CONFERÊNCIA INTERNACIONAL
COMEMORAÇÃO DO 30.º ANIVERSÁRIO
ASSEMBLEIA DA REPÚBLICA
24 DE JUNHO DE 2024

PROTEÇÃO DE DADOS PESSOAIS

QUE FUTURO ESTAMOS A CONSTRUIR?

PERSONAL DATA PROTECTION

BUILDING THE FUTURE

INTERNATIONAL CONFERENCE
30TH ANNIVERSARY CELEBRATION
PORTUGUESE PARLIAMENT
24 JUNE 2024

CNPD
Comissão Nacional de Proteção de Dados

30 ANOS

CONFERÊNCIA INTERNACIONAL
COMEMORAÇÃO DO 30.º ANIVERSÁRIO
ASSEMBLEIA DA REPÚBLICA
24 DE JUNHO DE 2024

PROTEÇÃO DE DADOS PESSOAIS

QUE FUTURO ESTAMOS A CONSTRUIR?

PERSONAL DATA PROTECTION

BUILDING THE FUTURE

INTERNATIONAL CONFERENCE
30TH ANNIVERSARY CELEBRATION
PORTUGUESE PARLIAMENT
24 JUNE 2024

CNPD
Comissão Nacional de Proteção de Dados

30 ANOS

TÍTULO
Conferência Internacional – Comemoração do 30.º Aniversário da CNPD

COORDENAÇÃO
CNPD

AUTOR
VV.AA.

DESIGN GRÁFICO, PAGINAÇÃO, REVISÃO E EDIÇÃO
SKA Brand Development

IMPRESSÃO E ACABAMENTO
Selecor Artes Gráficas

LOCAL E DATA DE EDIÇÃO
Lisboa, dezembro de 2025

DEPÓSITO LEGAL: **557318/25**
EDIÇÃO n.º **1**

TITLE
International Conference – CNPD's 30th Anniversary Celebration

COORDINATION
CNPD

AUTHOR
VV. AA.

GRAPHIC DESIGN, LAYOUT, PROOFREADING AND EDITING
SKA Brand Development

PRINTING
Selecor Artes Gráficas

PLACE AND DATE OF PUBLICATION
Lisbon, December 2025

LEGAL DEPOSIT: **557318/25**
EDITION No. **1**


PAULA
MEIRA LOURENÇO

ÍNDICE CONTENTS

MENSAGEM DA PRESIDENTE DA CNPD

MESSAGE FROM THE PRESIDENT OF CNPD

MENSAGEM DE PRESIDENTE DA CNPD

Assinalamos o 30.º aniversário da Comissão Nacional de Proteção de Dados (CNPD), instituída no dia 7 de janeiro de 1994, com a publicação desta obra que reúne as intervenções da Conferência Internacional comemorativa da efeméride, sob o tema "PROTEÇÃO DE DADOS PESSOAIS: QUE FUTURO ESTAMOS A CONSTRUIR?", que se realizou no dia 24 de junho de 2024, na Sala do Senado da Assembleia da República, órgão de soberania junto do qual a CNPD funciona e com o qual tem mantido uma excelente cooperação institucional ao longo de três décadas.

Esta obra transcende a mera compilação das intervenções realizadas durante o evento, assumindo-se como um testemunho histórico da evolução da proteção de dados em Portugal e da atuação da CNPD ao longo de trinta anos, e constituindo ainda uma reflexão centrada no futuro e nas soluções adequadas aos desafios que se colocam à defesa do direito humano fundamental à proteção de dados pessoais, pedra angular da missão da CNPD.

Com efeito, o direito humano fundamental à proteção de dados pessoais, consagrado no artigo 12.º da Declaração Universal dos Direitos Humanos (DUDH), no artigo 8.º da Convenção Europeia dos Direitos Humanos (CEDH), no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), no artigo 16.º do Tratado de Funcionamento da União Europeia (TFUE), e no artigo 35.º da Constituição da República Portuguesa (CRP) – tendo Portugal sido pioneiro, a nível mundial, na sua previsão como direito fundamental na sua Constituição, a sua Lei Fundamental –, é a pedra angular dos princípios da dignidade da pessoa humana[1], da igualdade e da não discriminação, em razão de ascendência, sexo, raça, etnia, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual[2], do direito à reserva da intimidade da vida privada, à identidade pessoal, à identidade genética do ser humano, ao desenvolvimento da personalidade, ao bom nome, à reputação e à imagem[3], e bem assim do direito à liberdade[4] e o direito à liberdade de expressão[5] – direitos, liberdades e garantias constitucionais que assumem particular relevância em ambiente digital, e que é essencial debater, numa visão multidisciplinar, para enfrentar os desafios éticos e legais que se colocam às pessoas, à vida coletiva e ao Estado de direito democrático.

Trata-se de direitos fundamentais, direitos humanos, que emergiram há cerca de 50 anos com a democracia, com o eclodir do Estado de direito democrático, e que desde 1976 têm assento na Constituição da República Portuguesa.

A CNPD é a Autoridade Nacional de Controlo, a Autoridade administrativa independente que tem por atribuição controlar e fiscalizar o cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD), e da Lei n.º 58/2019, de 8 de agosto, que assegura a execução na ordem jurídica interna do RGPD, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.

Ora, os momentos de celebração implicam olhar para o nosso legado histórico enquanto instituição pública, pois não há ação, sem raízes, mas, concomitantemente, importa termos uma

1. *Artigo 1.º da DUDH e artigo 1.º da CRP.*
2. *Artigos 2.º e 7.º da DUDH, artigo 14.º da CEDH e artigo 13.º da CRP.*
3. *Artigo 12.º. da DUDH, artigo 8.º da CEDH e artigo 26.º da CRP.*
4. *Artigos 3.º da DUDH, artigo 5.º da CEDH e artigo 27.º da CRP.*
5. *Artigo 19.º da DUDH, artigo 10.º da CEDH, e artigo 37.º da CRP.*

visão prospetiva, capaz de avaliar os desafios e as oportunidades que o futuro nos coloca, sobretudo na Era digital, e propor soluções eficazes. Foi este o mote da nossa Conferência, cujo sucesso justifica a publicação da presente obra, para memória histórica e futura reflexão, aproveitando a presença de Oradores provenientes de vários espaços geográficos que vieram refletir connosco o futuro do direito à proteção de dados pessoais, à escala global, na sua interação com outros direitos digitais e na sua relação com outras dimensões da sociedade, num contexto de evolução tecnológica sem precedentes.

Estamos convictos que a divulgação das intervenções da Presidente do Comité Europeu para a Proteção de Dados, da Autoridade Europeia para a Protecção de Dados, da Relatora Especial da Organização das Nações Unidas para o Direito à Privacidade, da Diretora da Agência Espanhola de Proteção de Dados, do Presidente da Comissão Nacional de Proteção de Dados de Cabo Verde, da Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais do México, que detinha a Presidência da Rede Ibero-americana de Proteção de Dados, e de um Professor Associado do Instituto Superior Técnico da Universidade de Lisboa, com o tema da proteção de dados pessoais na Era da inteligência artificial generativa, constitui um passo relevante na promoção do conhecimento do direito fundamental à proteção de dados pessoais e direitos, liberdades e garantias conexos, que desejamos aprofundar.

Gostaríamos de deixar um agradecimento especial a Sua Excelência o Presidente da Assembleia da República, a Casa da Democracia, Deputado José Pedro Aguiar-Branco, que nos deu a honra do encerramento da nossa Conferência, a todos os Oradores, a todos aqueles que contribuíram para a elaboração desta publicação, e bem assim um agradecimento a todos aqueles que integram ou integraram a CNPD ao longo destes 30 anos, pois é a sua competência, empenho e profissionalismo que permite assegurar a excelência no desempenho da missão da CNPD de forma totalmente independente, isenta, imparcial e transparente, enquanto Autoridade Nacional de Controlo do direito fundamental à proteção de dados pessoais, e direitos, liberdades e garantias conexos, de referência nacional e internacional, nestas três décadas de história ao serviço de Portugal.

A Presidente da CNPD
Paula Meira Lourenço

MESSAGE FROM THE PRESIDENT OF THE CNPD

We celebrate the 30th anniversary of the Comissão Nacional de Proteção de Dados (CNPD), the Portuguese Data Protection Supervisory Authority, established on 7 January 1994, with this publication that brings together the interventions from the International Conference commemorating our anniversary, under the theme "PERSONAL DATA PROTECTION: BUILDING THE FUTURE", which took place on 24 June 2024, in the Senate Room of the Portuguese Parliament (called the Assembleia da República), within which the CNPD operates and with which it has maintained excellent institutional cooperation.

This publication transcends the mere compilation of interventions made during the event, becoming a historical testimony of the evolution of data protection in Portugal and of CNPD`s activity over thirty years, being also a reflection focused on the future and on the appropriate solutions to the challenges facing the defense of the fundamental human right to the protection of personal data, the cornerstone of the CNPD's mission.

The fundamental human right to the protection of personal data, enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR), Article 8 of the European Convention on Human Rights (ECHR), Article 8 of the Charter of Fundamental Rights of the European Union (CFREU), Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 35 of the Constitution of the Portuguese Republic (CPR) – being Portugal a global pioneer in enshrining this right as a fundamental right in its Constitution – is the cornerstone of the principles of human dignity[1], equality and non-discrimination on grounds of descent, sex, race, ethnicity, language, territory of origin, religion, political or ideological beliefs, education, economic situation, social condition or sexual orientation[2], the right to privacy, personal identity, the genetic identity of the human being, of personality development, good name, reputation and image[3], as well as the right to liberty[4] and the right to freedom of expression[5]– constitutional rights, freedoms and guarantees that are particularly relevant in the digital environment, and that it is essential to discuss, in a multidisciplinary vision, how to address the ethical and legal challenges faced by individuals, by collective life and the democratic rule of law.

These are fundamental rights, human rights, which emerged about 50 years ago with democracy, with the outbreak of the democratic rule of law, and which have been enshrined in the Constitution of the Portuguese Republic since 1976.

The CNPD is the Portuguese Data Protection Supervisory Authority, an independent administrative Authority whose task is to monitor and supervise compliance with the General Data Protection Regulation (GDPR) and Law 58/2019 of 8 August 2019, which implements the GDPR in the domestic legal order, as well as other legal and regulatory provisions on the protection of personal data, in order to defend the rights, freedoms and guarantees of natural persons in the context of the processing of personal data.

Now, the moments of celebration imply looking at our historical legacy as a public institution, because there is no action without roots. At the same time, we need a forward-looking vision, able to assess the challenges and opportunities that the future presents us, especially in the digital Era, and to propose effective solutions. This was the main theme of our Conference,

1. *Article 1 of the UDHR and Article 1 of the CPR.*
2. *Articles 2 and 7 of the UDHR, Article 14 of the ECHR and Article 13 of the CPR.*
3. *Article 12 UDHR, Article 8 ECHR and Article 26 CPR.*
4. *Articles 3 of the UDHR, Article 5 of the ECHR and Article 27 of the CPR.*
5. *Article 19 of the UDHR, Article 10 of the ECHR, and Article 37 of the CPR.*

and its success justifies the present publication for historical memory and future reflection, taking advantage of the presence of Speakers from various geographical spaces who have come to reflect with us the future of the fundamental right to the protection of personal data, on a global scale, in its interaction with other digital rights and in its relationship with other dimensions of society, in a context of unprecedented technological evolution.

We are convinced that the publication of the interventions of the President of the European Data Protection Board, the European Data Protection Supervisor, the United Nations Special Rapporteur on the Right to Privacy, the Director of the Spanish Data Protection Supervisory Authority, the President of the Data Protection Supervisory Authority of Cape Verde, the Commissioner of the National Institute of Transparency, Access to Information and Protection of Personal Data of Mexico, who held the Presidency of the Ibero-American Data Protection Network, and an Associate Professor at the Instituto Superior Técnico of the University of Lisbon, on the subject of personal data protection in the Era of generative artificial intelligence, is a relevant step in promoting knowledge of the fundamental right to the protection of personal data and related rights, freedoms and guarantees, which we wish to further explore.

We would like to express our special thanks to His Excellency the President of the Portuguese Parliament, the House of Democracy, Mr José Pedro Aguiar-Branco, who has given us the honor of closing our Conference, to all the Speakers, to all those who contributed to the preparation of this publication, and also to all those who are or have been part of the CNPD over the last 30 years, because it is their competence, commitment and professionalism that allows us to ensure excellence in the performance of the CNPD's mission in a totally independent, impartial and transparent manner, as the National Supervisory Authority for the fundamental right to the protection of personal data, and related rights, freedoms and guarantees, of national and international reference throughout these three decades of history at the service of Portugal.

The President of the CNPD
Paula Meira Lourenço

INTERVENÇÕES
INTERVENTIONS

SESSÃO DE ABERTURA
OPENING SESSION


NPD

Manuel Magno

Vice-Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, da Assembleia da República

Vice-Chairman of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament

Os momentos de celebração implicam um olhar para o nosso legado histórico enquanto instituição política pois não há ação sem raízes. Concomitantemente, importa termos uma visão prospetiva, capaz de avaliar os desafios e as oportunidades que o futuro nos coloca, sobretudo na era digital e propor soluções eficazes. É, pois, indispensável que pensemos seriamente nas opções que se nos apresentam.

The moments of celebration imply a look at our historical legacy as a political institution as there is no action without roots. At the same time, it is important to have a forward-looking vision, able to assess the challenges and opportunities that the future presents us, especially in the digital age and to propose effective solutions. It is therefore essential that we give serious thought to the options before us.

Paula Meira Lourenço
Presidente da Comissão Nacional de Proteção de Dados

PROTEÇÃO DE DADOS PESSOAIS
QUE FUTURO ESTAMOS A CONSTRUIR

Exmo. Senhor Vice-Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República

Excelência

Exmo. Vice-Procurador-Geral da República

Excelência

Exma. Senhora Presidente do Grupo Parlamentar do Partido Socialista

Exmo. Senhor Vice-Presidente do Grupo Parlamentar do Partido Social Democrata

Exma. Senhora Presidente da Comissão de Saúde da Assembleia da República

Exma. Senhora Vice-Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República

Exmas. e Exmos. Senhoras e Senhores Deputados

Exmos. Senhores

Juízes Conselheiros do Tribunal de Contas

Vice-Presidente do Conselho Superior de Estatística

Vice-Governador do Banco de Portugal

Vogal do Conselho Regulador da ERC - Entidade Reguladora para a Comunicação Social

Presidentes, Vice-Presidentes e Representantes das Autoridades Reguladoras: Autoridade da Concorrência, Autoridade Nacional de Aviação Civil, Autoridade Nacional de Comunicações, Autoridade de Segurança Alimentar e Económica, Autoridade de Supervisão de Seguros e Fundos de Pensões e Comissão do Mercado de Valores Mobiliários

Vogal da Entidade para a Transparência

Vogais do Conselho de Administração da Imprensa Nacional-Casa da Moeda, SA

Presidentes das Entidades Administrativas Independentes que funcionam junto da Assembleia da República: Comissão Nacional de Eleições, Comissão de Acesso aos Documentos Administrativos, Conselho Nacional de Ética para as Ciências da Vida e Conselho de Fiscalização do Sistema Integrado de Informação Criminal

Diretor-Geral do Gabinete Nacional de Segurança

Diretores de Serviço e Chefes de Divisão da Assembleia da República

Bastonário da Ordem dos Solicitadores e Agentes de Execução

Presidente do Conselho Regional do Porto da Ordem dos Advogados

Presidente do Conselho Superior da Ordem dos Advogados

Presidente do Conselho Fiscal da Ordem dos Advogados

Presidente da Associação Para o Desenvolvimento da Sociedade de Informação

Vogais do Conselho de Administração da Ius Omnibus

Diretor Nacional e Diretor Nacional Adjunto da Polícia Judiciária

Diretor da Unidade Nacional de Combate à Corrupção da Polícia Judiciária

Inspetor da Guarda Nacional Republicana

Representante do Diretor Nacional da Polícia de Segurança Pública

Exmos. Senhoras e Senhores Presidentes e Diretores de variadíssimas instituições nacionais: Centros, Direções-Gerais, Gabinetes, Institutos e Serviços Partilhados do Ministério da Saúde, da Presidência do Conselho de Ministros, do Ministério das Finanças, do Ministério dos Negócios Estrangeiros, do Ministério da Economia, do Ministério da Justiça e do Ministério da Saúde

Antigo Presidente da CNPD, Mestre Luís Lingnau da Silveira

Secretária Executiva da Comissão Nacional da UNESCO do Ministério dos Negócios Estrangeiros

Representantes do Ministro Adjunto e da Coesão Territorial, da Secretária da Estado da Saúde, do Secretário de Estado da Gestão da Saúde, do Secretário de Estado da Administração Interna, do Secretário de Estado Segurança Social, da Secretária de Estado da Cultura e do Secretário de Estado do Turismo

Exmos. Senhoras e Senhores Presidentes e Diretores de variadíssimas instituições nacionais e internacionais, como seja, as Universidades, Faculdades e Autoridades de Proteção de Dados de Angola, Brasil, Cabo Verde, Croácia, Finlândia, Espanha, Marrocos, México, Polónia, São Tomé e Príncipe, e Uruguai.

Presidente da Associação Internacional de Oficiais de Justiça e Agentes de Execução

Excelentíssimos Oradores desta Conferência Internacional

Excelentíssimos Encarregados de Proteção de Dados de várias organizações aqui presentes

Minhas Senhoras e meus Senhores,

Em nome da Comissão Nacional de Proteção de Dados de Portugal, é uma honra dar-vos as boas vindas, aqui, na Assembleia da República, Casa da Democracia, nesta lindíssima Sala do Senado, à Conferência Internacional "Proteção de Dados Pessoais: que futuro estamos a construir", comemorativa do 30.º aniversário da Comissão Nacional de Proteção de Dados, na sua atividade de proteção do direito fundamental à proteção de dados pessoais, ao serviço de Portugal, de forma independente, isenta, objetiva, imparcial e transparente, assegurando o estrito cumprimento da lei.

On behalf of the Portuguese Data Protection Supervisory Authority, it is an honor to welcome you, here, at the Portuguese Parliament, the House of Democracy, in this beautiful Senate Room, to the International Conference "Personal Data Protection: Building the Future", commemorating the 30th anniversary of the Portuguese Data Protection Supervisory Authority, in its activity to protect the fundamental right to the protection of personal data, and related fundamental rights, at the service of Portugal, independently, impartially, objectively, and transparently, ensuring strict compliance with the law.

Em meu nome, e em nome da Comissão Nacional de Proteção de Dados, as minhas primeiras palavras são dirigidas ao Senhor Presidente da Assembleia da República, ao Senhor Secretário-Geral da Assembleia da República, e às Senhoras e Senhores Deputados da Nação, agradecendo a disponibilidade e a gentileza em receber-nos na Casa da Democracia, no ano em que celebramos o 30.º aniversário ao serviço de Portugal, lembrando esta que é também a Casa da Comissão Nacional de Proteção de Dados –, porquanto a Comissão é uma Entidade independente que funciona junto da Assembleia da República —, e a Casa de todos nós, enquanto cidadãos.

Agradeço também ao Senhor Vice-Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, da Assembleia da República, a honra que nos deu ao presidir à sessão de abertura.

