCP) Vital Moreira.

Os números 1 e 2 do artigo são votados por unanimidade. O n.º 3, que consagra a proibição de atribuição de um número nacional único aos cidadãos, é objeto de um pedido de esclarecimento por parte do deputado Vital Moreira: *É apenas para pedir um esclarecimento aos autores da proposta de alteração, neste sentido: Em primeiro lugar, qual é a diferença entre esta nova redação; em segundo lugar, quais as razões que motivaram a alteração; em terceiro lugar, se esta redação tem algo a ver ou tem alguma relevância para a prática, que hoje creio ser comum, de atribuir permanentemente o mesmo número aos bilhetes de identidade dos cidadãos. Os autores da proposta desculparão as perguntas de leigo nesta matéria.*

Ao que a deputada Emília Melo responde: *Não temos nada que desculpar. É natural que agora sejamos nós, informáticos, a maçar, quando os advogados já nos maçaram tanto tempo.*

No diário da Assembleia Constituinte n.º 38, página 1059, foram registados 'risos'.

A deputada proponente explicou: *a ideia de número nacional significa um número único que identifica o cidadão, que acompanha o cidadão desde que nasce até à morte. (…), há efetivamente teses, e que me parecem com fundamento, para rejeitar a criação desse número, pelo menos enquanto não forem conseguidas condições de um controle perfei-*

tamente claro sobre ele. Porque leva a uma certa radiografia da vida privada dos cidadãos (…) É nesse sentido e não no sentido de número de identidade, porque o número de identidade é um, o número de beneficiário da previdência é outro, o número da carta de condução é outro. Evidentemente, todos esses números existem. Mas este número nacional seria um número único.

O n.º 3 do artigo foi então aprovado com 1 abstenção. Quanto ao n.º 4, houve um debate mais alargado. O deputado Vital Moreira defendeu que era excessivo consagrar constitucionalmente a existência de uma Comissão *dando-lhe já um nome, com letras grandes e tudo.* Propôs que a redação do n.º 4 apenas previsse o seguinte: *«A lei assegurará a defesa dos cidadãos contra a utilização abusiva da informática.»*. Na mesma linha, pronunciou-se o deputado Luís Catarino, do Movimento Democrático Português (MDP/CDE), suscitando dúvidas sobre a inclusão na Constituição de uma comissão de técnicos.

A deputada Emília Melo contrapôs, defendendo a inclusão no texto constitucional da criação de uma Comissão de Inspeção da Informática: *(…) parece-me aqui que é de pôr, na medida em que os programas que são corridos no computador, os registos e a obtenção desses registos em disco ou noutro suporte magnético são coisas que, efetivamente, só pessoas ligadas à matéria podem interpretar. Portanto, (…) a matéria dela [da lei] tem de ser interpretada e julgada por pessoas ligadas à informática.*

O n.º 4 acabou por ser aprovado, com 16 votos contra e 3 abstenções. Estava, pois, aprovado o artigo 22.º com a nova redação proposta pelo PS ao seu próprio projeto inicial.

Mas a discussão parlamentar em torno do teor do artigo 22.º extravasou para o exterior. Na sessão do dia 3 de setembro de 1975, o secretário da Comissão lê, na íntegra, um telegrama da Associação Portuguesa de Informática, relativo ao artigo 22.º já aprovado na especialidade:

Tendo tido conhecimento jornais intervenção Deputada Emília Melo sobre informática lamentamos inclusão sob forma indicada artigo 22.º Constituição sem estudo profundo consequências nível informática nacional e não só que não temos conhecimento ter sido efetuado solicitamos sua intervenção Deputada discuta assunto nível profissional intermédio desta Associação com trabalhadores sector visto discussão assunto Assembleia enfermar desconhecimento informática pela Assembleia e pessoas em geral reservamos direito Associação efetuar parecer final sobre este assunto e aprovação dada artigo. Presidente direção Porto. Presidente direção Lisboa. Associação Portuguesa Informática.