Gostaria ainda de saudar todos os Antigos Senhores Presidentes da Comissão, Antigos e atuais Vogais, a Senhora Secretária e os antigos e atuais colaboradores da Comissão – muitos dos quais presentes – e, permitam-me uma especial saudação ao Antigo Presidente Dr. Luís Lingnau da Silveira, cuja presença física neste dia muito nos honra.

Como sabemos, são as pessoas que fazem as instituições, pelo que gostaria de agradecer a todos quantos na Comissão Nacional de Proteção de Dados ajudaram – e aqueles que ainda hoje ajudam –, a construir a Comissão como um exemplo de exigência, de coragem e de desassombro, no panorama do nosso serviço público.

Gostaria ainda de saudar os Presidentes e representantes das Autoridades Nacionais de Proteção de Dados dos países de língua oficial portuguesa aqui presentes, com os quais a Comissão Nacional de Proteção de Dados sempre teve uma profícua cooperação, a qual urge reforçar. Os nossos laços históricos, o respeito pela identidade cultural e por uma visão comum de democracia, aliados à riqueza da troca de experiências e da entreajuda, como se espera com países irmãos, em cinco continentes — Angola, Brasil, Cabo Verde, Guiné Bissau, Macau, Moçambique, São Tomé e Príncipe e Timor Leste —, impelem ao reforço da cooperação de países que representam 35 Estados /distritos federais, que falam a língua portuguesa em todo o mundo.

Uma saudação especial também a todos os países da Rede Ibero-americana de Proteção de Dados (que engloba Andorra, Espanha, os países da América Latina, Portugal e Cabo Verde), fundada pela iniciativa de Portugal e de Espanha há 21 anos e, em especial, aos Presidentes, Diretores e Comissionados aqui presentes do Brasil, de Cabo Verde, de Espanha e do México.

E uma saudação especial ainda aos países da União Europeia, que faço na pessoa da Presidente do Comité Europeu para a Proteção de Dados, Prof. Doutora Anu Talus, e bem assim da Autoridade Europeia para a Proteção de Dados, Prof. Doutor Wojciech Wiewiórowski, que nos dão a honra de ser nossos Oradores nesta Conferência.

Como sabemos, em 2018, com a entrada em execução do Regulamento (UE) 2016/679 – também conhecido por Regulamento Geral sobre a Proteção de Dados (RGPD) –, assistiu-se ao reforço da cooperação entre os países do Espaço Económico Europeu no seio do Comité Europeu para a Proteção de Dados, em cujas reuniões também participa de forma muito ativa a Autoridade Europeia para a Proteção de Dados, sendo hoje crescente a utilização de instrumentos jurídicos de cooperação (assistência mútua e realização de operações conjuntas) no tratamento de casos transfronteiriços, para facilitar a obtenção de consensos, e bem assim os procedimentos de controlo da coerência, tendo em vista a interpretação e aplicação uniforme dos princípios e normas jurídicas previstas no RGPD.

Por último, uma saudação a todas as instituições públicas e privadas, com as quais a CNPD já colabora, ou que têm vindo a manifestar interesse em iniciar uma cooperação com a CNPD, designadamente:

No plano nacional (por ordem alfabética):

a. Autoridade Nacional de Comunicações;
b. Centro Internet Segura;
c. Centro Nacional de Cibersegurança;
d. Conselho de Fiscalização do Sistema Integrado de Informação Criminal e Conselho de Fiscalização da Base de Dados de Perfis de ADN;
e. Instituições do Ensino Superior e respetivos Centros de Investigação;
f. Instituto Nacional de Administração;
g. Instituto Português de Acreditação;
h. Instituto Português da Qualidade;
i. Provedoria de Justiça.

É ainda de destacar os órgãos, grupos de trabalho e fóruns europeus e internacionais em que a CNPD participa regularmente:

a. Assembleia Mundial da Privacidade (Global Privacy Assembly), e seus vários subgrupos, que organiza a Conferência Internacional;
b. Grupos de peritos do Comité Europeu para a Proteção de Dados;
c. Comité de Supervisão Coordenada para os sistemas de informação europeus;
d. Conferência Europeia de Comissários de Proteção de Dados;
e. Grupos de Trabalho da Rede Ibero-americana de Proteção de Dados.

Na data em que se assinala a abertura das comemorações do 30.º aniversário da CNPD, impõe-se uma breve nota histórica.

Desde a Constituição da República Portuguesa de 1976, Portugal reconhece a proteção de dados pessoais como direito fundamental, tendo sido pioneiro a nível mundial.

Em 1994, a CNPD entrou em funcionamento (no dia 7 de janeiro), sendo na altura designada por Comissão Nacional de Proteção de Dados Pessoais Informatizados – CNPDPI (porque a proteção de dados apenas abrangia os ficheiros informatizados e não os tratamentos de dados manuais).

A revisão constitucional de 1997 veio consagrar a existência de uma entidade administrativa independente como garante da proteção de dados (artigo 35.º da CRP), e em 1998 fixou-se a atual designação de Comissão Nacional de Proteção de Dados (CNPD), quando foi transposta para o direito português a Diretiva europeia de proteção de dados (Diretiva 95/46/CE), através da Lei n.º 67/98, de 26 de outubro, tendo sido alargado o regime jurídico de proteção aos dados manuais.

E em 2004, a CNPD passou a ter uma Lei de Organização e Funcionamento e Funcionamento, aprovada pela Lei n.º 43/2004, de 18 de agosto, com a redação dada pela Lei de Execução do RGPD (Lei n.º 58/2019, de 8 de agosto), mantendo a Comissão como um órgão colegial, composta por 7 membros, nos mesmos moldes da primeira Lei de Proteção de Dados (a Lei n.º 10/91), e criando o órgão do Fiscal Único.

A CNPD é a Autoridade Nacional de Controlo, a Autoridade administrativa independente que tem por atribuição controlar e fiscalizar o cumprimento do RGPD e da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.

No cumprimento dessa atribuição, a CNPD desenvolve a sua atividade em dois planos fundamentais: a orientação prévia e de sensibilização, e a fiscalização (sucessiva) dos tratamentos de dados pessoais, tendo em vista assegurar o respeito pelo princípio da dignidade da pessoa humana, pilar do Estado de direito democrático, consagrado no artigo 1.º da Constituição da República Portuguesa (CRP), e pelo direito fundamental à proteção dos dados pessoais (consagrado no n.º 1, do artigo 8.º, da Carta dos Direitos Fundamentais da União Europeia, no n.º 1, do artigo 16.º, do Tratado de Funcionamento da União Europeia e no artigo 35.º da CRP), o qual deve ser conjugado com outros direitos fundamentais conexos, como seja o direito à reserva da intimidade da vida privada, à identidade pessoal, à identidade genética do ser humano, ao desenvolvimento da personalidade, ao bom nome, à reputação e à imagem (artigo 26.º da CRP), e bem assim o princípio da igualdade (artigo 13.º da CRP) e o direito à liberdade (artigo 27.º da CRP) – direitos, liberdades e garantias constitucionais que assumem particular relevância, que na realidade física, quer em ambiente digital.

Sublinhe-se que se trata de direitos fundamentais, direitos humanos, que emergiram há cerca de 50 anos com a democracia, com o eclodir do Estado de direito democrático, e que desde 1976 têm assento na Constituição da República Portuguesa.

Mas se é certo que a perspetiva histórica assume uma inelutável relevância na vida das instituições, a Conferência comemorativa do nosso 30.º aniversário é marcada por uma visão prospetiva, face aos desafios mais prementes que se colocam aos cidadãos, enquanto titulares dos dados pessoais.

Por isso, a nossa Conferência conta com a participação de vários Presidentes de Autoridades e instituições europeias e internacionais, para refletir e debater o futuro da proteção de dados pessoais, na sua interação com outros direitos digitais e na sua relação com outras dimensões da sociedade, num contexto de evolução tecnológica sem precedentes, sobretudo em face das oportunidades e desafios da proteção de dados pessoais e privacidade em ambiente digital, em especial da inteligência artificial generativa.

Teremos as honrosas intervenções da Presidente do Comité Europeu para a Proteção de Dados, da Autoridade Europeia para a Proteção de Dados, da Relatora Especial da Organização das Nações Unidas para o Direito à Privacidade, da Diretora da Agência Espanhola de Proteção de Dados, do Presidente da Comissão Nacional de Protecção de Dados de Cabo Verde, da Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais do México, que detém a Presidência da Rede Ibero-americana de Proteção de Dados, e terminará com a intervenção de um Professor Associado do Instituto Superior Técnico da Universidade de Lisboa, que nos falará sobre a Proteção de Dados Pessoais na Era da Inteligência Artificial Generativa.

Sendo a proteção de dados pessoais a pedra angular dos princípios da dignidade da pessoa humana, da igualdade e da não discriminação, entre outros, e constituindo a garantia do exercício de outros direitos fundamentais, como o direito à reserva da intimidade da vida privada, o direito ao desenvolvimento da personalidade ou o direito à liberdade de expressão, é essencial debater, numa visão multidisciplinar, como enfrentar os desafios éticos e legais que se colocam às pessoas, à vida coletiva e ao Estado de direito democrático.

Senhor Vice-Presidente
Minhas Senhoras e Meus Senhores,

Em nome da Comissão Nacional de Proteção de Dados, fica o nosso reconhecimento pelo empenho de todos os nossos colaboradores, órgãos de soberania, instituições públicas e privadas, e parceiros institucionais, no esforço permanente para cumprirmos a nossa missão.

Que as comemorações dos 30 anos da CNPD permitam relembrar, com confiança e determinação, e com uma visão prospetiva, adaptada aos atuais desafios, a incontornável relevância da proteção dos dados pessoais num mundo em constante mudança, e que precisa da ação de todas e de todos.

Paula Meira Lourenço
President of the Portuguese Data Protection Supervisory Authority

PERSONAL DATA PROTECTION
BUILDING THE FUTURE

Vice-Chair of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament

Vice-Prosecutor General of the Republic

President of the Parliamentary Group of the Socialist Party

Vice-President of the Parliamentary Group of the Social Democratic Party

President of the Health Committee of the Portuguese Parliament

Vice-Chairwoman of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament

Members of the Portuguese Parliament

Judges Counsellors of the Portuguese Court of Auditors

Vice-President of the Council of Statistics

Vice-Governor of Banco de Portugal

Member of the Regulatory Board of the Portuguese Regulatory Authority for the Media

Presidents, Vice-Presidents and Representatives of Portuguese Regulatory Authorities: Competition Authority, National Civil Aviation Authority, National Communications Authority, Food and Economic Safety Authority, Insurance and Pension Funds Supervisory Authority and Securities Market Commission

Member of the Transparency Entity

Members of the Board of Directors of the Imprensa Nacional-Casa da Moeda, SA

Presidents of the Entities that operate under the aegis of the Portuguese Parliament: National Election Commission, Commission for Access to Administrative Documents, National Council of Ethics for Life Sciences, and Council for the Supervision of the Integrated Criminal Information System

Director-General of the National Security Cabinet

Service Directors and Heads of Division of the Portuguese Parliament

President of the Order of Solicitors and Enforcement Agents

President of the Porto Regional Council of the Bar Association

President of the Supreme Council of the Bar Association

Chairman of the Supervisory Board of the Bar Association

President of the Association for the Development of the Information Society

Members of the Board of Directors of Jus Omnibus

National Director and Deputy National Director of the Portuguese Criminal Investigation Police

Director of the National Anti-Corruption Unit of the Portuguese Criminal Investigation Police

Inspector of the National Republican Guard

Representative of the National Director of the Public Safety Police

Dear Sir /Madam, Presidents and Directors of many national institutions: Centres, Directorates-General, Offices, Institutes and Shared Services of the Ministry of Health, the Presidency of the Council of Ministers, the Ministry of Finance, the Ministry of Foreign Affairs, the Ministry of Economy, the Ministry of Justice and the Ministry of Health

Former President of the CNPD, Luís Lingnau da Silveira

Executive Secretary of the UNESCO National Commission of the Ministry of Foreign Affairs

Representatives of the Deputy Minister for Territorial Cohesion, the Secretary of State for Health, the Secretary of State for Health Management, the Secretary of State for Internal Affairs, the Secretary of State for Social Security, the Secretary of State for Culture, the Secretary of State for Tourism

Presidents and Directors of various national and international institutions, such as the Universities, Faculties and Data Protection Authorities of Angola, Brazil, Cape Verde, Croatia, Finland, Spain, Morocco, Mexico, Poland, São Tomé and Príncipe, and Uruguay.

President of the International Association of Judicial Officers

Dear Speakers of this International Conference

Data Protection Officers from various organisations present here.

Ladies and Gentlemen,

On behalf of the Portuguese Data Protection Supervisory Authority it is an honour to welcome you here, in the Portuguese Parliament, House of Democracy, in this beautiful Senate Room, to the International Conference "Protection of Personal Data: Building the Future", commemorating the 30th anniversary of the Portuguese Data Protection Supervisory Authority, in its activity of protecting the fundamental right to the protection of personal data, at the service of Portugal, independently, impartially, objectively, and transparently, ensuring strict compliance with the law.

On my behalf, and on behalf of the Portuguese Data Protection Supervisory Authority, my first words are addressed to the President of the Portuguese Parliament, Deputy José Pedro Aguiar-Branco, to the Secretary-General of the Portuguese Parliament, and to the Deputies and all Members of the Portuguese Parliament, thanking them for their willingness and kindness in welcoming us to the House of Democracy in the year in which we celebrate our 30th anniversary of service to Portugal, recalling that this is also the house of the Portuguese Data Protection Supervisory Authority – because the Commission is an independent entity that works with the Portuguese Parliament – our House, as citizens.

I also thank the Vice-President of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament for the honour he has given us by chairing this Opening Session.

I would also like to greet all the former Presidents of the Portuguese Data Protection Supervisory Authority, former and current Members, the Secretary and the former and current collaborators of the Commission – many of whom are present – and allow me to say a special greeting to former President Luís Lingnau da Silveira, whose physical presence on this day greatly honours us.

As we know, it is the people who make the institutions, so I would like to thank all those in the Portuguese Data Protection Supervisory Authority who helped – and those who still help today – to build the Commission as an example of demand, courage and dismay in the panorama of our public service.

I would also like to greet the Presidents and representatives of the Data Protection Authorities of the Portuguese-speaking countries present here, and our fruitful cooperation, which needs to be strengthened. Our historical ties, respect for cultural identity and for a common vision of democracy, coupled with the wealth of exchange of experiences and mutual aid, as is expected among sister countries, on five continents – Angola, Brazil, Cape Verde, Guinea Bissau, Macau, Mozambique, São Tomé and Príncipe and East Timor – encourage the strengthening of cooperation between countries representing 35 federal states /districts, which speak Portuguese around the world.

A special greeting also to all the countries of the Ibero-American Data Protection Network (encompassing Andorra, Spain, the countries of Latin America, Portugal, and Cape Verde), founded by the initiative of Portugal and Spain 21 years ago and, in particular, to the Presidents, Directors and Commissioners present here from Brazil, Cape Verde, Spain and Mexico.

And a special greeting also to the countries of the European Union, which I offer in the person of the President of the European Data Protection Board, Prof. Anu Talus, as well as the European Data Protection Supervisor, Prof. Wojciech Wiewiórowski, who give us the honour of being our Speakers at this Conference.

As we know, in 2018, with the implementation of Regulation (EU) 2016/679 – also known as the General Data Protection Regulation (GDPR) – there was a strengthening of cooperation between the countries of the European Economic Area within the European Data Protection Board (EDPB), in whose meetings the European Data Protection Supervisor (EDPS) also participates very actively, and today the use of legal cooperation instruments (mutual assistance and joint operations) is increasing in the handling of cross-border cases, to facilitate consensus-building, as well as the procedures for monitoring consistency, with a view to the uniform interpretation and application of the legal principles and rules laid down in the GDPR.

Finally, a greeting to all public and private institutions, with which the Portuguese Data Protection Supervisory Authority already collaborates, or which have expressed interest in initiating cooperation with the CNPD, namely:

At national level (in alphabetical order):

a. National Communications Authority;
b. Secure Internet Centre;
c. National Cybersecurity Centre;
d. Supervision Board of the Integrated Criminal Information System and Supervision Board of the DNA Profile Database;
e. Higher Education Institutions and their Research Centres;
f. National Institute of Administration;
g. Portuguese Accreditation Institute;
h. Portuguese Institute of Quality;
i. Portuguese Ombudsman.

Also noteworthy are the European and international bodies, working groups and fora in which the CNPD regularly participates:

a. The Global Privacy Assembly, and its various subgroups, which organises the International Conference;

b. Expert groups of the European Data Protection Board;

c. The Coordinated Oversight Committee for European Information Systems;

d. European Conference of Data Protection Commissioners;

e. Working Groups of the Ibero-American Data Protection Network.

On the date of the opening of the celebrations of the 30th anniversary of the CNPD, a brief historical note is required.

Since the Constitution of the Portuguese Republic of 1976, Portugal has recognised the protection of personal data as a fundamental right and has been a pioneer worldwide.

In 1994, the CNPD became operational (on 7 January) and was then called the National Commission for the Protection of Computerised Personal Data (CNPDPI) (because data protection covered only computerised files and not manual data processing).

The constitutional revision of 1997 established the existence of an independent administrative entity as a data protection guarantor (Article 35 of the CRP), and in 1998, the current designation of the National Data Protection Commission (Comissão Nacional de Proteção de Dados — CNPD) was established, when the European Data Protection Directive (Directive 95/46/EC) was transposed into Portuguese law, through Law 67/98, of 26 October 1998, and the legal regime for the protection of manual data was extended.

And in 2004 was approved the Law on the Organisation and Functioning of the CNPD (Law 43/2004 of 18 August 2004, as amended by the Law on the Enforcement of the GDPR – Law 58/2019, of 8 August 2019), maintaining the Commission as a collegiate body, composed of 7 members, along the same lines as the first data protection law (Law 10/91), and creating the Single Tax Auditor.

The CNPD is the National Supervisory Authority, an Independent Administrative Authority whose task is to monitor and supervise compliance with the GDPR, the Law 58/2019 of 8 August 2019, which implements the GDPR in the national legal order, as well as other legal and regulatory provisions on the protection of personal data, in order to defend the rights, freedoms and guarantees of natural persons in the context of the processing of personal data.

In fulfilling this task, the CNPD develops its activity in two fundamental plans: prior guidance and awareness-raising, and the (successive) monitoring of the processing of personal data, with a view to ensuring respect for the principle of human dignity, a pillar of the democratic rule of law, enshrined in Article 1 of the Constitution of the Portuguese Republic (CRP), and for the fundamental right to the protection of personal data (enshrined in Article 8(1) of the Charter of Fundamental Rights of the European Union, Article 16(1) of the Treaty on the Functioning of the European Union, and Article 35 of the CRP), which must be combined with other related fundamental rights, such as the right to privacy, personal identity, the genetic identity of the human being, the development of personality, good name, reputation and image (Article 26 of the CRP), as well as the principle of equality (Article 13 of the CRP) and the right to liberty (Article 27 of the CRP) – rights, freedoms and constitutional guarantees that are of particular relevance, both in physical reality and in a digital environment.