Por fim, na sessão do dia 2 de abril de 1976, dia em que foi aprovada a Constituição, é aceite a proposta da Comissão de Redação, que prevê a eliminação do tão controverso n.º 4 do artigo 22.º, consolidando-se assim o texto constitucional nos três primeiros números do renumerado *a final* **artigo 35.º da Constituição de 1976, com a epígrafe "Utilização da informática".**

A evolução do texto constitucional

Artigo 35.º (Utilização da informática)

1970

1ª lei de proteção de dados (LPD), Estado de Hesse, Alemanha

1973

LPD na Suécia

1976

1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização.
2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
3. É proibida a atribuição de um número nacional único aos cidadãos.

1981

Convenção 108

1982

1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos informáticos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização.
2. São proibidos o acesso a terceiros a ficheiros com dados pessoais e a respetiva interconexão, bem como os fluxos de dados transfronteiras, salvo em casos excecionais previstos na lei.
3. A informática não pode ser usada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate do processamento de dados estatísticos não individualmente identificáveis.
4. A lei define o conceito de dados pessoais para efeitos de registo informático.
5. É proibida a atribuição de um número nacional único aos cidadãos.

50 anos CSM Conselho Superior da Magistratura

A evolução do texto constitucional

Artigo 35.º (Utilização da informática)

1989

1. Todos os cidadãos têm o direito de tomar conhecimento dos dados constantes de ficheiros ou registos informáticos a seu respeito e do fim a que se destinam, podendo exigir a sua retificação e atualização, sem prejuízo do disposto na lei sobre segredo de Estado e segredo de justiça.
2. É proibido o acesso a ficheiros e registos informáticos para conhecimento de dados pessoais relativos a terceiros e respetiva interconexão, salvo em casos excecionais previstos na lei.
3. A informática não pode ser usada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate do processamento de dados estatísticos não individualmente identificáveis.
4. A lei define o conceito de dados pessoais para efeitos de registo informático, bem como de bases e bancos de dados e respetivas condições de acesso, constituição e utilização por entidades públicas e privadas.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A lei define o regime aplicável aos fluxos de dados transfronteiras, estabelecendo formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

1991

Lei n.º 10/91

1994

Estabelecimento da CNPDPI

1995

Diretiva 95/46/CE

1997

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
3. A informática não pode ser usada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido o livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

1998

Lei n.º 67/98

2009

Carta dos Direitos Fundamentais da UE

2016

Novo regime de proteção de dados da UE

© arquivo DN

CSM aprova recomendações sobre uso de IA

O CSM aprovou, no Plenário de 8 de abril de 2026, um conjunto de recomendações para o uso de inteligência artificial por juízes dos tribunais judiciais no exercício da atividade jurisdicional, com vista a uma utilização responsável destas ferramentas tecnológicas na atividade judicial.

Atendendo a que o uso de inteligência artificial por uma autoridade judiciária é classificado como de risco elevado, de acordo com o Regulamento de Inteligência Artificial, a sua utilização pelos juízes deve obedecer a um decálogo de princípios: princípio do controlo humano eficaz; princípio da não substituição dos juízes; princípio da responsabilidade judicial; princípio da independência judicial; princípio do respeito pelos direitos fundamentais; princípios da confidencialidade e da segurança; princípio da prevenção dos vieses algorítmicos; princípios da proporcionalidade e da utilização limitada; princípio da formação e capacitação; princípio da transparência (cf. artigo 3.º das recomendações).

A proteção de dados pessoais assume um papel de relevo nestas recomendações (cf. artigo 9.º), estabelecendo-se que, no exercício da sua atividade judicial, os juízes devem utilizar sistemas de IA em plena conformidade com a legislação de proteção de dados, devendo ser garantidos os princípios aplicáveis aos tratamentos, reconhecidos no artigo 5.º do RGPD.

O documento alerta para o facto de a eventual utilização de elementos processuais, não anonimizados, em sistemas de inteligência artificial abertos, poder comprometer os dados pessoais dos intervenientes processuais, pelo que os juízes não podem, em caso algum, fornecer ou utilizar dados judiciais nestes sistemas de IA, devendo qualquer elemento processual estar devidamente anonimizado (cf. n.ºs 3 e 4 do artigo 8.º).

Nesse contexto, o CSM estabelece que só devem ser usados os sistemas disponibilizados pelo sistema de informação de suporte à atividade dos tribunais, desde que previamente validados pelo CSM, ou diretamente fornecidos pelo CSM.