It should be emphasised that these are fundamental human rights, which emerged approximately 50 years ago with the advent of democracy and the establishment of democratic rule of law, and have been enshrined in the Constitution of the Portuguese Republic since 1976.

Although the historical perspective recognises an inevitable relevance in the life of the institutions, the Conference commemorating our 30th anniversary is marked by a forward-looking vision, in the face of the most pressing challenges facing citizens as data subjects.

Therefore, our Conference relies on the participation of several Presidents of Authorities and European and international institutions to reflect on and discuss the future of personal data protection, its interaction with other digital rights, and its relationship with other aspects of society, in a context of unprecedented technological evolution. This especially includes the opportunities and challenges of personal data protection and privacy in the digital environment, notably generative artificial intelligence (AI).

We will have the esteemed interventions from the President of the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the United Nations (UN) Special Rapporteur on the Right to Privacy, the Director of the Spanish Data Protection Supervisor Authority, the President of the Data Protection Supervisory Authority of Cape Verde, the Commissioner of the National Institute of Transparency, Access to Information and Protection of Personal Data of Mexico, who holds the Presidency of the Ibero-American Data Protection Network, and will conclude with the speech of an Associate Professor from the Instituto Superior Técnico at the University of Lisbon, who will discuss Personal Data Protection in the Era of Generative Artificial Intelligence.

Since the protection of personal data is the cornerstone of the principles of human dignity, equality and non-discrimination, among others, and is the guarantee of the exercise of other fundamental rights, such as the right to privacy, the right to personality development or the right to freedom of expression, it is essential to discuss, in a multidisciplinary perspective, how to address the ethical and legal challenges facing individuals, collective life and the democratic rule of law.

Dear Vice-President of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament
Ladies and Gentlemen,

On behalf of the Portuguese Data Protection Supervisory Authority, we acknowledge the commitment of all our employees, sovereign bodies, public and private institutions, and institutional partners, in the permanent effort to fulfil our mission.

May the celebrations of the 30th anniversary of the CNPD allow us to recall, with confidence and determination, and with a forward-looking vision, adapted to the current challenges, the unavoidable relevance of the protection of personal data in a world that is constantly changing, and that needs the action of all and everyone.

SESSÃO DA MANHÃ
MORNING SESSION


CONFERÊNCIA INTERNACIONAL
INTERNATIONAL CONFERENCE
24 JUN 2024
PROTEÇÃO DE DADOS PESSOAIS
QUE FUTURO ESTAMOS A CONSTRUIR?
BUILDING THE FUTURE
CNPD
30
CNPD

Anu Talus
Presidente do Comité Europeu para a Proteção de Dados

Anu Talus é a Comissária para a Informação finlandesa desde o outono de 2020. Chefia o Gabinete do Comissário para a Informação (TSV) e é presidente do Comité Europeu para a Proteção de Dados (CEPD). Antes de ocupar estes cargos, trabalhou como Comissária-adjunta para a Informação, de agosto de 2019 a novembro de 2020.

Antes de trabalhar no IMY, Talus foi Conselheira Sénior no Ministério da Justiça por mais de dez anos. No Ministério da Justiça, liderou a execução do RGPD na Finlândia e atuou como representante do Governo finlandês nas negociações do RGPD na UE. Talus também trabalhou na Comissão Europeia, na Unidade Proteção e Fluxos de Dados (DG Justiça e Consumidores) como perita nacional destacada (PND).

Talus é doutor em Direito e mestre em Direito pela Universidade de Helsínquia e mestre em Artes pela Universidade de Vaasa.

Anu Talus has served as the Finnish Information Commissioner since autumn 2020. She is the Head of the Office of the Information Commissioner (TSV) and the Chair of the European Data Protection Board (EDPB). Before holding these positions, she worked as Deputy Information Commissioner from August 2019 until November 2020.

Prior to her work at the IMY, Talus served as Senior Adviser at the Ministry of Justice for over ten years. At the Ministry of Justice she led the implementation of the GDPR in Finland and acted as representative of the Finnish government in the EU GDPR negotiations. Talus has also worked at the European Commission, International Data Flows and Protection Unit (DG Justice and Consumers) as Seconded National Expert (SNE).

Talus holds a Doctor of Laws degree and a Master of Laws degree from the University of Helsinki and a Master of Arts degree from the University of Vaasa.

O PAPEL FUNDAMENTAL DO COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS (CEPD) NA DEFESA DO DIREITO À PROTEÇÃO DE DADOS NO CONTEXTO DOS DIREITOS DIGITAIS: CONVERGÊNCIAS E DISSONÂNCIAS

Senhora Presidente Meira Lourenço, Querida Paula, Querida Clara, Senhoras e Senhores, Ilustres convidados

É com enorme prazer que estou hoje aqui convosco para celebrar o 30.º aniversário da Comissão Nacional de Proteção de Dados, a CNPD.

Ao longo dos últimos 30 anos, a Autoridade Portuguesa de Proteção de Dados demonstrou o seu compromisso com a defesa do direito fundamental à privacidade e à proteção de dados, em Portugal e na Europa.

A nível nacional, a CNPD é um regulador muito respeitado, ativo e visível. Por exemplo, em 2023, a Autoridade Portuguesa iniciou 1.818 processos de investigação, realizou 45 ações de inspeção e aplicou nada menos do que 52 sanções.

A CNPD é também um membro valioso do Comité Europeu para a Proteção de Dados (CEPD) e, neste último ano desde que fui eleita Presidente do CEPD, tive a oportunidade de testemunhar em primeira mão o vosso trabalho árduo na proteção dos direitos dos cidadãos portugueses e europeus em matéria de proteção de dados.

Penso, por exemplo, no papel de destaque que assumiram no Comité de Supervisão Coordenada (CSC), cuja missão é garantir a supervisão coordenada de sistemas informáticos de grande escala e de organismos, gabinetes e agências da UE, tais como: IMI, Eurojust, EPPO, Europol, SIS e, a partir de outubro de 2024, o Sistema de Entradas e Saídas. Em nome do Secretariado do CEPD, gostaria de expressar a nossa gratidão pelo trabalho da Clara como coordenadora do CSC. O seu empenho e dedicação tiveram um impacto significativo na forma como o CSC foi estruturado e tem funcionado ao longo destes anos e todos beneficiámos da sua vasta experiência. Será difícil substituir a Clara quando elegermos um novo coordenador do CSC em julho.

De forma mais geral, no CEPD adotamos decisões vinculativas, emitimos orientações, promovemos a cooperação na aplicação da lei e garantimos que a proteção de dados continua a ser um foco central no novo quadro legislativo digital da UE. Permitam-me dar-vos uma breve atualização sobre o trabalho do CEPD, no qual a CNPD participa ativamente.

Ao longo dos anos, no CEPD investimos muitos recursos na construção de um compêndio abrangente com mais de 50 orientações e recomendações. As nossas orientações são cruciais para ajudar as organizações nos seus esforços de conformidade e para garantir a aplicação consistente do RGPD pelas autoridades de proteção de dados. Incluem muitos exemplos práticos e respostas a questões reais enfrentadas pelos profissionais da privacidade.

Em termos de aplicação transfronteiriça, o CEPD já tomou 1.200 decisões finais no mecanismo de balcão único, das quais menos de 1% passaram pelo mecanismo de resolução de litígios. Nos últimos seis meses, o EDPB emitiu decisões vinculativas históricas e forneceu pareceres jurídicos sem precedentes, incluindo a proibição do tratamento de dados pessoais pela *Meta Ireland Limited* para fins de publicidade comportamental e o subsequente parecer de consistência ao abrigo do artigo 64.º(2) sobre a validade do consentimento para o tratamento de dados pessoais para fins de publicidade comportamental no contexto dos modelos de "consentimento ou pagamento" utilizados por grandes plataformas online. Este trabalho está a ser acompanhado de perto por intervenientes em todo o mundo e espera-se que tenha impacto nos ecossistemas de tecnologia publicitária.

Embora as Autoridades de Proteção de Dados sejam responsáveis pela aplicação do RGPD, o CEPD desempenha um papel crucial na coordenação da cooperação na aplicação da lei. Nos últimos meses, continuámos a expandir os nossos métodos de

cooperação, garantindo sinergias e uma colaboração estreita entre as autoridades. Em fevereiro, o CEPD lançou a sua terceira ação conjunta, no âmbito da Ação de Supervisão Coordenada, sobre o direito de acesso, na qual participam 31 Autoridades. Através da iniciativa de apoio com peritos, desenvolvemos uma ferramenta de auditoria de websites que ajuda a analisar se os sites estão em conformidade com a legislação de proteção de dados e auxilia as autoridades na investigação e recolha de provas. Por fim, o grupo de trabalho sobre o ChatGPT adotou recentemente o seu relatório, analisando aspetos de interpretação comum das disposições relevantes do RGPD.

As funções e tarefas do CEPD crescem ano após ano. Um aspeto muito importante do nosso trabalho que veio à tona nos últimos meses é a interação com o novo quadro regulatório digital. As novas leis digitais da Europa — o DMA, o DSA, o Data Act e o AI Act — terão impacto na proteção de dados.

É importante que o futuro panorama regulatório se caracterize por uma colaboração inter-regulatória fluída entre Autoridades de diferentes áreas. O CEPD acredita que é benéfico quebrar barreiras e promover a cooperação com outros Reguladores.

No futuro, a mesma questão será abordada sob diferentes perspetivas, como a proteção de dados, preocupações com o mercado interno e a prevenção de atividades ilegais ou prejudiciais online. O trabalho realizado pelas diferentes autoridades será complementar e com o mesmo objetivo: moldar uma sociedade em que os serviços digitais estejam alinhados com os valores europeus comuns.

Em abril, adotámos a Estratégia do CEPD para os próximos quatro anos. Esta estratégia baseia-se no trabalho realizado pelo CEPD nos últimos seis anos. Continuaremos a promover a aplicação consistente das leis de proteção de dados, a desenvolver a cooperação na aplicação da lei e a garantir o alinhamento do RGPD com o novo quadro regulatório digital, para criar um espaço digital mais seguro onde os direitos fundamentais dos utilizadores sejam protegidos. Também contribuiremos para o diálogo global sobre proteção de dados. Queremos apoiar a convergência das leis de proteção de dados a nível mundial. É por isso que participamos em conferências internacionais — este ano, por exemplo, estive presente na Cimeira Global da IAPP e no Simpósio de Privacidade de Veneza, e no outono participarei na Mesa Redonda das Autoridades do G7 e na Assembleia Global da Privacidade.

O CEPD continuará a sensibilizar para o RGPD a nível europeu e internacional, para que os indivíduos conheçam os seus direitos e possam exercê-los, e para que as empresas, mesmo as mais pequenas, compreendam como cumprir os seus deveres legais. Para tal, queremos desenvolver mais ferramentas para públicos não especializados, como o nosso Guia para Pequenas e Médias Empresas e um website dedicado a crianças, professores e pais.

Todo este trabalho só poderá ser concretizado se tivermos pessoal e recursos suficientes. Este é um desafio para a CNPD, mas também para o CEPD. Embora a nossa colaboração estreita crie sinergias e apoio mútuo, no final é essencial que todas as Autoridades de proteção de dados tenham recursos suficientes para lidar com o número crescente de tarefas.

Para concluir, gostaria de expressar pessoalmente os meus sinceros parabéns à Paula e a toda a equipa da CNPD pelo vosso compromisso e dedicação contínuos para fazer funcionar o RGPD em Portugal e na Europa. Através do vosso trabalho, estão a fortalecer e a manter uma verdadeira cultura de proteção de dados em Portugal, na Europa e nos países vizinhos.

Também em nome do Secretariado do CEPD em Bruxelas, gostaria de sublinhar mais uma vez que valorizamos muito o vosso conhecimento especializado e dedicação, e é um enorme prazer trabalhar convosco quase diariamente.

Parabéns por alcançarem este marco notável de 30 anos na defesa do direito fundamental à proteção de dados! Espero muitos mais anos de cooperação frutífera!

Anu Talus
Chair of the European Data Protection Board

THE KEY ROLE OF THE EUROPEAN DATA PROTECTION BOARD (EDPB) IN UPHOLDING THE RIGHT TO DATA PROTECTION WITHIN THE CONTEXT OF DIGITAL RIGHTS: CONVERGENCES AND DISSONANCES

Dear President Meira Lourenço, dear Paula, dear Clara, ladies and gentlemen, esteemed guests

It is a great pleasure to be here today with you to celebrate the 30th anniversary of the Comissão Nacional de Proteção de Dados, the CNPD.

For the last 30 years, the Portuguese Data Protection Supervisory Authority has demonstrated its commitment to upholding the fundamental right of privacy and data protection, in Portugal and in Europe.

At national level, the CNDP is a much respected regulator, very active and visible. For instance, in 2023 the Portuguese DPA initiated 1,818 investigation procedures, performed 45 inspection actions and adopted no less than 52 sanctions.

The CNPD is also a valuable member of the European Data Protection Board (EDPB), and, in this last year since I was elected Chair of the EDPB, I had the chance to witness first-hand your hard work in protecting Portuguese and European citizens' data protection rights.

I think for example of the prominent role you have taken within the Coordinated Supervision Committee (CSC), whose mission is to ensure the coordinated supervision of large scale IT systems and of EU bodies, offices and agencies, such as: IMI, Eurojust,

EPPO, Europol, SIS and, as of October 2024, the Entry /Exit System. On behalf of the whole EDPB Secretariat, I would like to express our gratitude for Clara's work as CSC coordinator. Her hard work and dedication have made a significant impact on how CSC was set up and has functioned in these past years and we have all benefited from her extensive experience. It will be hard to fill Clara's shoes when we elect a new CSC coordinator in July.

More generally, at the EDPB we adopt binding decisions, issue guidance, promote enforcement cooperation and ensure that data protection remains a central focus in the new EU digital rulebook. Allow me to provide a brief update on the work of the EDPB, to which the CNPD actively participates.

Over the years, at the EDPB we have invested a great deal of resources to build a comprehensive compendium of over 50 guidelines and recommendations. Our guidance is crucial to help organisations in their compliance efforts and to ensure the consistent application of the GDPR by the DPAs. It provides many practical examples and answers real-life questions that privacy professionals are faced with.

In terms of cross-border enforcement, the EDPB has so far taken 1200 final one-stop-shop decisions, of which less than 1% has gone through the dispute resolution mechanism.

In the past six months, the EDPB has issued landmark binding decisions and provided unprecedented legal advice, including a ban on Meta Ireland Limited's processing of personal data for behavioural advertising purposes, and the subsequent Art. 64(2) consistency opinion on the validity of consent to process personal data for the purposes of behavioural advertising in the context of 'consent or pay' models deployed by large online platforms. This work is currently being closely followed by stakeholders worldwide and is expected to impact ad tech ecosystems.

While DPAs are in charge of enforcing GDPR, the EDPB has a crucial role in streamlining enforcement cooperation. In the past months, we continued to expand our enforcement cooperation methods, by ensuring synergies and close cooperation among DPAs. In February, the EDPB launched its third Coordinated Enforcement Framework action, on the right of access in which 31 DPAs are taking part. Through the support pool of experts initiative we have developed a website auditing tool that helps to analyse whether websites are compliant with data protection law and help DPAs to investigate and collect evidence. Finally, the taskforce on ChatGPT recently adopted its report, analysing aspects of common interpretation of relevant GDPR provisions.

The EDPB's roles and tasks are growing year by year. A very important aspect of our work that has come to the fore in the past months, is the interplay with the new regulatory digital framework. Europe's new digital laws, the DMA, DSA, Data Act & AI Act will have an impact on data protection.

It is important that the future regulatory landscape is characterized by seamless inter-regulatory collaboration between authorities from different fields. The EDPB believes that it is good to break down silos and promote cooperation with other regulators.

In the future, the same issue will be approached from different angles like data protection, internal market concerns and preventing illegal or harmful activities online. The work carried out by the different authorities in charge will be complementary and with the same objective: shaping a society in which digital services are aligned with common European values.

In April, we adopted the EDPB's Strategy for the four years to come. This strategy builds on the work that has been done by the EDPB in the past 6 years. We will continue to promote consistent application of data protection laws, to develop enforcement cooperation and to ensure the alignment of the GDPR with the new regulatory digital framework to create a safer digital space where the fundamental rights of users are protected. We will also contribute to the global dialogue on data protection. We want to support convergence of data protection laws worldwide. This is why we take part in international conferences, for instance this year I attended the IAPP Global Summit and the Venice Privacy Symposium, and in autumn I will take part in the G7 DPA Roundtable and the Global Privacy Assembly.

The EDPB will continue to raise awareness about the GDPR at the European and international level, so that individuals know their rights and can exercise them, and that companies, even small ones, can understand how to comply with their legal duties. To this end, we want to develop more tools for non-expert audiences, such as our Guide for Small Business and a website dedicated to children, teachers and parents.

All of this work can of course only be completed if we have enough staff and resources. This is a challenge for the CNPD, but also for the EDPB. While our close collaboration creates synergies and mutual support, in the end it is important that all DPAs have sufficient resources to be able to deal with their growing number of tasks.

To conclude, I personally would like to extend my heartfelt congratulations to Paula and the entire staff at CNPD for your continuous commitment and dedication to make GDPR work across Portugal and Europe. Through your work, you are strengthening and keeping a true data protection culture in Portugal, Europe and its neighbouring countries.

Also on behalf of the EDPB Secretariat in Brussels, I would like to stress again that we are highly appreciative of your expert knowledge and dedication, and it is a great pleasure to work with you on a nearly daily basis.

Congratulations on reaching this remarkable milestone of 30 years of upholding the fundamental right of data protection! I am looking forward to many more years of fruitful cooperation!

Mar España Martí
Diretora da Agência Espanhola de Proteção de Dados

Mar España Martí é licenciada em Direito pela ICADE (Universidade Pontifícia de Comillas), é perita universitária em gestão de entidades sem fins lucrativos (Fundação Luís Vives), possui um mestrado em Proteção Internacional dos Direitos Humanos (Universidade de Alcalá de Henares – Madrid) e um mestrado em Mindfulness e investigação em contextos de saúde (Universidade Complutense).

Foi Secretária-Geral do Instituto das Mulheres, Secretária-Geral do Provedor de Justiça espanhol e Vice-Ministra da Presidência e das Administrações Públicas do Governo Regional de Castela-Mancha. Foi nomeada Diretora da Agência Espanhola de Proteção de Dados em julho de 2015.

Desde 1989, é funcionária da Administração Geral Espanhola, como membro do Corpo Superior de Gestores Civis do Estado.

Participou também em atividades académicas, entre outras, como docente no Mestrado em Proteção Internacional dos Direitos Humanos da Universidade de Alcalá de Henares e no Mestrado em Ação Política da Universidade Rey Juan Carlos de Madrid.

Mar España Martí holds a University Degree in Law from the ICADE (Pontifical University of Comillas), is University Expert in management of not-for-profit entities (Luis Vives Foundation), holds a Masters on International Protection of Human Rights (University of Alcalá de Henares – Madrid), and Master in Mindfulness and research in health contexts (Complutense University).

She was General Secretary of the Institute of Women, General Secretary of the Spanish Ombudsman and Vice Minister of Presidency and Public Administrations in the Regional Government of Castilla La Mancha. She was appointed Director of the Spanish Data Protection Agency in July 2015.