Os sistemas de IA utilizados pelos juízes no exercício da sua atividade jurisdicional devem incorporar medidas técnicas e organizativas adequadas que garantam a segurança dos dados tratados, a prevenção do acesso não autorizado, a rastreabilidade das operações e a impossibilidade de reutilização dos dados para fins diferentes daqueles para os quais foram tratados (cf. n.º 5 do artigo 9.º).

As recomendações foram elaboradas pelo Grupo de Acompanhamento da Inteligência Artificial (GAIA) do CSM, no qual também participa a Encarregada da proteção de dados. ■

Saber+
Recomendações no uso de inteligência artificial, CSM, 8/4/2026

Livre fluxo de dados entre UE e Brasil

A Comissão Europeia adotou a Decisão de Execução (UE) da Comissão 2026/179, de 26 de janeiro de 2026, ao abrigo do artigo 45.º do RGPD, reconhecendo o Brasil como um país terceiro que oferece um nível adequado de proteção de dados, o que permite a transferência livre de dados da UE, Islândia, Liechtenstein e Noruega para o Brasil. Em contrapartida, o Brasil aprovou decisão equivalente, a Resolução 32 de 26 de janeiro de 2026, considerando a UE como um destino seguro para a transferência de dados pessoais. Com este acordo mútuo, que confirma que os respetivos níveis de proteção são comparáveis, criou-se a maior área do mundo para fluxos seguros de dados transfronteiras, constituída pelo Brasil e pelos 29 países do Espaço Económico Europeu, abrangendo mais de 670 milhões de pessoas. ■

Feito por humanos

A palavra ELIZA

Primeiro *chatbot* do mundo, criado por Joseph Weizenbaum, no MIT, em 1966. Foi um programa pioneiro de processamento em linguagem natural que surpreendeu toda a gente pela sua capacidade de mimar uma conversa humana, apesar de não ter uma efetiva compreensão das palavras que processava. ELIZA foi concebido para simular uma conversa com um psicoterapeuta 'rogeriano', através de simples correspondência de padrões e de regras pré-definidas para gerar respostas às questões dos utilizadores, que, ao dialogarem com o ELIZA, sentiam estar genuinamente a conversar com uma pessoa que entendia as suas emoções e preocupações. Apesar de os utilizadores saberem que estavam a relacionar-se com uma máquina, ainda assim reportavam sentir-se compreendidos e apoiados pelo ELIZA. Uma ilusão de empatia. Este fenómeno, conhecido como o 'efeito ELIZA', revelou bastante sobre a psicologia humana e a nossa tendência para antropomorfizar as máquinas, atribuindo-lhes qualidades humanas que elas não têm. Apesar da sua simplicidade, o impacto real do ELIZA na IA e na computação foi profundo, pois demonstrou que as máquinas podem dialogar com os humanos, o que abriu caminho para o desenvolvimento dos *chatbots* modernos e dos assistentes virtuais com quem interagimos nos dias de hoje.

(Disponível em https://liacademy.co.uk/the-story-of-eliza-the-ai-that-fooled-the-world/)

Saber+
Artigo de Joseph Weizenbaum, 'Computational Linguistics', 1966
ELIZA como uma história do presente, 2019
Sobre os perigos dos papagaios estocásticos, 2021

Judiciary Tech Summit

Judiciary tech summit
LISBOA '26

Realiza-se entre os dias 18 e 20 de novembro de 2026, no Pavilhão de Portugal, em Lisboa, a Judiciary Tech Summit, um evento internacional dedicado à utilização da tecnologia nos sistemas de justiça, na sua vertente de aplicação prática ao trabalho dos tribunais. Ao longo dos três dias, será possível conhecer experiências concretas, soluções em desenvolvimento e projetos já concretizados nesta área. A cimeira contará com a participação de figuras reconhecidas no panorama internacional e provenientes de diferentes continentes para partilhar as inovações mais recentes no domínio da tecnologia aplicada ao judiciário, a par de estimulantes debates em jeito de tertúlia, masterclasses, e uma feira tecnológica para que as empresas possam mostrar os seus projetos e as suas soluções tecnológicas mais recentes. Estão ainda previstas outras atividades de relevo que serão divulgadas brevemente.