Since 1989, she is a civil servant of the Spanish General Administration, as member of the Upper Corps of Civil State Managers.

She has also been involved in academic activities, participating as lecturer, among others, in the Master on International Protection of Human Rights at Alcalá de Henares University and in the Master on Political Action, at Madrid's Rey Juan Carlos University.

PROTEGER A LA INFANCIA Y ADOLESCENCIA EN EL ENTORNO DIGITAL EN EL SISTEMA ESPAÑOL

El derecho a la protección de datos garantiza los derechos y libertades fundamentales de las personas en cuanto al tratamiento de sus datos personales, especialmente de quienes, por diversas razones, se encuentran en una situación de vulnerabilidad, como es el caso de la infancia y adolescencia, que por encontrarse en pleno proceso de formación y desarrollo. Así lo recoge el Reglamento General de Protección de Datos (RGPD), que establece que "los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales, en particular entre otros cuando se utilicen para la elaboración de perfiles".

En el marco jurídico universal de protección de los niños hay que destacar la Convención de las NNUU de 1989 que, bajo la rúbrica del interés superior del menor, recoge los derechos de los niños, todos los menores de 18 años, y cuya observancia obliga a los 196 Estados firmantes, entre los que se encuentran Portugal y España.

La Observación General núm. 15, adoptada en 2013 por el Comité de los Derechos del Niño, que supervisa la aplicación de la Convención, en su apartado 38 expresa: "Preocupa al Comité el aumento de la mala salud mental en los adolescentes, en concreto trastornos en el desarrollo y la conducta, depresión, trastornos alimentarios, ansiedad, traumas psicológicos resultantes de (…) comportamientos obsesivos, como un uso excesivo de Internet y otras tecnologías hasta un punto adictivo y la autolesión y el suicidio".

Y en la Observación General núm. 25, de 2021, sobre los derechos de los niños en relación con el entorno digital señala, en su apartado 96, que "Los Estados parte deben establecer normas para evitar los daños conocidos y tener en cuenta de forma proactiva las nuevas investigaciones y pruebas en el sector de la salud pública a fin de evitar la difusión de información errónea y de materiales y servicios que puedan dañar la salud mental o física de los niños. También puede ser necesario adoptar medidas para prevenir cualquier participación perjudicial en juegos digitales o en las redes sociales, por ejemplo, reglamentaciones que prohíban los programas digitales que menoscaben el desarrollo y los derechos de los niños".

Estas referencias al entorno digital y uso de sus servicios y productos fue uno de los elementos tenidos en cuenta por el RGPD al recoger en sus considerandos que "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales".

En los últimos tiempos, el desarrollo vertiginoso de las tecnologías digitales ha impactado directamente en el derecho a la protección de datos. La magnitud de la recogida e intercambio de datos personales, propiciado por la conectividad, esencial para los servicios y productos digitales, ha desbordado todas las previsiones de hace apenas unos años, aumentando los riesgos para los derechos y libertades de la infancia y adolescencia como personas vulnerables.

La protección de los menores y el desarrollo tecnológico constante, que impacta en sus derechos y libertades, ha llevado a reconocer la necesidad de adoptar medidas y estrategias para su protección a través de las normas que componen el denominado "paquete digital", como el Reglamento de Servicios Digitales (DSA) o el Reglamento del Mercado Digital (DMA).

Si, a diferencia de innovaciones y avances de épocas anteriores, el desarrollo de las tecnologías de la información y comunicación ha supuesto una profunda y vertiginosa transformación en la vida de todas las personas permitiéndonos relacionarnos e

interactuar desde todas las partes del mundo, para los menores de edad ha supuesto un drástico cambio en su forma de vida, de informarse, comunicarse y de relacionarse en un momento clave para su desarrollo personal.

Esta es la realidad que vivimos hoy en un mundo altamente tecnologizado y globalizado que, junto con sus ventajas, supone enormes retos para los derechos y libertades de las personas en el tratamiento de sus datos personales.

Los principales perjudicados por un uso inadecuado de Internet son los colectivos vulnerables, en especial los niños y adolescentes que se han convertido, sin duda alguna, en los que más servicios y contenidos digitales consumen, en ocasiones dirigidos exclusivamente a los adultos.

Todos los estudios, encuestas y análisis los muestran como los mayores consumidores de sus contenidos, servicios y aplicaciones desde edades muy tempranas.

La encuesta del Instituto Nacional de Estadística sobre equipamiento y uso de tecnologías de información y comunicación en los hogares de 2023 recoge que el 91,7% de los menores de 10 años utilizaron Internet, porcentaje que sube al 97,1% con 15 años, mientras que disponen de móvil el 94,8%.

UNICEF en su estudio 'Impacto de la tecnología en la adolescencia' (2021) recoge que la edad media del primer móvil son los 10,96 años. El 98,5% de los adolescentes está registrado en más de una red social, y el 61,5% dispone de más de un perfil.

El 31,5% usa internet más de 5 horas a diario, porcentaje que asciende al 49,6 % los fines de semana. 6 de cada 10 adolescentes duermen con el móvil y 1 de cada 5 se conecta a partir de la medianoche.

Según un reciente informe de este año de la Federación de Ayuda a la Drogadicción, el 53,2% reconoce un uso excesivo del móvil y vive con cierto descontrol y dependencia de las redes sociales.

Otros datos preocupantes son los relativos al acceso de los menores de edad a contenidos online para adultos, en concreto a la pornografía, pero también a otros contenidos como violencia extrema, las apuestas o los juegos con recompensas.

Save the Children informa de que la mayor parte de los estudios y testimonios de familias alertan de que los primeros contactos con la pornografía comienzan en torno a los 8-9 años. El 58% lo ha tenido antes de los 13 años y el 8,7% antes de los 10. Algunos informes hablan de grandes consumidores de porno con 12 años, edad en la que su desarrollo cognitivo no les permite entender lo que están viendo. El 47,4% confiesa que alguna vez ha imitado lo que ha visto, pero no siempre de común acuerdo.

El acceso a esos contenidos a edades tan tempranas afecta a su desarrollo integral en un momento en el que la personalidad no está formada, generando importantes desórdenes en la concepción de las relaciones sexuales y del rol de la mujer.

La Fiscalía General del Estado en su Memoria de 2023, alerta del alarmante incremento en los últimos cinco años en España de las agresiones sexuales perpetradas por menores, un 116%. La Fiscalía señala que, si bien, este incremento obedece a causas complejas y que confluyen diversos factores, apunta a la carencia de una adecuada formación ético-sexual y al visionado inapropiado y precoz de material pornográfico violento.

Otro efecto importante derivado del uso de la tecnología digital es el de la violencia digital de género.

En este sentido, el informe de UNICEF refleja que:

- El 42% ha recibido mensajes sexuales y un 13,8% los ha enviado.
- Un 8% ha enviado fotos /vídeos suyos con contenido sexual.

- El 3,7% ha sido objeto de chantaje con material digital sexual.
- 1 de cada 10 ha recibido una proposición sexual de un adulto.

Un reciente estudio de la Fundación ANAR refleja que las TIC tienen una implicación relevante en los casos de violencia de género entre adolescentes, un 79,9%, que, según ANAR, ha aumentado en 11,9 puntos en la postpandemia, favorecida por el temprano acceso a los dispositivos electrónicos.

La implicación de las TIC se encuentra asociada significativamente con casos de violencia sexual contra niños, niñas y adolescentes como el ciberbullying, el grooming, la ciberviolencia de género o el sexting, así como el acceso y consumo de pornografía entre población menor de edad.

El estudio de la Fundación ANAR refleja un crecimiento preocupante de los comportamientos machistas entre los más jóvenes, con unos datos de lo más inquietantes: el 70,3% de los adolescentes no denuncian la violencia que sufren ni tienen intención de hacerlo; pero es que el 47,1% no es consciente del problema; observándose una evolución negativa en cuanto a la conciencia del problema, pues el 63,7% de las adolescentes que solicitaron ayuda "No eran conscientes de conductas violentas que sus parejas o exparejas estaban teniendo con ellas".

Los casos de violencia de género en adolescentes generan problemas de salud mental a un 48,8%, de los que 7 de cada 10 víctimas no reciben tratamiento psicológico.

Otro aspecto derivado del uso de los servicios y productos digitales va ligado a las compras que los menores realizan a través de Internet. Según el último informe de IAB Spain, uno de cada dos menores ha comprado por influencia de las redes sociales, que actúan como buscadores digitales y promueven las compras de los más pequeños.

El uso problemático y adictivo de Internet por los menores tiene unos efectos nocivos que afectan gravemente a su desarrollo personal en diferentes ámbitos y materias:

- La salud
- El neurodesarrollo
- El aprendizaje
- Las relaciones familiares y sociales
- La privacidad
- Los hábitos de consumo
- La monetización de sus datos

Además, la sobreexposición de información personal los hace más proclives a las situaciones de riesgo que el consumo intensivo de tecnología puede causar, como el ciberacoso, sexting, o el grooming, con consecuencias en algunos casos lamentablemente irreparables.

El uso inadecuado de la tecnología impacta en la salud a todos los niveles (física, mental, psicosocial y sexual) y a cualquier edad. Los adolescentes y niños, por encontrase en formación tanto física como de su personalidad, constituyen un grupo especialmente vulnerable, según se pone de manifiesto por los pediatras.

Un mayor tiempo de pantallas se asocia con un mayor riesgo de insomnio, de padecer síntomas depresivos, además de otros riesgos como impulsividad, obesidad, fatiga visual, conductas de riesgo…; y de afectar a la interacción social cara a cara.

La adolescencia es un período crítico para el desarrollo del córtex prefrontal y un período de máxima vulnerabilidad para la adquisición y el desarrollo de trastornos adictivos, psiquiátricos y comportamentales.

Estamos, sin duda, ante un problema de salud pública de primera magnitud al que se está llegando tarde, aunque todavía se está a tiempo para garantizar la salud y el bienestar digital de nuestros menores mediante la adopción de medidas y políticas, fundamentalmente preventivas, que inculquen el uso saludable, razonable, responsable y seguro de las tecnologías.

Pero no sólo en la salud se producen efectos negativos, también en el ámbito educativo. Afecta igualmente al neurodesarrollo, aprendizaje y a la adquisición de capacidades, así como al rendimiento educativo de los menores y a las relaciones familiares y escolares.

Según un estudio del Centro de Investigación Económica Ragnar Frisch, publicado en la Revista de Ciencias de los Estados Unidos, el coeficiente intelectual de las nuevas generaciones está disminuyendo desde el cambio de milenio una media entre 2'5 y 4'3 puntos cada diez años.

El nivel de lecto escritura de los menores se ha visto afectado por el uso intensivo que realizan de los dispositivos electrónicos, que ha caído a plomo desde el año 2016. En España ha supuesto una bajada de 7 puntos, los mismos que estamos por debajo de la media de la UE.

La UNESCO, en su Informe GEM (Global Education Monitoring) 2023 sobre tecnología en la educación, recoge que el tiempo que los niños pasan frente a la pantalla ha aumentado, tanto con fines educativos como por ocio. Este incremento de tiempo frente a la pantalla puede afectar negativamente al autocontrol y a la estabilidad emocional, y aumentar la ansiedad y la depresión.

El último informe PISA incide en el descenso de la comprensión lectora de los alumnos, 3 puntos en España y 11 puntos en el ámbito de la OCDE, respecto a la anterior edición de 2018, y de 8 puntos en matemáticas. Distraerse con los móviles supone perder la mitad de los conocimientos de un curso de matemáticas.

Pocos países cuentan con una reglamentación estricta en este sentido. Suecia se ha replanteado la digitalización en las aulas y Noruega parece que la sigue. En China, el Ministerio de Educación limitó el uso de dispositivos digitales como herramientas educativas a un 30% del tiempo de enseñanza global.

En Estados Unidos, las plataformas educativas han demandado a las principales empresas de internet por los daños en la salud mental a la juventud.

Estas consecuencias llevaron el año pasado a la Agencia Española de Protección de Datos a proponer a las Autoridades educativas que valorasen la adopción de medidas de restricción o limitación del uso de dispositivos electrónicos en los centros escolares por los graves perjuicios que causan a la salud y a los resultados académicos de los menores, además de a la convivencia escolar, pues los estudios realizados en aquellas regiones en las que se había restringido el uso de los dispositivos electrónicos en los centros escolares demostraron que había disminuido significativamente el riesgo de ciberacoso y aumentado el rendimiento escolar.

La propuesta ha sido y está siendo seguida por las autoridades educativas del resto de regiones (Comunidades Autónomas) de España.

MEDIDAS E INICIATIVAS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

En la Agencia estamos profundamente comprometidos con el bienestar y la protección de los derechos y libertades de la infancia y adolescencia en el ámbito digital, con actuaciones y medidas de sensibilización, concienciación y formación sobre el uso responsable y saludable de las pantallas. El objetivo es que puedan aprovechar y sacar el mayor partido de las ventajas y oportunidades que ofrece la tecnología y, al mismo tiempo, evitar los riesgos de un uso inadecuado.

El compromiso de la Agencia con la protección de los menores tiene un largo recorrido. Ha formado siempre parte de sus objetivos estratégicos, como se recoge en su primer Plan Estratégico (2015 – 2019). Uno de cuyos ejes de actuación prioritaria tiene el marco y la rúbrica de la prevención para la protección más eficaz de los derechos en Internet, en particular la de los menores.

Ese compromiso se ha mantenido a través del Marco de Responsabilidad Social de la Agencia 2019 – 2024, y al que responde también la Estrategia reforzada de la Agencia para la protección de los menores online.

Entre las distintas acciones de la Agencia dirigidas a la protección de los menores en el entorno digital desde un enfoque fundamentalmente preventivo se encuentran las siguientes iniciativas:

- La creación de un Área temática en la web de la Agencia dedicada exclusivamente a la "Educación y menores", que comprende un variado material audiovisual, guías, fichas, recursos, informes, enlaces de interés y para la seguridad de los menores.
- El establecimiento de un Canal específico para consultas sobre el tratamiento de datos de menores y por menores, que comprende varias vías: WhatsApp, línea telefónica y dirección electrónica. En 2023 recibió más de 4.000 consultas.
- La elaboración de materiales, contenidos y recursos dirigidos tanto a los propios menores como a las familias y docentes, disponibles en el área de "Educación y menores".
- La concienciación y formación de menores, familias, profesores, equipos directivos de los centros educativos, en colaboración con el Ministerio de Educación y el Instituto Nacional de Ciberseguridad, mediante la celebración periódica y sistemática de cursos formativos dirigidos a la comunidad educativa (MOOC, NOOC y cursos en línea).
- La creación del Canal Prioritario, en 2019, que permite solicitar la retirada urgente de contenidos sexuales o violentos publicados en internet sin el consentimiento de las personas que aparecen en ellos. Dispone de una línea específica para las denuncias de los menores de edad, mayores de 14 años, que no necesitan la certificación electrónica.

  En la Agencia hemos observado cómo la tecnología digital es empleada con frecuencia para controlar, acosar, humillar, extorsionar o atemorizar y, aunque todo ciudadano puede ser una víctima, los menores de edad y las mujeres son el principal blanco de estas conductas. La violencia digital contra mujeres y niñas aglutina un porcentaje muy importante de los casos que se denuncian en el Canal prioritario.
- La constitución e impulso, desde 2019, del grupo de trabajo "Menores, salud digital y privacidad", dedicado a analizar las situaciones que afectan a los derechos de los menores en la Red. Aglutina a los diferentes actores implicados en la defensa y bienestar de los menores, que se viene reuniendo con regularidad para dar respuesta a los problemas y situaciones que se plantean en este ámbito.
- Desde el grupo de trabajo se han impulsado iniciativas que se han plasmado en acciones como la creación de la web ASEGURATIC en el Ministerio de Educación, con el mayor repositorio de materiales, recursos y contenidos de apoyo para la educación digital a disposición de docentes, familias y demás actores implicados en la educación y formación de los niños, niñas y adolescentes.
- Promoción de buenas prácticas educativas y su intercambio en el uso saludable, responsable y seguro de internet por los menores con los premios anuales a los centros educativos que se distinguen por su labor y proactividad, así como a las personas y entidades que se distingan por su labor en pro del uso saludable, responsable y seguro de Internet.

- Realización de campañas de sensibilización y concienciación sobre el uso saludable y responsable de Internet. Sirva de ejemplo la campaña conjunta con UNICEF dirigida a las familias (finales de 2022) "Más que un móvil" que incluye "La guía que no viene con el móvil", con el decálogo de claves que deben tener en cuenta las familias antes de entregar a sus hijos e hijas el primer móvil.
- Concienciación y exigencia de responsabilidad a menores y progenitores por la difusión online ilícita de imágenes, audios o información sensible, con responsabilidad administrativa, civil, penal y disciplinaria educativa. La Ley de protección integral a la infancia y adolescencia frente a la violencia ya prevé que los mayores de 14 años podrán ser sancionados por hechos constitutivos de infracción administrativa de acuerdo con la normativa sobre protección de datos personales.
- Actuaciones frente a páginas de contenidos online para adultos (pornografía) que carecen de sistemas de verificación de la edad o bien estos son inconsistentes, como la mera declaración de mayoría de edad.

Dentro de este abanico de acciones y medidas, durante el último año, el Grupo de Trabajo "Menores, salud digital y privacidad" y la Agencia han dedicado su trabajo:

a. Por una parte, a concienciar sobre el uso intensivo, problemático o adictivo de Internet, a la vista de los datos expuestos anteriormente.

   Las pantallas han causado una profunda trasformación del funcionamiento intelectual y comportamental de los jóvenes, donde la inmediatez, el paso frenético de una actividad a otra y su validación en las redes sociales forman parte esencial de su día a día.

   La Federación de Ayuda a la Drogadicción, en el informe antes citado, recoge que el 70,8% no es consciente del tiempo que pasa en las redes sociales y el 64,3% quiere verlas en todo momento.

   Los efectos o síntomas de estas conductas guardan similitud con las adicciones a sustancias y han de ser conocidos para poder enfrentarse a ellas, la tolerancia, los síndromes de abstinencia, las dificultades en control conductual, las interferencias con actividades cotidianas o perturbaciones en las relaciones interpersonales, y que en los menores afecta gravemente a su desarrollo como personas, son muestra de que algo no marcha bien y es necesario identificarlos precozmente y adoptar medidas para evitar daños.

   Al igual que ocurre con las adicciones a las drogas, es difícil que un adicto a internet o a las redes sociales se considere como tal, sino que normaliza, minimiza, justifica o niega el problema. Por lo general, es un suceso muy negativo (un fracaso escolar, trastornos de conducta, mentiras reiteradas, aislamiento social, problemas económicos, presión familiar) lo que hace tomar conciencia del problema, fundamentalmente por los progenitores cuando se trata de menores de edad.

   En relación con el uso adictivo, la Agencia apoya todas aquellas iniciativas científicas destinadas proporcionar pautas y orientaciones que contribuyan a la salud digital de los menores, tanto física como mental. Las acciones para hacer frente al uso problemático o adictivo de las TIC por los menores.

   Fruto de la labor del Grupo de Trabajo, además de determinar qué es una conducta problemática y adictiva, han sido:

- La suscripción de Protocolos de Actuación con los Consejos de Colegios de Psicólogos y de Médicos para la colaboración en medidas y acciones con esta finalidad.
- Colaboración con la Asociación Española de Pediatría, y apoyo a su Plan Familiar Digital mediante campañas de difusión.

   Plan Familiar Digital incide, desde la evidencia científica, en cómo afecta a los menores el uso de pantallas y el número de horas que pasan frente a ellas, ofreciendo recomendaciones, adaptadas a las necesidades de cada familia y a la edad de

los menores que la componen, para que hagan un buen uso de los medios digitales con el fin de obtener las ventajas que aportan y reduciendo los riesgos para su salud y bienestar.

Establece pautas sobre el máximo de horas de uso de pantallas por edades que incluye los tiempos de ocio y de aula. El Plan Digital Familiar recoge que el uso rutinario de dispositivos para distraer o calmar genera dificultad para el desarrollo de estrategias de autogestión; ocasiona dependencia de las pantallas y determinará dificultades de autorregulación en etapas posteriores. Por ese motivo, desaconseja el uso de pantallas antes de los seis años, considerándose que no existe un tiempo seguro, estableciendo como excepción usar las pantallas para el contacto social en tiempos cortos y con un objetivo concreto bajo supervisión de un adulto.

b. El otro ámbito de actuación es el del acceso de los menores de edad a contenidos online para adultos, en particular a la pornografía, así como a otros contenidos también inapropiados como la violencia extrema, las apuestas o los juegos con recompensas.

El Grupo de Trabajo ha celebrado reuniones plenarias y delegadas conformado una línea de trabajo encaminada a poder disponer de una herramienta que verifique la edad para acceder a los contenidos online para adultos de conformidad con el marco del derecho a la protección de datos personales.

La verificación de la edad para el acceso a contenidos online para adultos es una necesidad puesta de manifiesto desde diferentes regulaciones, como la DSA, para proteger a los menores de contenidos o contactos que los puedan molestar, asustar, entristecer, preocupar, enfadar o acosar; o la Directiva 2018/1808, de modificación de la Directiva 2010/13 de servicios de comunicación audiovisual.

El resultado de los trabajos llevados a cabo por la Agencia ha sido la presentación en diciembre de 2023, del Decálogo con los principios y criterios que debe cumplir un sistema para verificar la edad en el acceso a contenidos online respetuoso con la regulación de protección de datos y la privacidad, cuya aplicación se ha probado con éxito, a través de pruebas de concepto, en los 3 navegadores de mayor uso (Windows, IOS y Android).

En enero de 2024 la Agencia presentó su Estrategia reforzada para la protección de los menores.

La estrategia se proyecta sobre 3 líneas fundamentales de actuación de la Agencia que se refuerzan con 10 intervenciones de base.

LA PRIMERA DE LAS LÍNEAS ESTÁ DIRIGIDA A LOGRAR UNA PROTECCIÓN INTEGRAL A LOS MENORES EN L ENTORNO DIGITAL Y PROTEGER SUS DERECHOS Y LIBERTADES EN EL TRATAMIENTO DE SUS DATOS PERSONALES MEDIANTE:

1. El apoyo para alcanzar un Pacto de Estado.
2. La total puesta a disposición para colaborar, a través de la coordinación del Grupo de Trabajo, en el análisis y los estudios jurídicos y tecnológicos para la elaboración de un proyecto de Ley de protección integral a los menores en internet, que incluya los neurodatos, como categoría especial de datos de carácter personal, y sus correlativos neuroderechos, en especial de los menores de edad.

EL SEGUNDO EJE DE ESTA ESTRATEGIA ES EL REFUERZO DE LAS GARANTÍAS DE LOS DERECHOS DE LOS MENORES EN INTERNET, MEDIANTE:

3. El impulso y colaboración con los organismos competentes para el desarrollo de apps de verificación de la edad en el acceso a contenidos digitales para adultos conforme a los principios y requisitos adoptados por la Agencia, probados con éxito en las pruebas de concepto realizadas, y su presentación en el marco europeo y transatlántico para que sirvan de modelo a seguir.

4. Herramientas de control parental y recursos para la configuración de la privacidad en redes sociales, navegadores y sistemas operativos, en colaboración con el Instituto Nacional de Ciberseguridad.
5. Educación digital sobre privacidad a las familias y al resto de la comunidad educativa en colaboración con el Ministerio de Educación y el Instituto Nacional de Ciberseguridad.
6. El apoyo a las autoridades educativas en la utilización de las plataformas y herramientas digitales adecuadas a la normativa de protección de datos.
7. Actuaciones de investigación sobre dichas herramientas y plataformas para garantizar la protección de los datos personales.
8. El fomento de evaluaciones de impacto en privacidad y salud digital en función de la edad y los riesgos de las tecnologías digitales, en colaboración con las autoridades educativas, sanitarias y los Consejos de Colegios de Médicos, Psicólogos y Pedagogos.

LA TERCERA LÍNEA DE ACTUACIÓN ESTRATÉGICA ES LA LUCHA CONTRA LAS PRÁCTICAS ILÍCITAS EN MATERIA DE PROTECCIÓN DE DATOS DE LOS MENORES, MEDIANTE:

9. La priorización de las investigaciones a las webs de contenidos pornográficos, en especial de la verificación de la edad de los usuarios, y la coordinación con las autoridades de la UE para las webs que no tengan el establecimiento en España.
10. El análisis de los algoritmos y patrones adictivos que creen dependencia a Internet y que tienen como objetivo influir en los comportamientos y decisiones de usuarios, y la coordinación con el Comité Europeo de Protección de Datos.

Las intervenciones que refuerzan estas líneas estratégicas se complementan y desarrollan con otras 35 medidas en distintos marcos de actuación, entre ellas por destacar algunas:

- El impulso a la regulación de desarrollo y complementaria que requiere la protección integral de los menores.
- Medidas, en el marco del ejercicio de las potestades de la Agencia, focalizadas en las potestades de investigación y sancionadoras, y de comprensión de los riesgos, normas, garantías y derechos que afectan a los menores en el tratamiento de sus datos.
- Del mismo modo, en los marcos de la educación, la salud y bienestar digital se han identificado aquellas medidas que, en colaboración con autoridades educativas y miembros de la comunidad educativa, las autoridades sanitarias y las organizaciones y sociedades científicas, contribuyan a garantizar en el marco de la privacidad y la protección de datos un espacio digital seguro para los derechos de la infancia y la adolescencia.

Una parte significativa de estas medidas encuentran en el Grupo de Trabajo impulsado por la Agencia el marco idóneo para su desarrollo y ejecución; y con las que esperamos contribuir al objetivo de la sociedad: conseguir que los menores puedan navegar seguros por Internet.

La totalidad de las medidas están publicadas y disponibles en la web de la Agencia.

Además de las acciones acometidas por la Agencia, la situación del acceso y utilización de los servicios y productos digitales por los menores, y las nocivas consecuencias que se pueden producir por su uso inadecuado y problemático, ha dado lugar a un intenso debate que ha situado como prioridad la protección de los menores en el mundo digital, y se han puesto en marcha diversas iniciativas de ámbito nacional.

En enero de 2024 se creó un Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia, en el seno del Ministerio de Juventud e Infancia, y del que forma parte activa la Agencia, con la finalidad de realizar un informe con el diagnóstico sobre la situación de los menores en el entorno online, analizando buenas prácticas y elaborando recomendaciones, medidas y actuaciones para contribuir a su protección.

El informe analiza la situación desde diferentes ámbitos, entre otros, los de salud, educativo, o privacidad.

Algo más de un mes después, se constituyó, en el seno del Ministerio para la Transformación Digital, un Grupo de Trabajo específico para el desarrollo de una solución tecnológica que evite el acceso de menores al contenido inapropiado respetando la privacidad de los usuarios y asegurando la autenticidad de la fuente, en el que la Agencia aporta su catálogo de principios y su experiencia en el desarrollo de estos sistemas.

Igualmente, el Gobierno de España ha presentado un Anteproyecto de Ley para la protección de los menores en los entornos digitales que incluye una serie de medidas para hacer frente a los daños potenciales que el uso de Internet puede llegar a producir, atendiendo a aquellas situaciones que se han ido generando y de las que no protege la Ley de Protección de Datos y garantía de los derechos digitales de 2018, que contiene varios preceptos en su Título X dedicados a la protección de los menores en Internet.

Las medidas afectan a los siguientes ámbitos:

- Educativo, para que los centros educativos, de acuerdo con las disposiciones de las autoridades, regulen el uso de los dispositivos móviles y digitales en las aulas.
- Sanitario, para detectar usos problemáticos y promover la atención sanitaria especializada para los menores con conductas adictivas sin sustancia.
- Consumo, con prohibición de acceso a servicios digitales con mecanismos aleatorios de recompensa y la obligación de incluir herramientas de control parental por defecto en los dispositivos digitales.
- Protección de datos, elevando de 14 a 16 la edad de prestación del consentimiento para el tratamiento de datos personales, en el arco establecido por el RGPD.
- Penal, adecuando y estableciendo las disposiciones del código penal para la protección de los menores, como el uso de identidades falsas o las deepfakes.

Esta es la situación en la que se encuentra actualmente el sistema de protección de los menores en Internet y de las medidas en marcha para generar un entorno digital saludable y seguro que garantice sus derechos y el pleno desarrollo de su personalidad.

Estamos ante un verdadero problema de salud pública para el que ya llegamos tarde, pero aún a tiempo, y que requiere el compromiso de todos los sectores y agentes implicados: poderes públicos, sanidad, educación, seguridad digital, familias, industria, etc.

Finalizo en la confianza de que aunando esfuerzos podemos conseguir la protección de nuestra infancia y adolescencia en el entorno digital, pues está en juego su futuro, que también es el nuestro.

Muito obrigado.

Mar España Martí
Director of the Spanish Data Protection Supervisory Authority

THE PERSONAL DATA PROTECTION OF CHILDREN AND YOUNG PEOPLE IN THE DIGITAL ENVIRONMENT IN THE SPANISH SYSTEM

The right to data protection guarantees the fundamental rights and freedoms of individuals with regard to the processing of their personal data, especially those who, for various reasons, are in a vulnerable situation, such as children and adolescents, who are in the process of being fully trained and developed. This is provided for in the General Data Protection Regulation (GDPR), which states that 'children deserve specific protection of their personal data, as they may be less aware of the risks, consequences, safeguards and rights related to the processing of personal data, in particular when used for profiling'.

In the universal legal framework for the protection of children, attention should be drawn to the 1989 UN Convention, which, under the heading of the best interests of the child, covers the rights of children, all children under the age of 18, and the observance of which is binding for the 196 signatory States, including Portugal and Spain.

General Comment N. 15, adopted in 2013 by the Committee on the Rights of the Child, which oversees the implementation of the Convention, paragraph 38 states: "The Committee is concerned by the increase in mental ill-health among adolescents, including developmental and behavioural disorders, depression, eating disorders, anxiety, psychological trauma resulting from (...) obsessive behaviour, such as excessive use of and addiction to the Internet and other technologies; and self-harm and suicide".

And in General Comment N. 25 of 2021 on children's rights in relation to the digital environment states, in paragraph 96, that 'States parties should regulate against known harms and proactively consider emerging research and evidence in the

public health sector, to prevent the spread of misinformation and materials and services that may damage children's mental or physical health. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children's development and rights".

These references to the digital environment and the use of its services and products were one of the elements taken into account by the GDPR by stating in its recitals that "Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data."

In recent times, the dramatic development of digital technologies has had a direct impact on the right to data protection. The scale of the collection and sharing of personal data, enabled by connectivity, essential for digital services and products, has overwhelmed all the predictions just a few years ago, increasing the risks to the rights and freedoms of children and adolescents as vulnerable persons.

Protection of minors and constant technological development, which has an impact on their rights and freedoms, has led to the recognition of the need to adopt measures and strategies for their protection through the rules that make up the so-called 'digital package', such as the Digital Services Act (DSA) or the Digital Market Act (DMA).

While, unlike innovations and advances in previous times, the development of information and communication technologies has brought about a profound and dramatic transformation in the lives of all people by enabling us to connect and interact from all parts of the world, for minors it has brought about a dramatic change in their way of life, to inform each other, to communicate and to connect at a time that is key to their personal development.

This is the reality we live today in a highly technologised and globalised world that, together with its benefits, poses enormous challenges to the rights and freedoms of individuals in the processing of their personal data.

The main victims of inappropriate use of the Internet are vulnerable groups, especially children and adolescents who have undoubtedly become the most popular digital content and services consumers, sometimes exclusively aimed at adults.

All studies, surveys and analyses show them as the largest consumers of their content, services and applications from a very early age.

The National Statistics Institute's survey on equipment and use of information and communication technologies in households in 2023 shows that 91.7 % of children under the age of 10 used the Internet, up to 97.1 % with 15 years old, while they have a mobile phone rate of 94.8 %.

UNICEF, in its study 'Impact of technology on adolescence' (2021), states that the average age of the first mobile phone is 10,96. 98.5 % of adolescents are registered on more than one social network and 61.5 % have more than one profile.

31.5 % use the Internet over 5 hours a day, up to 49.6 % at weekends. 6 out of 10 teenagers sleep with the mobile and 1 out of 5 are connected from midnight.

According to a recent report of this year by the Federation of Aid to Drug Addiction, 53.2 % recognise excessive use of mobile phones and live with some lack of control and dependence on social media.

Other worrying data relate children's access to online content for adults, in particular pornography, but also to other content such as extreme violence, betting or reward games.

Save the Children reports that most studies and testimonies from families warn that first contacts with pornography start around the age of 8-9. 58 % were before the age of 13 and 8.7 % before the age of 10. Some reports refer to large porn consumers aged 12, an age at which their cognitive development does not allow them to understand what they are seeing. 47.4 % confesses that they have sometimes mirrored what they have seen, but not always by mutual consent.

Access to such content at such an early age affects their integral development at a time when personality is not formed, generating significant disorder in the conception of sexual relations and the role of women.

In its 2023 report, the State Prosecutor's Office warned of the alarming increase in sexual assaults committed by minors in the last five years in Spain, by 116 %. The Public Prosecutor's Office points out that, while this increase is due to complex causes and combines various factors, it points to the lack of adequate ethical and sexual training and the inappropriate and early viewing of violent pornographic material.

Another important effect stemming from the use of digital technology is digital gender-based violence.

In this regard, UNICEF report reflects that:

- 42 % received sexual messages and 13.8 % sent them.
- 8 % have sent photos /videos with sexual content.
- 3.7 % have been blackmailed with digital sexual material.
- 1 out of 10 have received a sexual offer from an adult.

A recent study by the ANAR Foundation shows that ICTs have a significant involvement in cases of gender-based violence among adolescents, 79.9 % of which, according to ANAR, has increased by 11,9 points in the post-pandemic, facilitated by early access to electronic devices.

The involvement of ICT is significantly associated with cases of sexual violence against children and adolescents such as cyberbullying, grooming, gender-based cyberviolence or sexting, as well as access to and consumption of pornography among the younger population.

The ANAR Foundation study reflects a worrying increase in machist behaviour among the youngest, with data of the most worrying: 70.3 % of adolescents do not report and do not intend to report violence; however, 47.1 % are not aware of the problem; there was a negative trend in awareness of the problem, as 63.7 % of adolescents who applied for help "were not aware of violent behaviour that their partners or ex-partners were having with them".

Cases of gender-based violence in adolescents cause mental health problems at 48.8 %, of which 7 out of 10 victims do not receive psychological treatment.

Another aspect arising from the use of digital services and products is linked to purchases made by minors over the Internet. According to IAB Spain's latest report, one in two children has bought under the influence of social media, which act as digital search engines and promote purchases by the smallest.

The problematic and addictive use of the Internet by minors has harmful effects that severely affect their personal development in different areas and subjects:

- Health
- Neurodevelopment

- Learning
- Family and social relations
- Privacy
- Consumption habits
- Monetisation of their data

Furthermore, overexposure of personal information makes them more prone to risk situations that technology-intensive consumption can cause, such as cyberbullying, sexting, or grooming, with regrettably irreparable consequences in some cases.

Inappropriate use of technology has an impact on health at all levels (physical, mental, psychosocial and sexual) and at any age. Teenagers and children, being in both physical and personality training, are a particularly vulnerable group, as evidenced by paediatricians.

Longer screen time is associated with an increased risk of insomnia, of suffering from depressive symptoms, as well as other risks such as impulsivity, obesity, visual fatigue, risky behaviour, etc.; and to affect face-to-face social interaction.

Adolescence is a critical period for the development of the pre-frontal cortex and a period of maximum vulnerability for the acquisition and development of addictive, psychiatric and behavioural disorders.

We are undoubtedly faced with a major public health problem that is coming late, although it is still on time to ensure the digital health and well-being of our children by adopting primarily preventive measures and policies that instil the healthy, reasonable, responsible and safe use of technologies.

But not only on health, there are negative effects, they are also in education. It also affects neurodevelopment, learning and skills acquisition, as well as children's educational performance and family and school relationships.

According to a study by the Centre for Economic Research Ragnar Frisch published in the US Science Review, the intellectual coefficient of new generations is decreasing by an average of between 2' 5 and 4' 3 points every ten years since the millennium change.

The level of literacy of minors has been affected by their intensive use of electronic devices, which has plummeted since 2016. In Spain, this has resulted in a decrease of 7 points, which are below the EU average.

UNESCO, in its GEM (Global Education Monitoring) Report 2023 on technology in education, states that the time children spend in front of the screen has increased, both for educational and leisure purposes. This increase in time vis-à-vis the screen can negatively affect self-control and emotional stability, and increase anxiety and depression.

The latest PISA report highlights the decline in pupils' reading comprehension, 3 points in Spain and 11 points at OECD level, compared to the previous 2018 edition, and by 8 points in mathematics. Distracting with mobile phones means losing half of the knowledge of a mathematics course.

Few countries have strict regulation in this regard. Sweden has rethought digitalisation in the classrooms and Norway seems to follow it. In China, the Ministry of Education limited the use of digital devices as educational tools to 30 % of the overall teaching time.

In the United States, educational platforms have sued major Internet companies for harm to mental health in young people.

These consequences led last year to the Spanish Data Protection Agency to propose to the educational authorities to assess the adoption of measures restricting or limiting the use of electronic devices in schools on the grounds of the serious harm they cause to the health and academic results of minors, as well as to school coexistence, as studies carried out in those regions where the use of electronic devices in schools had been restricted showed that the risk of cyberbullying had significantly decreased and increased school performance.

The proposal has been and is being followed by the educational authorities of the regions (Autonomous Communities) in Spain.

MEASURES AND INITIATIVES OF THE SPANISH DATA PROTECTION AGENCY

In the Agency we are deeply committed to the well-being and protection of the rights and freedoms of children and adolescents in the digital sphere, with awareness-raising and training actions and measures on the responsible and healthy use of screens. The aim is to enable them to take full advantage of the benefits and opportunities offered by technology and at the same time avoid the risks of misuse.

The Agency's commitment to the protection of minors has a long journey. It has always been part of its strategic objectives, as set out in its first Strategic Plan (2015-2019). One of the priority areas for action is the prevention framework and heading for the most effective protection of rights on the Internet, in particular children's rights.