A primeira edição da Judiciary Tech Summit tem um significado especial por se realizar no ano em que o CSM celebra os seus 50 anos. Este evento é organizado pelo CSM em conjunto com a Faculdade de Direito de Lisboa (FDUL), o AI Innovation Lab by FDUL e o Centro Nacional de Inovação Jurídica.

Não se esqueça, *save the date!*

10 anos de novo regime de proteção de dados

Assinalou-se no dia 27 de abril de 2026 uma década sobre a publicação do Regulamento (UE) 2016/679 (RGPD) e da Diretiva (UE) 2016/680, relativa ao tratamento de dados pelas autoridades competentes para a investigação e repressão de infrações penais. Estes dois instrumentos jurídicos constituem o novo quadro legal em matéria de proteção de dados pessoais na UE, revogando, respetivamente a Diretiva de Proteção de Dados e a Decisão-Quadro 2008/977/JAI do Conselho.

Enquanto a diretiva careceu de transposição pelos Estados-Membros, o regulamento é diretamente aplicável em todos os Estados-Membros da União e é extensível aos restantes países do Espaço Económico Europeu (EEE).

O RGPD entrou em aplicação no dia 25 de maio de 2018, ou seja, há precisamente oito anos. O período de dois anos entre a entrada em vigor e a sua aplicação deu tempo aos Estados-Membros para realizarem os ajustes legislativos necessários à execução do regulamento e permitiu às organizações públicas e privadas prepararem-se para a transição para o novo regime jurídico de proteção de dados pessoais.

Em Portugal, o quadro legal foi completado pela Lei n.º 58/2019, de 8 de agosto, que dá execução ao RGPD e pela Lei n.º 59/2019, de 8 de agosto, que transpõe para o direito interno a Diretiva (UE) 2016/680.

50 anos CSM Conselho Superior da Magistratura

Feito por humanos

O número

73

Percentagem de indivíduos em Portugal que afirma utilizar dispositivos IoT (Internet of Things) conectados à Internet. A proliferação de dispositivos deste tipo levou a um aumento do número de vulnerabilidades, que são frequentemente exploradas para fins maliciosos.

(Relatório Cibersegurança em Portugal, 7.ª edição, abril 2026)

Novo membro na equipa do SPD

O Serviço da Proteção de Dados (SPD) do CSM tem um novo membro na sua equipa desde abril deste ano. É a técnica superior Luisa Pedroso Macedo, que veio preencher o lugar deixado vago pela colega Márcia Faro, a quem desejamos os maiores sucessos na sua nova aventura profissional. Recomposta a equipa, o SPD continua a todo o vapor a desempenhar as suas funções na garantia dos direitos dos titulares e para assegurar a conformidade dos tratamentos de dados pessoais efetuados pelo CSM com o quadro legal aplicável de proteção de dados. ■

Cibersegurança
Boas & Práticas

A Constituição protege os cidadãos quanto ao tratamento dos seus dados pessoais. Mas os cidadãos, enquanto utilizadores de sistemas e aplicações informáticas, também desempenham um papel muito importante na defesa dos dados pessoais, seja em contexto profissional, seja em contexto privado. Alcançar uma proteção eficaz passa muitas vezes por gestos simples, como bloquear o ecrã ou aplicar políticas de conservação para evitar que a informação seja armazenada durante mais tempo do que o necessário.
Aqui ficam algumas dicas práticas para o dia-a-dia.
Pequenos gestos, grandes proteções!

#1 Levantou-se? Bloqueou.

Basta uma ausência de poucos segundos para que informação pessoal ou processual, contendo dados pessoais, e por vezes de natureza confidencial, fique exposta a quem passa. Um ecrã desbloqueado pode revelar, designadamente, conteúdo de e-mails, documentos, identificação de terceiros, acessos a outras plataformas.

Porquê?

- A exposição visual também pode comprometer dados pessoais;
- Em gabinetes partilhados, salas de audiência, balcões ou outros espaços comuns, as pessoas em redor podem ver informação que não lhes é destinada;
- Terceiros podem facilmente realizar operações no seu computador, logo em seu nome;
- Bloquear o computador é uma medida simples, rápida e eficaz que ajuda a prevenir acessos indevidos, mesmo que acidentais.

O que deve fazer:

- Sempre que se ausentar, bloqueie o computador;
- Feche documentos sensíveis quando deixar de os utilizar;
- Evite deixar plataformas abertas sem necessidade;
- Tenha especial cuidado em salas partilhadas, atendimento ao público e videoconferências.