This commitment has been maintained through the Agency's Social Responsibility Framework 2019-2024, which is also addressed by the Agency's reinforced strategy for the protection of minors online.

Among the Agency's various actions aimed at protecting children in the digital environment from a primarily preventive approach are the following initiatives:

- The creation of a thematic area on the Agency's website dedicated exclusively to 'Education and minors', comprising a variety of audiovisual material, guides, factsheets, resources, reports, links relevant to and for the safety of minors.
- The establishment of a dedicated channel for queries on the processing of data relating to minors and by minors, comprising several channels: WhatsApp, telephone line and e-mail address. In 2023, it received more than 4.000 consultations.
- The production of materials, content and resources aimed at both minors themselves and families and teachers, available in the area of 'Education and minors'.
- Awareness raising and training of minors, families, teachers, school management teams, in cooperation with the Ministry of Education and the National Cybersecurity Institute, through regular and systematic training courses for the educational community (MOOC, NOOC and online courses).
- The creation of the Priority Channel in 2019, which makes it possible to request the urgent removal of sexual or violent content posted on the Internet without the consent of those appearing. It has a specific line for reporting of minors over the age of 14 who do not need electronic certification.

In the Agency, we have seen how digital technology is often used to control, harass, humiliate, extort or frighten, and although every citizen can be a victim, minors and women are the main targets of this behaviour. Digital violence against women and girls accounts for a very large percentage of cases reported in the Priority Channel.

- The establishment and promotion since 2019 of the working group, 'Children, Digital Health and Privacy', dedicated to analysing situations affecting children's rights in the Internet. It brings together the various actors involved in the defence and well-being of children, who have met regularly to respond to the problems and situations in this area.

- The working group has promoted initiatives that have resulted in actions such as the creation of the ASEGURATIC website in the Ministry of Education, with the largest repository of materials, resources and support content for digital education available to family teachers and other actors involved in the education and training of children and adolescents.
- Promotion of good educational practices and their exchange on the healthy, responsible and safe use of the Internet by minors through the annual awards to schools that are distinguished by their work and proactivity, as well as to individuals and entities who are distinguished by their work for the healthy, responsible and safe use of the Internet.
- Conducting awareness-raising and awareness-raising campaigns on the healthy and responsible use of the Internet. An example is the joint campaign with UNICEF targeting families (end of 2022) 'More than a mobile phone', which includes 'The guide that doesn't come with the mobile phone', with the decalogist of keys to be taken into account by families before giving their children the first mobile phone.

Raising awareness and holding children and parents liable for the unlawful online dissemination of images, audios or sensitive information, with administrative, civil, criminal and educational disciplinary liability. The Law on the Comprehensive Protection of Children and Adolescence from Violence already provides that persons over the age of 14 may be penalised for acts constituting an administrative offence in accordance with the rules on the protection of personal data.

- Actions against online content pages for adults (pornography) which either lack or are inconsistent with age verification systems, such as a mere declaration of majority.

Within this range of actions and measures, over the past year, the Working Group on Children, Digital Health and Privacy and the Agency have dedicated their work:

a. On the one hand, to raise awareness of the intensive, problematic or addictive use of the Internet, in the light of the data set out above.

   The screens have caused a profound transformation of the intellectual and behavioural performance of young people, where the proximity, the slowdown from one activity to another and their validation on social media are an essential part of their daily lives.

   In the above-mentioned report, the Federation for Aid to Drug Addiction states that 70.8 % are unaware of the time spent on social media and 64.3 % want to see them at all times.

   The effects or symptoms of such behaviour are similar to addictions to substances and need to be known in order to be able to cope with them, tolerance, abstinence syndromes, behavioural control difficulties, interference with everyday activities or disturbances in interpersonal relationships, and which in minors seriously affects their development as individuals, show that something is not going well and need to be identified early and action taken to prevent harm.

   As with drug addictions, it is difficult for an Internet or social media addict to consider him or herself as such, instead he / she normalises, minimises, justifies or denies the problem. It is generally a very negative event (school failure, behavioural disorders, repeated lies, social isolation, economic problems, family pressure) that alerts to the problem, mainly parents when it comes to minors.

   Regarding addictive use, the Agency supports all scientific initiatives aimed at providing guidelines and guidance that contribute to children's digital health, both physical and mental. Actions to tackle problematic or addictive use of ICT by minors.

   As a result of the work of the Working Group, in addition to identifying what constitutes problematic and addictive behaviour, it has been:

- The signing of Protocols of Action with the Councils of Associations of Psychologists and Physicians for collaboration on measures and actions to this end.
- Cooperation with the Spanish Pediatrics Association and support for its Digital Family Plan through awareness campaigns.

From scientific evidence, the Digital Family Plan has an impact on how the use of screens and the number of hours spent on them affects minors, offering recommendations, adapted to the needs of each family and the age of their children, so that they make good use of digital means in order to reap the benefits they bring and reduce the risks to their health and well-being.

It lays down guidelines on the maximum hours of use of screens by age, including leisure and classroom times. The Family Digital Plan states that the routine use of devices for distraction or calming purposes hinders the development of self-management strategies; it results in dependency on screens and will identify difficulties of self-regulation at later stages. For this reason, it advises against the use of screens before the age of six, considering that there is no safe time, with the exception of the use of screens for social contact in short times and for a specific purpose under the supervision of an adult.

b. The other area of action is the access of minors to online adult content, in particular pornography, as well as other inappropriate content such as extreme violence, betting or reward games.

The Working Group has held plenary and delegated meetings in the form of a workstream aimed at having an age verification tool for accessing online content for adults in accordance with the framework of the right to the protection of personal data.

Age verification for access to adult online content is a requirement set out in various regulations, such as the DSA, to protect minors from content or contacts that may upset, frighten, sadden, worry, anger or harass them; or Directive 2018/1808, amending Directive 2010/13 on audiovisual media services.

The outcome of the work carried out by the Agency was the presentation in December 2023 of the Decalogue with the principles and criteria to be met by an age verification system in accessing online content that respects data protection and privacy regulations, the implementation of which has been successfully tested, through proofs of concept, in the 3 largest browsers (Windows, IOS and Android).

In January 2024, the Agency presented its reinforced Strategy for the Protection of Children.

The strategy is designed on 3 core lines of action of the Agency, which are reinforced by 10 grassroots interventions.

THE FIRST LINE IS AIMED AT ACHIEVING COMPREHENSIVE PROTECTION OF CHILDREN IN THE DIGITAL ENVIRONMENT AND PROTECTING THEIR RIGHTS AND FREEDOMS IN THE PROCESSING OF THEIR PERSONAL DATA BY:

1. Support for reaching a State Pact.
2. The total amount made available to collaborate, through the coordination of the Working Group, on legal and technological analysis and studies in order to draw up a draft law on the comprehensive protection of minors on the Internet, including neurodata, as a special category of personal data, and their corresponding neurorights, in particular of minors.

THE SECOND FOCUS OF THIS STRATEGY IS TO STRENGTHEN THE GUARANTEES OF CHILDREN'S RIGHTS ON THE INTERNET BY:

3. Encouraging and collaborating with the bodies responsible for developing age verification apps in accessing digital content for adults in accordance with the principles and requirements adopted by the Agency, successfully tested in the proof-of-concept tests carried out, and presenting them in the European and transatlantic framework to serve as a model to follow.
4. Parental control tools and resources for privacy settings on social media, browsers and operating systems, in collaboration with the National Cybersecurity Institute.
5. Digital education on privacy for families and the rest of the education community in collaboration with the Ministry of Education and the National Cybersecurity Institute.
6. Support for educational authorities in the use of digital platforms and tools in line with data protection rules.
7. Investigative actions on these tools and platforms to ensure the protection of personal data.
8. Promoting impact assessments on privacy and digital health based on the age and risks of digital technologies, in cooperation with education, health authorities and the Councils of Physicians, Psychologists and Educators.

THE THIRD STRATEGIC COURSE OF ACTION IS THE FIGHT AGAINST UNLAWFUL PRACTICES IN THE FIELD OF CHILD DATA PROTECTION, BY:

9. Prioritising investigations into pornographic content websites, in particular checking the age of users, and coordinating with the EU authorities for websites that do not have an establishment in Spain.
10. The analysis of algorithms and addictive patterns that create dependence on Internet and which aim to influence user behaviour and decisions, and the coordination with the European Data Protection Board.

The interventions that reinforce these strategic lines are complemented and developed by a further 35 measures in different policy frameworks, including the following:

- The promotion of development and complementary regulation that requires the comprehensive protection of minors.
- Measures, in the exercise of the Agency's powers, focusing on investigative and sanctioning powers and understanding of the risks, rules, safeguards and rights affecting minors in the processing of their data.
- Similarly, in education, digital health and well-being frameworks, measures have been identified that, in cooperation with educational authorities and members of the educational community, health authorities and scientific organisations and societies, contribute to ensuring a secure digital space for children's and adolescents' rights in the framework of privacy and data protection.

A significant part of these measures find the right framework for their development and implementation in the Task Force driven by the Agency; and we hope to contribute to the goal of society: ensure that children can navigate safe over the Internet.

All measures are published and available on the Agency's website.

In addition to the actions undertaken by the Agency, the state of play of access to and use of digital services and products by minors, and the harmful consequences that may arise from their inappropriate and problematic use, has led to an intense debate that has put the protection of minors in the digital world as a priority, and several initiatives have been launched at national level.

A Committee of Experts for the Development of a Safe Digital Environment for Youth and Children was set up in January 2024 within the Ministry of Youth and Children, and of which the Agency is an active part, with the aim of producing a report containing

a diagnosis of the situation of minors in the online environment, analysing best practices and developing recommendations, measures and actions to contribute to their protection.

The report analyses the situation from different areas, including health, education, or privacy.

Just over a month later, a dedicated Task Force was set up within the Ministry for Digital Transformation to develop a technological solution to prevent minors from accessing inappropriate content while respecting users' privacy and ensuring the authenticity of the source, in which the Agency provides its catalogue of principles and its experience in developing these systems.

Similarly, the Spanish Government has submitted a preliminary draft law for the protection of minors in digital environments, which includes a series of measures to address the potential harm that Internet use may cause, taking into account the situations that have arisen and which are not protected by the Data Protection Law and the guarantee of digital rights of 2018, which contains several provisions in Title X on the protection of minors on the Internet.

The measures concern the following areas:

- Education, for schools, in accordance with the authorities' provisions, to regulate the use of mobile and digital devices in classrooms.
- Health, to identify problematic uses and promote specialised health care for children with substance-free addictive behaviour.
- Consumption, with a ban on access to digital services with random reward mechanisms and an obligation to include default parental control tools in digital devices.
- Data protection, raising the age of consent to the processing of personal data from 14 to 16, in the framework established by the GDPR.
- Criminal, adapt and lay down the provisions of the Criminal Code for the protection of minors, such as the use of false identities or deepfakes.

This is the current state of play of the system of protection of minors on the Internet and of the measures in place to create a healthy and safe digital environment that guarantees their rights and the full development of their personality.

We are facing a real public health problem for which we already arrive late, but still on time, and which requires the commitment of all sectors and actors involved: public authorities, health, education, digital security, families, industry, etc.

I conclude on the confidence that by combining efforts we can achieve the protection of our children and adolescents in the digital environment, as their future, which is also ours, is at stake.

Thank you.

Faustino Varela Monteiro
Presidente da Comissão Nacional de Protecção de Dados de Cabo Verde

Faustino Varela Monteiro é licenciado em Direito e mestrando em Direito e Ciências Jurídicas, menção Ciências Jurídico-Políticas, especialidade Direito Constitucional, na Faculdade de Direito da Universidade de Lisboa.

É Presidente da Comissão Nacional de Proteção de Dados desde 2015. É Conselheiro Jurídico da Rede Africana de Autoridades de Proteção de Dados Pessoais e representa Cabo Verde nas reuniões plenárias do Comité da Convenção 108 do Conselho da Europa.

Foi Diretor do Centro Jurídico da Chefia de Governo de Cabo Verde de outubro de 2011 a abril de 2015 e foi Juiz de Direito entre 2004 e 2011, primeiro de competência genérica e depois de competência especializada – Jurisdição Crime. Por designação do Conselho Superior da Magistratura Judicial, desempenhou também as funções de Juiz Auditor do Tribunal Militar de Instância, e foi membro da Comissão de Programas Especiais de Segurança.

Desde 2009 que é docente das disciplinas de Direito Penal, Direito Processual Penal e Direito das Contraordenações em cursos de formação especializados para inspetores de polícia judiciária, guardas municipais, oficiais de diligências e oficiais de justiça.

Participa regularmente em conferências e seminários nacionais e internacionais, com destaque para as dos Comissários de Proteção de Dados e Privacidade, hoje Assembleia Global da Privacidade (GPA), as organizadas pela Rede Africana das Autoridades de Proteção de Dados, Associação Francófona de Proteção de Dados e ID4 África.

Faustino Varela Monteiro holds a degree in Law, and he is taking his Master's degree in Law and Legal Sciences, Legal-Politic Sciences, with specialty in Constitutional Law, at the Faculty of Law of the University of Lisbon.

He has been President of the Data Protection Supervisory Authority since 2015. He is Legal Advisor to the African Network of Personal Data Protection Authorities and represents Cape Verde at the plenary meetings of the Convention 108 Committee of the Council of Europe.

He was Director of the Legal Centre of the Head of Government of Cape Verde from October 2011 to April 2015 and served as Judge of Law between 2004 and 2011, first of generic competence and then of specialized competence – Jurisdiction Crime. By appointment of the Supreme Judicial Council, he also served as Judge Auditor of the Military Court of Instance, and was a member of the Special Security Programs Commission.

Since 2009, he has been a lecturer in the disciplines of Criminal Law, Criminal Procedural Law and Administrative Offence Law in specialized training courses for judiciary police inspectors, municipal guards and bailiffs.

He regularly participates in national and international conferences and seminars, with emphasis on those of the Data Protection and Privacy Commissioners, today Global Privacy Assembly (GPA), those organized by the African Network of Data Protection Authorities, the Francophone Association of Data Protection and ID4 Africa.

OS DESAFIOS DO ESTABELECIMENTO DE UMA AUTORIDADE DE PROTEÇÃO DE DADOS E A IMPORTÂNCIA DA COOPERAÇÃO

I — INTRODUÇÃO

A criação de uma Autoridade de Proteção de Dados não é uma questão nova na legislação de proteção de dados. Tem a sua origem na segunda metade do século passado na Alemanha, mais precisamente na Lei de Proteção de Dados do estado de Hesse de 1970, como nos dá conta o Professor Alexandre Sousa Pinheiro[1].

Essa lei criou a figura do "Comissário de Proteção de Dados," o qual era eleito "pela Assembleia do estado federado, após apresentação de candidatura pelo Executivo. A sua ação verificava-se na área de tratamento de dados automatizados, informando a entidade responsável que incumpria a lei dos ilícitos em causa."[2]

De entre os vários contributos dessa percussora Lei de Proteção de Dados, destaca-se justamente a criação de entidade administrativa com competência para fiscalização em sede de proteção de dados, pelo facto de esta solução se transmigrar para diversos instrumentos jurídico-legislativos nacionais e internacionais.

Nesse particular, a lei de Proteção de Dados do estado de Hesse abriu as portas, designamente, para a Diretiva n.º 95/46/CE, de 24 de outubro (Diretiva sobre Proteção de Dados), transposta para o direito português através da Lei n.º 67/98, de 26 de outubro, que determinou que cada Estado-Membro estabelecesse que uma ou mais autoridades públicas, totalmente independentes no exercício de suas competências, fossem responsáveis pela fiscalização em matéria de proteção de dados pessoais[3].

Mas igualmente para a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, adotada na vigésima terceira sessão ordinária da cimeira, realizada em Malabo, Guiné Equatorial, a 27 de junho de 2014, mais conhecido por Convenção de Malabo.

Uma vez sinalizada a aparição do organismo de controlo em matéria de proteção de dados, procuraremos a seguir revelar, em breves notas históricas, o acolhimento do direito fundamental à proteção pessoais no direito cabo-verdiano, o estabelecimento do regime jurídico geral de proteção de dados pessoais das pessoas singulares e a sua alteração que culminou com a criação da Comissão Nacional de Protecção de Dados (CNPD) de Cabo Verde.

Evidentemente, o estabelecimento de uma autoridade de proteção de dados é condicionado pela natureza jurídica que lhe é atribuída, bem como pelas circunstâncias jurídico-constitucional-legal e socioeconómica e culturais que a envolvem. Assim, no segundo tópico expositivo apresentaremos alguns traços desses contextos que condicionam o efetivo funcionamento de uma autoridade de proteção de dados, particularizando o caso da CNPD de Cabo Verde.

Como é sabido, quer na fase do arranque de uma autoridade de proteção de dados quer, posteriormente, durante o exercício dos seus poderes, uma profícua cooperação com outras autoridades de proteção de dados configura-se como inexcedível à fiscalização do cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais.

1. *Seguimos de perto a posição da Cf. ALEXANDRE SOUSA PINHEIRO, Privacy e Protecção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional, Lisboa, AAFDL, 2015, p. 516, 517, 555 e 556.*
2. *Cf. ALEXANDRE SOUSA PINHEIRO, Privacy e Protecção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional, Lisboa, AAFDL, 2015, p. 516, 517.*
3. *Artigo 28.º da DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 24 de Outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.*

Assim, no último tópico dedicaremos breves palavras à importância da cooperação entre as autoridades de proteção de dados.

II

1. BREVES NOTAS HISTÓRICAS DO ACOLHIMENTO DO DIREITO FUNDAMENTAL À PROTEÇÃO PESSOAIS NO DIREITO CABO-VERDIANO E A CRIAÇÃO DA COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

A Constituição da República de Cabo Verde de 1992[4] (CRCV), na sua Parte II, (Direitos e Deveres dos Cidadãos), Título II (Direitos, Liberdades e Garantias) consagrou, pela primeira vez[5], a proteção de dados individualmente identificáveis tratados através de meios informáticos como direito fundamental.

Com a primeira revisão constitucional ordinária ocorrida em 1999[6], consolidou-se o texto do atual artigo 45.º da CRVC, o qual prevê, no seu n.º 1, o direito de acesso dos cidadãos aos dados informatizados que lhes dizem respeito, o direito de os retificar e atualizar, bem como o direito de conhecer a finalidade a que se destinam.

O preceito constitucional antes aludido remete, no seu n.º 3, a regulação da "proteção de dados constantes dos registos informáticos, as condições de acesso aos bancos de dados, de constituição e de utilização por autoridades públicas e entidades privadas de tais bancos ou de suportes informáticos dos mesmos" para a lei.

Nestes termos, veio a Assembleia Nacional, através da Lei n.º 133/V/2001, de 22 de janeiro[7], estabelecer o Regime Jurídico Geral de Proteção de Dados Pessoais de Pessoas Singulares, tendo como nítida fonte inspiradora a lei portuguesa já aludida sobre a matéria, (Lei n.º 67/98, de 26 de outubro), que transpôs para o direito português a Diretiva n.º 95/46/CE, de 24 de outubro (Diretiva sobre Proteção de Dados).

Não obstante o Regime Jurídico Geral de Proteção de Dados Pessoais de Pessoas Singulares ter seguido de muito perto a Lei Portuguesa, em relação à natureza da autoridade para a fiscalização de proteção de dados pessoais, houve um desvio considerável desta, tendo consagrado, no seu artigo 22.º, que "a fiscalização da proteção de dados pessoais é assegurada pela Assembleia Nacional, através de uma Comissão Parlamentar de Fiscalização, que seria regulada por lei própria.

No entanto, a Comissão Parlamentar de Fiscalização não se operacionalizou.

Assim sendo, em 2013, a Lei n.º 133/V/2001, de 22 de janeiro, foi alterada pela Lei n.º 41/VIII/2013 de 17 de setembro[8], tendo consagrado que "a fiscalização de proteção de dados pessoais é assegurada por uma autoridade administrativa independente, a Comissão Nacional de Proteção de Dados (CNPD), que funciona junto da Assembleia Nacional".

Importa sublinhar que, diferentemente da Constituição da República Portuguesa que, no n.º 2 do seu artigo 35.º, faz expressa menção à supervisão do tratamento de dados pessoais através de entidade administrativa independente, "tornando incontornável a obrigatoriedade da criação desta entidade pelo legislador", a Constituição da República de Cabo Verde[9] é omissa neste aspeto.

4. *Lei Constitucional n.º 1/IV/92, de 25 de setembro.*
5. *A Lei sobre Organização Política do Estado (LOPE), aprovada a 4 de julho de 1975 para entrar em vigor dia seguinte, ou seja, 5 de julho de 1975, dia da Independência nacional, era omissa em matéria de direitos fundamentais. A Constituição da República de Cabo Verde aprovada em 5 de setembro 1980 e publicada a 13 de outubro do mesmo ano, não obstante consagrar um conjunto de direitos fundamentais, ignorou quer o direito à reserva da intimidade da vida privada e familiar quer o direito à proteção de dados.*
6. *Lei Constitucional n.º 1/V/99, de 23 de novembro.*
7. *É considerada a primeira Lei de Proteção de Dados aprovada por um país africano.*
8. *Por seu turno, alterada pela Lei n.º 121/IX/2021, de 17 de março.*
9. *O n.º 12.º do artigo 60.º da CRCV determina que "cabe a uma autoridade administrativa independente assegurar a regulação da comunicação social", garantindo um conjunto de direitos e interesses.*

Parece-nos importante dar nota que a CRCV estabelece no n.º 3 do artigo seu 240.º a possibilidade da lei criar autoridades administrativas independentes.

É sobretudo com base neste artigo que a CNPD tem respaldo constitucional, tendo a Lei n.º 42/VIII/2013, de 17 de setembro[10], regulado a sua composição, a competência, a organização e o modo de funcionamento, estabelecendo que é uma entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade e dotada de autonomia administrativa e financeira.

A CNPD é composta por três membros de reconhecida competência e integridade moral, incluindo o presidente, eleitos pela Assembleia Nacional, por maioria de dois terços dos deputados presentes, desde que superior à maioria absoluta dos Deputados em efetividade de funções, por um mandato de seis anos podendo ser renovado uma única vez.

Os membros da CNPD são inamovíveis, não podendo as suas funções cessar antes do término do mandato, exceto em casos de: (1) morte ou incapacidade física permanente ou com uma duração que se preveja ultrapassar a data do termo do mandato; (2) Renúncia ao mandato; (3) ou Perda do mandato.

Note-se que a fiscalização da proteção de dados pessoais incumbida à CNPD visa "acompanhar, avaliar e controlar" o cumprimento das disposições constitucionais, legais e regulamentares em matéria de proteção dados pessoais. Assim, enquanto autoridade pública responsável pela fiscalização, dispõe de:

I. Poderes de investigação e de inquérito;

II. Poderes de autoridade;

III. Poder de emitir pareceres prévios ao tratamento de dados pessoais.

No entanto, como é sabido, a fiscalização levada ao cabo pela CNPD não dispensa o controlo jurisdicional exercido através dos tribunais, ao qual a CNPD está sempre sujeita.

Neste ponto passemos ao segundo tópico:

2. CIRCUNSTÂNCIAS JURÍDICO-CONSTITUCIONAL-LEGAL E SOCIOECONÓMICA E CULTURAIS QUE INFLUENCIAM O ESTABELECIMENTO DE UMA AUTORIDADE DE PROTEÇÃO DE DADOS

A natureza jurídica da autoridade de proteção de dados é de suma importância na sua institucionalização. O modelo adotado pela Constituição da República Portuguesa antes referido, o qual consiste na elevação à natureza de norma constitucional a garantia institucional de proteção de dados pessoais, é, a nosso ver, mais adequado, sobretudo para os Estados onde, ainda, o respeito pela dignidade da pessoa humana, pelos direitos e liberdades fundamentais e pela separação de funções entre os órgãos de soberania e, por conseguinte, o Estado de Direito e a democracia não se encontram consolidados.

A CRP, ao estabelecer no n.º 2 do seu artigo 35.º que a supervisão do tratamento de dados pessoais é garantida por entidade administrativa independente, confere-lhe uma força

10. *Alterada pela Lei n.º 120/IX/2021, de 17 de março.*

especial que decorre da necessária vinculação de todos os poderes públicos constituídos (também em certa medida dos particulares) aos ditames constitucionais.

No caso de Cabo Verde, a CNPD beneficia, como já dissemos, da referência genérica feita no n.º 3 do artigo 240.º da CRCV quanto à possibilidade da lei criar autoridades administrativas independentes.

Assim sendo, um dos grandes desafios do estabelecimento de uma autoridade de proteção de dados é, uma vez eleitos ou designados os seus membros, (processos que admitem alguma influência política), estes não se deixarem ser capturados pela direção, tutela ou superintendência[11] dos poderes políticos.

Entendemos que as funções de garantia e de tutela de direitos, liberdades garantias das pessoas singulares pressupõem um funcionamento imparcial das autoridades de proteção de dados, para o qual muito contribui um estatuto garantístico dos membros.

A independência financeira ou, melhor, a suficiência financeira de autoridade de supervisão de tratamento de dados constitui um outro desafio.

Como é sabido, a independência funcional requer, em parte, que a autoridade de proteção de dados tenha, por um lado, o seu orçamento inscrito, de forma autónoma, podendo ser no orçamento geral do Estado ou no orçamento privativo das respetivas Assembleias Nacionais, que é o caso do orçamento da CNPD de Cabo Verde; e, por outro lado, que seja a autoridade de proteção de dados a executar o seu orçamento, observando obviamente os princípios e as regras de execução orçamental.

Só desse modo, a nosso ver, estará garantida a independência necessária ao cumprimento eficaz das suas atribuições.

Aliado ao desafio de insuficiência financeira, encontra-se a escassez de recursos humanos especializados. O rítmo estonteante da evolução tecnológica e a mudança rápida do universo físico para o digital, em que o dado pessoal é "o combustível, cujo tratamento "não implica o seu dispêndio e pode, inclusivamente, aumentar o seu valor"[12], exigem que uma autoridade de proteção de dados tenha trabalhadores qualificados e com conhecimentos específicos para acompanhar as inovações tecnológicas e antecipar os riscos para as pessoas relativamente aos seus direitos à reserva da vida privada e à proteção dos dados pessoais em virtude do tratamento dos seus dados pessoais.

Ora, isso requer que os trabalhadores sejam bem remunerados e estejam constantemente a atualizar os seus conhecimentos no domínio das tecnologias e da proteção de dados pessoais.

Os desafios elencados encontram expressão quer nos n.ºs 1 e 8 do artigo 11.º da Convenção de Malabo, que dispõem que cada Estado Parte deve criar uma autoridade responsável pela proteção de dados pessoais, a qual é um órgão administrativo independente e autónomo, devendo ainda comprometer-se em dotar a autoridade de recursos humanos, técnicos e financeiros necessários para o cumprimento da sua missão.

Quer nos considerandos 117 e 120 do RGPD, segundo os quais "a criação de autoridade de controlo nos Estados-Membros, habilitada a desempenhar as suas funções e a exercer os seus poderes com total independência, constituiu um elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais." E que "Deverão

11. *VITAL MOREIRA, Administração Autónoma e Associações Públicas, Coimbra, Coimbra Editora, 1997, p. 127, define a administração independente "toda a administração infra-estadual prosseguida por instâncias administrativas não integradas na administração direta do Estado e livres da orientação e da tutela estadual, sem, todavia, corresponderem à auto-administração de quaisquer interesses organizados".*

12. *JORGE PEREIRA DA SILVA, Direitos Fundamentais para o Universo Digital, Lisboa, Fundação Francisco Manuel dos Santos, 2023, p. 92. Acrescenta este autor que, "ao contrário do que sucede com os derivados do petróleo, cuja utilização implica sempre o seu consumo, os dados podem ser utilizados e reutilizados sem limites, para diferentes finalidades".*

ser dados às autoridades de controlo os recursos financeiros e humanos, as instalações e as infraestruturas necessárias ao desempenho eficaz das suas atribuições, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União)."

Dependendo do contexto sociocultural, embora nos pareça que no universo digital praticamente não há sociedade que não careça de ações pedagógicas, as quais, aliás, devam merecer um esforço contínuo, qualquer autoridade de proteção de dados, no seu arranque, tem de ter um viés mais educativo do que punitivo. Pelo menos, isso revelou ser o mais adequado para a CNPD de Cabo Verde.

Como é sabido, para que se adquira uma cultura de proteção de dados pessoais na "sociedade técnica" de hoje, é preciso que a autoridade de controlo adote preferencialmente ações educativas e de sensibilização dos cidadãos, das empresas e das entidades públicas sobre a importância do respeito pela proteção dos dados pessoais e das responsabilidades impostas pelo seu tratamento.

Assim, a nosso ver, constitui um desafio renovado debater questões de proteção de dados pessoais e disseminar as boas práticas, num esforço de sensibilização de todos para a importância destas matérias, sem prejuízo de se socorrer de ação sancionatória se se justificar.

Nesta tarefa de educar e sensibilizar a sociedade em geral sobre a importância da proteção de dados, não se pode olvidar a evolução da regulamentação e os padrões globais neste domínio, daí a importância decisiva da cooperação, a qual será abordada no próximo e último tópico.

3. IMPORTÂNCIA DA COOPERAÇÃO ENTRE AS AUTORIDADES DE PROTEÇÃO DE DADOS

Comecemos com o Considerando 116 do RGPD, segundo o qual: "Sempre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras." (…). "Por conseguinte, revela-se necessário promover uma cooperação mais estreita entre as autoridades de controlo da proteção de dados, a fim de que possam efetuar o intercâmbio de informações e realizar investigações com as sua homólogas internacionais."

Assiste-se, hoje, uma intensa migração de praticamente todas as dimensões das atividades humanas para o "universo digital", através de grandes meios tecnológicos de informação e comunicação ou plataformas movidos, sobretudo, por dados pessoais de pessoas singulares. E se há coisa que este universo não conhece são fronteiras[13], pelo que os dados pessoais de pessoas singulares estão permanentemente e de forma intensa a atravessar fronteiras.

Neste sentido, nos domínios das atribuições das autoridades de proteção de dados, a cooperação entre as mesmas é absolutamente necessária, designadamente na assistência mútua através do intercâmbio de informações relevantes e úteis, na coordenação de investigações e na condução de ações conjuntas para o efeito.

13. *JORGE PEREIRA DA SILVA, Direitos Fundamentais para o Universo Digital, Lisboa, Fundação Francisco Manuel dos Santos, 2023, p. 9.*

Essa cooperação em matéria de proteção de dados revela-se assaz útil, pois existe, hoje, uma tendência para se alinhar gradualmente as leis de proteção de dados, quer com a Convenção 108 modernizada, quer com a Convenção de Malabo, quer, ainda, com o RGPD[14].

E essa harmonização é crucial não só para proteger eficazmente os cidadãos relativamente à sua vida privada e ao tratamento automatizado dos seus dados pessoais, bem como para facilitar o comércio e investimento internacionais numa sociedade cada vez mais digital e globalizada.

Reputamos, igualmente, de extraordinária importância a cooperação, sobretudo quando uma autoridade de proteção de dados se encontra nos arrancos das suas funções.

A esse nível, a cooperação revela-se profícua em assistência e troca de experiências, de conhecimento e das melhores práticas, bem como na formação dos trabalhadores e na colaboração do desenvolvimento de instrumentos de gestão e de diretrizes, na disseminação de guias e outros materiais de sensibilização.

Outrossim, a cooperação entre as autoridades de proteção de dados tem proporcionado, além de assinatura de acordos bilaterais[15], a adesão de Estados à Convenção 108 e à Convenção de Malabo; a participação em fóruns e conferências internacionais relacionados com a proteção de dados, (de que esta conferência é um bom exemplo); a mobilização de recursos para implementação de projetos promovidos por autoridades de proteção de dados; e a criação de Redes e Associações de autoridades de proteção de dados, das quais destacamos a Rede Ibero-americana de Proteção de Dados, a Rede Africana de Autoridades de Proteção de Dados[16], a Associação Francófona de Autoridades de Proteção de Dados e a Assembleia Global da Privacidade[17].

Esses organismos têm desempenho relevantes funções em ordem à fixação de modelos e práticas uniformes e globais em matéria de proteção dados pessoais.

Outrossim têm incentivado reflexões sobre novas e renovadas questões de proteção de dados pessoais, bem como contribuído para a realização de trabalhos em rede, de pesquisas, estudos, etc, abrindo portas para intercâmbios mais fluidos e seguros entre as autoridades de proteção de dados.

Face a essas enormes vantagens, terminamos com a seguinte pergunta: o que nos falta para a criação de uma Rede Lusófona de Autoridades de Proteção de Dados?

Muito obrigado pela vossa atenção.
Parabéns à CNPD!

14. *Não constitui novidade que, em matéria de proteção de dados, a Europa tem ditado os padrões, os quais têm sido seguidos em todos os continentes. Esses dois instrumentos jurídicos internacionais estimulam ações de cooperações entre as autoridades de proteção de dados e estabelecem formas de cooperação.*

15. *A CNPD de Cabo Verde assinou acordos bilaterais com a CNPD de Portugal e com a Agência de Proteção de Dados de Angola.*

16. *A CNPD de Cabo Verde é membro observador.*

17. *A CNPD de Cabo Verde é membro das duas organizações.*

Faustino Varela Monteiro
President of the Data Protection Supervisory Authority of Cape Verde

THE CHALLENGES OF SETTING UP A DATA PROTECTION AUTHORITY AND THE IMPORTANCE OF COOPERATION

I — INTRODUCTION

The creation of a Data Protection Authority is not a new issue in data protection legislation. It originated in the second half of the last century in Germany, more precisely with the Data Protection Act of the State of Hesse of 1970, as reported by Professor Alexandre Sousa Pinheiro[1].

This law created the figure of the "Commissioner for Data Protection", who was elected "by the Assembly of the Federal State, upon nomination by the Executive. Its action took place in the area of automated data processing, informing the responsible entity that it failed to comply with the law of the offences in question"[2].

Among the various contributions made by this pioneering Law on data protection, the creation of an administrative body with competence for data protection supervision is particularly noteworthy, as this solution was transferred to various national and international legal and legislative instruments.

In that regard, the Law on Data Protection of the State of Hesse opened the doors, namely to Directive 95/46/EC of 24 October 2006 (Data Protection Directive), – transposed into

1. *We closely follow the position of Cf. ALEXANDRE SOUSA PINHEIRO, Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional, Lisboa, AAFDL, 2015, p.516, 517, 555 and 556.*
2. *Cf. ALEXANDRE SOUSA PINHEIRO, Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional, Lisboa, AAFDL, 2015, p. 516, 517.*

Portuguese law by Law 67/98 of 26 October 2006 –, which provided that each Member State was to provide that one or more public authorities, fully independent in the exercise of their powers, were responsible for the supervision of the protection of personal data[3].

But also for the African Union Convention on Cybersecurity and Personal Data Protection, adopted at the twenty-third regular session of the Summit, held in Malabo, Equatorial Guinea on 27 June 2014, better known as the Malabo Convention.

Once we have signalled the appearance of the Data Protection Authority, we will seek below to reveal, in short historical notes, the reception of the fundamental right to personal protection in Cape Verdean law, the establishment of the general legal regime for the protection of personal data of natural persons and its amendment, which culminated in the creation of the Data Protection Supervisory Authority (CNPD) of Cape Verde.

Of course, the establishment of a data protection authority is conditioned by the legal nature attributed to it as well as by the constitutional, legal and socio-economic and cultural circumstances surrounding it. Thus, in the second expositive topic, we will present a number of features of these contexts that determine the effective functioning of a data protection authority, with a particular focus on the case of the CNPD of Cape Verde.

As it is well known, both during the start-up phase of a data protection authority and, subsequently, during the exercise of its powers, a fruitful cooperation with other data protection authorities appears to be beyond the control of compliance with the laws and regulations on the protection of personal data. Thus, in the last topic we will dedicate some brief words to the importance of cooperation between data protection authorities.

II

1. BRIEF HISTORICAL NOTES ON THE RECOGNITION OF THE FUNDAMENTAL RIGHT TO PERSONAL PROTECTION IN CAPE VERDEAN LAW AND THE CREATION OF THE DATA PROTECTION SUPERVISORY AUTHORITY

The Constitution of the Republic of Cape Verde of 1992[4] (CRCV), Part II (Rights and Duties of Citizens), Title II (Rights, Freedoms and Guarantees) enshrined, for the first time[5], the protection of individually identifiable data processed by computer means as a fundamental right.

With the first ordinary constitutional revision in 1999[6], the text of the current Article 45 of the CRVC was consolidated, which provides, in paragraph 1, for citizens' right of access to computerised data related to them, the right to rectify and update it and the right to know the purpose for which it was intended.

Paragraph 3 of the abovementioned constitutional provision refers to the regulation of 'the protection of data contained in computer records, the conditions of access to databases, and the creation and use by public authorities and private entities of such databases or their computer media' for the law.

Accordingly, by Law 133/V/2001 of 22 January[7], the National Assembly established the general legal framework for the protection of personal data of natural persons, taking as a

3. *Article 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*
4. *Constitutional Law No 1/IV/92, of 25 September.*
5. *The Law on State Political Organisation (LOPE), adopted on 4 July 1975 to enter into force on the following day, i.e. 5 July 1975, the day of national independence, was silent on fundamental rights. The Constitution of the Republic of Cape Verde adopted on 5 September 1980 and published on 13 October of the same year, while enshrining a number of fundamental rights, ignored both the right to privacy and family life and the right to data protection.*
6. *Constitutional Law 1/V/99, of 23 November.*
7. *It is considered the first Data Protection Act passed by an African country.*

clear inspiration the Portuguese law on the subject (Law 67/98 of 26 October 2009), which transposed into Portuguese law the Directive 95/46/EC of 24 October 2009 (Data Protection Directive).

Although the General Legal Framework for the Protection of Personal Data of Individual Persons has closely followed the Portuguese Law, in relation to the nature of the authority responsible for the supervision of personal data protection, there has been a considerable deviation from that law, stating in Article 22 that "the supervision of the protection of personal data is ensured by the National Assembly, through a Parliamentary Supervisory Committee, which would be regulated by its own law".