Como fazer:

No Windows, pressione: ⊞ Windows + L
O computador fica imediatamente bloqueado, mantendo a sessão aberta, mas impedindo o acesso por terceiros. Duas teclas e já está!

50 anos CSM Conselho Superior da Magistratura

Glossário de A a Z

Domínio de topo

É um dos componentes dos endereços de Internet, o que aparece em último lugar, e corresponde a um domínio de primeiro nível (em inglês, usada a sigla TLD – Top-Level Domain) na hierarquia do sistema de nomes de domínio (DNS – Domain Name System). Há duas grandes classes de domínios de topo: TLD genéricos, com mais de duas letras (por exemplo: .org, .com, .net, .edu) e TLD de código de país, com apenas duas letras (por exemplo: .pt, .uk, .br, .mz). A Autoridade para a Atribuição de Números na Internet (IANA) mantém uma lista de todos os domínios de topo válidos.

[fonte: www.icann.org]

Encriptação

Utilização de uma cifra na conversão de uma mensagem original numa mensagem não inteligível (criptograma), que não permita a sua leitura por pessoas não autorizadas. Sinónimo de cifragem. Não deve ser confundido com "codificação", que tem um significado diferente.

[fonte: www.apdsi.pt]

Firewall

Uma firewall é um sistema de segurança de rede de computadores que restringe o tráfego da Internet para, de ou em uma rede privada. Esse software ou unidade de hardware-software dedicada funciona bloqueando ou permitindo a entrada de pacotes de dados de forma seletiva. É uma ferramenta de segurança, que atua como um filtro, analisando o tráfego de rede e separando o confiável do não confiável.

[fonte: www.kasperski.com.br]

#2 Retenção não é esquecimento: é organização com prazo

Nem todos os e-mails devem ser guardados para sempre. Também nem todos devem ser logo apagados. Entre estes dois extremos existem prazos de conservação, que podem resultar da legislação de proteção de dados, relacionados com a finalidade para a qual os dados foram recolhidos, de normas arquivísticas, de outra legislação específica ou de políticas internas da organização.

No Outlook, esta gestão pode surgir de duas formas diferentes: através de políticas de retenção, definidas e configuradas pela organização, ou através de funcionalidades de arquivo automático, quando disponíveis na versão do Outlook utilizada.

Pode ser o utilizador a definir para os seus emails quanto tempo vai conservar as mensagens e os dados pessoais delas constantes. Diferentes prazos podem ser aplicados a pastas ou a mensagens específicas, conforme as opções disponibilizadas.

Porquê?

- Evita guardar dados pessoais por mais tempo do que o necessário;
- Ajuda a cumprir regras legais, arquivísticas ou institucionais;
- Reduz a acumulação de mensagens antigas nas caixas de correio;
- Permite tratar de forma diferente mensagens que exigem conservação específica.

Como fazer:

No novo Outlook:

- **Aplicar política a uma pasta:** Botão direito do rato sobre a pasta → Atribuir política → escolher política disponível;
- **Aplicar política a uma mensagem:** Botão direito do rato sobre a mensagem → Ações Avançadas → Atribuir política → escolher política disponível.

No Outlook Clássico:

- **Aplicar política a uma pasta:** Botão direito do rato sobre a pasta → Propriedades… → separador Política → escolher política disponível;
- **Aplicar política a uma mensagem:** Botão direito do rato sobre a mensagem → Atribuir política → escolher política disponível.

Nota: As políticas disponíveis são definidas pela organização. O utilizador pode escolher entre as opções existentes, mas normalmente não cria políticas novas.
Quando disponível no Outlook clássico, o "Arquivar Automaticamente" pode mover ou eliminar mensagens antigas.

FICHA TÉCNICA
Newsletter #5 maio 2026

EDIÇÃO
Serviço de Proteção de Dados do CSM
Clara Guerra, Filipe Matias e Luísa Pedroso

DESIGN E PAGINAÇÃO
Luísa Castelo dos Reis
Sardine & Carbone, Lda

DISTRIBUIÇÃO
no website do CSM
por email e através do Iudex

CONTACTOS
epd@csm.org.pt
www: csm.org.pt
T. +351 213 220 020