However, the Parliamentary Supervisory Committee has not been operational.

Thus, in 2013, Law 133/V/2001 of 22 January was amended by Law 41/VIII/2013 of 17 September[8], stating that 'the supervision of the protection of personal data is carried out by an independent administrative authority, the Data Protection Supervisory Authority (Comissão Nacional de Proteção de Dados – CNPD), which operates at the National Assembly.

It should be noted that, unlike the Constitution of the Portuguese Republic, which, in Article 35(2), makes express reference to the supervision of the processing of personal data by means of an independent administrative body, 'making mandatory the establishment of such an entity by the legislator', the Constitution of the Republic of Cape Verde[9] is silent on this point.

In our view, it is important to note that the CRCV establishes in Article 240(3) the possibility for the law to set up independent administrative authorities.

It is above all on the basis of this article that the CNPD has constitutional support, with Law 42/VIII/2013 of 17 September[10] regulating its composition, competence, organisation and method of operation, establishing that it is an independent administrative body, with legal personality governed by public law and powers of authority and with administrative and financial autonomy.

The CNPD is composed of three members of recognised competence and moral integrity, including the President, elected by the National Assembly, by a two-thirds majority of the members present, provided that it exceeds the absolute majority of effective Members, for a term of six years and may be renewed once.

Members of the CNPD shall be irremovable and their duties may not be terminated before the end of their term of office, except in cases of: (1) death or physical incapacity of permanent or expected duration beyond the end of the term of office; (2) resignation; (3) or loss of mandate.

It should be noted that the supervision of the protection of personal data entrusted to the CNPD aims to "monitor, evaluate and control" compliance with constitutional, legal and regulatory provisions on personal data protection. Thus, as the public authority responsible for supervision, it has:

I. Investigative and inquiry powers;

II. Authority powers;

III. The power to issue opinions prior to the processing of personal data.

8. *As amended by Law 121/IX/2021 of 17 March 2006.*

9. *Article 60.12 of the CRCV states that "it is for an independent administrative authority to ensure media regulation", ensuring a set of rights and interests.*

10. *Amended by Law 120/IX/2021 of 17 March.*

However, as is well known, the review carried out by the CNPD does not preclude judicial review through the courts, to which the CNPD is always subject.

On this point, we turn to the second topic:

2. CONSTITUTIONAL, LEGAL AND SOCIO-ECONOMIC AND CULTURAL CIRCUMSTANCES INFLUENCING THE ESTABLISHMENT OF A DATA PROTECTION AUTHORITY

The legal nature of the data protection authority is of paramount importance in its institutionalisation. The model adopted by the Constitution of the Portuguese Republic referred to above, which consists of upgrading the institutional guarantee for the protection of personal data to the status of constitutional rule, is, in my view, more appropriate, in particular, for States where respect for human dignity, fundamental rights and freedoms and the separation of powers between sovereign bodies and, therefore, the rule of law and democracy are not consolidated.

The CRP, by providing in Article 35(2) that supervision of the processing of personal data is to be ensured by an independent administrative body, confers on it a special force deriving from the need to bind all the public authorities constituted (also to a certain extent by individuals) to constitutional requirements.

In the case of Cape Verde, the CNPD benefits, as I have already said, from the general reference in Article 240(3) of the CRCV to the possibility of establishing independent administrative authorities.

Therefore, one of the major challenges of establishing a data protection authority is, once its members have been elected or appointed, (processes that admit some political influence), they are not captured by the direction, influence or oversight[11] of political powers.

We believe that the functions of guaranteeing and protecting the rights and freedoms of natural persons presuppose the impartial functioning of the data protection authorities, to which a guarantee based status of members is paramount.

Financial independence or, better, the financial sufficiency of a data protection authority is another challenge.

As is well known, functional independence requires, in part, that the data protection authority should, on the one hand, have its budget allocated autonomously and may be included in the general budget of the State or in the private budget of the respective National Assemblies, which is the case with the budget of the CNPD of Cape Verde; and, on the other hand, that the data protection authority executes its budget, obviously following the principles and rules of budget implementation.

Only then, in our view, the independence necessary for the effective performance of its tasks will be guaranteed.

Combined with the challenge of financial insufficiency, there is a shortage of specialised human resources. The current rhythm of technological change and the rapid change from the physical to digital universe, where personal data is "fuel, the processing of which "does not involve its expenditure and may even increase its value"[12], requires a data protection authority to have qualified and knowledgeable workers to keep up with technological innovations and

11. *Vital MOREIRA, Administração autónoma e associações públicas, Coimbra, Coimbra Editora, 1997, p.127, defines as independent administration 'any sub-state administration pursued by administrative bodies which are not part of the direct administration of the State and are free from State guidance and supervision, without, however, corresponding to the self-administration of any organised interests'.*

12. *Jorge PEREIRA DA SILVA, Direitos Fundamentais para o Universo Digital, Lisboa, Francisco Manuel dos Santos Foundation, 2023, p.92. It adds that, 'unlike petroleum derivatives, the use of which always involves their consumption, the data may be used and re-used without limitation, for different purposes'.*

anticipate the risks for individuals with regard to their rights to privacy and the protection of personal data as a result of the processing of their personal data.

This requires that workers be well paid and constantly update their knowledge in the field of technology and personal data protection.

The challenges listed are reflected in both Article 11(1) and (8) of the Malabo Convention, which provide that each State Party shall establish a personal data protection authority, which shall be an independent and autonomous administrative body and shall undertake to provide the authority with the necessary human, technical and financial resources to fulfil its mission.

Recitals 117 and 120 of the GDPR, state that 'the establishment of a supervisory authority in the Member States, empowered to carry out their tasks and exercise their powers in complete independence, is an essential element of the protection of individuals with regard to the processing of their personal data' and that '[T]he supervisory authorities shall be given the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities in the Union'.

Depending on the socio-cultural context, although it seems to me that in the digital world there is hardly any society that does not require educational actions, which, moreover, should be continuously pushed for, any data protection authority, when it starts, must have a more educational rather than punitive vision. At least, this proved to be the most appropriate for the CNPD of Cape Verde.

As is well known, in order to acquire a culture of personal data protection in today's 'technical society', the supervisory authority must preferably adopt educational and awareness-raising measures for citizens, businesses and public authorities on the importance of respect for the protection of personal data and the responsibilities imposed for their processing.

Thus, in our view, it is a renewed challenge to discuss issues of personal data protection and to disseminate best practices in an effort to raise awareness of the importance of these matters, without prejudice to the need for sanctions to be taken if appropriate.

In this task of educating and raising awareness among society about the importance of data protection, we should not forget the evolution of regulation and global standards in this area, hence the decisive importance of cooperation, which will be addressed in the next and last topic.

3. IMPORTANCE OF COOPERATION BETWEEN DATA PROTECTION AUTHORITIES

Let's start with Recital 116 GDPR, according to which: "When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders."(…) Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts".

Today, there is an intense migration of virtually every dimension of human activities to the "digital universe", through large technological means of information and communication or platforms driven mainly by personal data of individuals. And if this universe does not know any borders[13], so the personal data of natural persons are permanently and intensively crossing borders.

In this respect, the cooperation between the data protection authorities is absolutely necessary, in particular in mutual assistance through the exchange of relevant and useful information, the coordination of investigations and the conduct of joint actions to that end.

Such data protection cooperation is very useful, as there is now a tendency to gradually align data protection laws with both the modernised Convention 108, the Malabo Convention and the GDPR[14].

This harmonisation is crucial not only to effectively protect citizens with regard to their private lives and the automated processing of their personal data, but also to facilitate international trade and investment in an increasingly digital and globalised society.

We also consider cooperation to be of extraordinary importance, especially when a data protection authority is just starting out.

At this level, cooperation is fruitful in assisting and exchanging experience, knowledge and best practices, as well as in training workers and collaborating in the development of management tools and guidelines, the dissemination of guides and other awareness-raising materials.

Moreover, cooperation between data protection authorities has provided, in addition to the signing of bilateral agreements[15], for the accession of States to Convention 108 and the Malabo Convention; participation in international fora and conferences related to data protection (of which this conference is a good example); the mobilisation of resources for the implementation of projects promoted by data protection authorities; and the creation of networks and associations of data protection authorities, including the Ibero-American Data Protection Network[16], the African Network of Data Protection Authorities, the French-speaking Association of Data Protection Authorities and the Global Privacy Assembly[17].

Those bodies shall carry out relevant tasks in order to establish uniform and comprehensive models and practices for the protection of personal data.

They have also encouraged reflections on new and renewed personal data protection issues, as well as contributing to networking, research, studies, etc., opening doors for more fluid and safer exchanges between data protection authorities.

In view of these huge advantages, we end with the following question: What is missing for the creation of a Lusophone Network of Data Protection Authorities?

Thank you for your attention.
Congratulations to the CNPD!

13. *Jorge PEREIRA DA SILVA, Direitos Fundamentais para o Universo Digital, Lisboa, Francisco Manuel dos Santos Foundation, 2023, p.9.*

14. *It is not new that Europe has dictated the standards in data protection, which have been followed on all continents. These two international legal instruments stimulate cooperation between data protection authorities and establish forms of cooperation.*

15. *The CNPD of Cape Verde has signed bilateral agreements with the CNPD of Portugal and the Angolan Data Protection Agency.*

16. *The CNPD of Cape Verde is an observer member.*

17. *The CNPD of Cape Verde is a member of both organisations.*

Wojciech Wiewiórowski
Autoridade Europeia para a Proteção de Dados

É a Autoridade Europeia para a Proteção de Dados (EDPS) desde 6 de dezembro de 2019.

Professor adjunto na Faculdade de Direito e Administração da Universidade de Gdańsk.

Foi, entre outros, conselheiro no domínio do governo eletrónico e da sociedade da informação do Ministro do Interior e da Administração, Diretor do Departamento de Informatização do Ministério do Interior e da Administração. Representou igualmente a Polónia no Comité das Soluções de Interoperabilidade para as Administrações Públicas Europeias (Comité ISA), que assiste a Comissão Europeia.

Foi o Inspetor-Geral para a Proteção de Dados Pessoais (Comissário para a Proteção de Dados da Polónia) de 2010-2014, e Vice-Presidente do Grupo de Trabalho do Artigo 29.º em 2014. Em dezembro de 2014, foi nomeado Autoridade-Adjunta da Autoridade Europeia para a Proteção de Dados. Após a morte do EDPS – Giovanni Buttarelli, em agosto de 2019 – substituiu o Sr. Buttarelli como EDPS em exercício.

As suas áreas de atividade científica incluem, em primeiro lugar, o direito informático polaco e europeu, o tratamento e a segurança da informação, os sistemas de recuperação de informações jurídicas, a informatização da administração pública e a aplicação de novas ferramentas informáticas (web semântica, ontologias jurídicas, computação em nuvem, blockchain) no tratamento de informações jurídicas.

European Data Protection Supervisor (EDPS) since 6th December 2019.

Adjunct Professor in the Faculty of Law and Administration of the University of Gdańsk.

He was among others adviser in the field of e-government and information society for the Minister of Interior and Administration, the Director of the Informatization Department at the Ministry of Interior and Administration. He also represented Poland in committee on Interoperability Solutions for European Public Administrations (the ISA Committee) assisting the European Commission.

The Inspector General for the Protection of Personal Data (Polish Data Protection Commissioner) 2010-2014 and the Vice-Chair of the Working Party Article 29 in 2014. In December 2014, he was appointed Assistant European Data Protection Supervisor. After the death of the Supervisor – Giovanni Buttarelli in August 2019 – he replaced Mr. Buttarelli as acting EDPS.

His areas of scientific activity include first of all Polish and European IT law, processing and security of information, legal information retrieval systems, informatization of public administration, and application of new IT tools (semantic web, legal ontologies, cloud, blockchain) in legal information processing.

PROTEÇÃO DE DADOS E DEMOCRACIA
REFLEXÕES DA AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS (AEPD)

Senhor Vice-Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias

Senhora Presidente da Comissão Nacional de Proteção de Dados, querida Paula Meira Lourenço

Senhoras e senhores, queridos amigos

Por vezes, estamos muito concentrados ou focados nas datas e nos números: celebrar o 30.º aniversário é maravilhoso, mas o que realmente importa é a maturidade, a experiência e a fiabilidade da Autoridade de Proteção de Dados em Portugal. Devo dizer que sempre que a Autoridade Europeia para a Proteção de Dados tenta pensar nos aliados com os quais podemos começar algum assunto difícil, Portugal aparece como um dos primeiros. E um bom exemplo disso foi quando decidimos, em 2022, fazer a primeira ação coordenada de supervisão da Procuradoria Europeia, e a Comissão Nacional de Proteção de Dados de Portugal foi a Autoridade Nacional de Proteção de Dados que estava mais bem preparada para ter este papel de verificar a forma como os Procuradores estão a aplicar as regras relativas à Procuradoria Europeia. E também me leva diretamente a agradecer à pessoa cujo nome já foi falado hoje, Clara Guerra, pela cooperação neste campo.

Coincidentemente, há alguns dias, a Autoridade Europeia para a Proteção de Dados celebrava o seu 20.º aniversário e, mais uma vez, enquanto para as pessoas do meu país de origem, a Polónia, 2004 foi a data de acesso à União Europeia, para nós, na AEPD, é a data de nascimento da nossa instituição. Não foi há muito tempo. Não sei se se lembram que 2004 foi o ano do Campeonato da Europa de futebol, onde Cristiano Ronaldo já jogava.

Assim, ainda que já tenhamos feito os 20 anos em janeiro, na semana passada comemorámos o nosso aniversário com uma conferência especial: «Cimeira Europeia sobre a Proteção de Dados: Repensar os dados nas sociedades democráticas». Por conseguinte, tenho hoje a oportunidade de partilhar convosco as ideias da conferência e de refletir convosco sobre os papéis e o lugar da privacidade e da proteção de dados nas democracias, o que significa para elas enquanto disciplina. A nossa anfitriã Paula Meira Lourenço pediu-me que abordasse na minha apresentação de hoje os aspetos mais importantes do debate que tivemos em Bruxelas na quinta-feira passada.

Mas permitam-me que comece por explicar qual é o papel da Autoridade Europeia para a Proteção de Dados, que pode não ser tão óbvio para todas as pessoas aqui presentes. A Autoridade Europeia para a Proteção de Dados é a instituição de controlo das instituições, órgãos e organismos da União Europeia. Portanto, não estamos a supervisionar o mercado, mas sim as instituições. Se vierem a Bruxelas e tiverem problemas com a proteção de dados numa loja ou no hotel, têm de contactar a Autoridade Belga de Proteção de Dados. Mas quando tiverem estes problemas com o Parlamento Europeu, a Comissão Europeia, o Conselho ou qualquer agência que exista na Europa, dirijam-se à Autoridade Europeia para a Proteção de Dados (AEPD).

Por isso, temos também duas ilhas da nossa jurisdição aqui em Portugal com a EMSA (Agência Europeia da Segurança Marítima) e a Agência da União Europeia para a Droga que vai ganhar um novo nome a partir de 1 de julho deste ano. Enquanto AEPD, somos também o principal conselheiro no processo legislativo na União Europeia e estamos a assegurar o secretariado do Comité Europeu para a Proteção de Dados, de que a Anu Talus é presidente.

Enquanto AEPD, temos esta perspetiva específica que decorre do mandato específico limitado ao aconselhamento e supervisão de entidades exclusivamente públicas. O que isto implica – se me permitem, para efeitos de argumentação, considerar as Instituições Europeias como reflexo das funções do Estado – é, portanto, algo que tem sido do maior interesse para a AEPD há mais de 20 anos, e que escrutinamos com muito cuidado. Nas minhas observações iniciais na

conferência da passada quinta-feira, chamei a atenção para exemplos de fenómenos horríveis em termos de tratamento de dados por intervenientes estatais. Conhecemo-los muito bem: utilização de software espião intrusivo, tentativas de quebrar a cifragem, aumento da interoperabilidade em diferentes domínios e funções estatais. A interoperabilidade em si não é o problema, o problema é o que nos faz, reutilizando as informações que não estão no ambiente natural delas.

Mas na Cimeira não discutimos estes perigos, em vez disso, olhámos para a proteção de dados como uma disciplina para ver o quão eficaz é, preocupados com o facto de muitas vezes ser bastante impotente quando se trata de desafios societais emergentes do papel do Estado. Olhámos para a proteção de dados, acreditando também que a compreensão da aplicação da proteção de dados no contexto das autoridades públicas pode servir de porta de entrada para uma reflexão mais ampla sobre a proteção de dados e também de um ponto de vista mais geral.

A proteção de dados deve ser entendida como uma disciplina que vai além do âmbito do RGPD e da sua aplicação direta. Na AEPD, acreditamos que toda a disciplina – apesar dos sucessos extraordinários alcançados até agora, exemplificados pelo RGPD enquanto legislação de referência – pode ir mais longe. Pode ter um impacto mais profundo no funcionamento da democracia.

Como tornar a proteção de dados útil para a democracia? Esta foi a questão central da Cimeira, acompanhada por uma nota de autocrítica: a proteção de dados tende, por vezes, a centrar-se excessivamente em si própria.

Na sua intervenção de abertura, a Vice-Presidente da Comissão Europeia, Vera Jourová, enquadrou a privacidade num contexto mais amplo de questões cruciais que irão dominar cada vez mais o debate público – como a segurança e a economia. Não cabe apenas ao setor da segurança estar atento às preocupações com a privacidade e a proteção de dados; é igualmente essencial que a proteção de dados compreenda o chamado "grande quadro" e decida como pretende envolver-se com esses interesses. Só assim será possível alcançar uma formulação consciente de políticas públicas.

Este apelo a uma maior consciência do contexto interdisciplinar refletiu-se também em intervenções que destacaram percursos específicos dentro desse panorama, demonstrando maior sensibilidade do que outras. Birgit Sippel, deputada ao Parlamento Europeu, apelou às Autoridades de proteção de dados para que assumam uma postura mais política – no sentido de partilhar as suas preocupações pós-eleitorais quanto à direção que a União Europeia poderá seguir no próximo ciclo institucional.

O antigo Relator Especial das Nações Unidas para o Direito à Privacidade – antecessor de Ana Brian, que está hoje aqui connosco – salientou que o simples facto de existirem autoridades não garante, por si só, uma proteção genuína dos Direitos Fundamentais. Alertou para o fosso entre as promessas feitas e as práticas das autoridades públicas, que infelizmente também se verifica na Europa.

O que foi particularmente marcante, contudo, foi a rapidez com que múltiplos fenómenos preocupantes – emergentes de entidades públicas e privadas – foram identificados e associados a propostas de solução que vão além das instituições tradicionais de proteção de dados. O viés algorítmico, os sistemas de recomendação publicitária, entre outros, foram mencionados como exemplos das dificuldades que as leis e autoridades de proteção de dados enfrentam para oferecer respostas significativas.

Ao mesmo tempo, a comunidade alargada da proteção de dados está especialmente bem posicionada para identificar estas práticas ameaçadoras. Isso demonstra que os especialistas, defensores e entusiastas da proteção de dados são capazes de reconhecer os problemas. E, se falharmos em enfrentá-los, não devemos hesitar em considerar métodos alternativos, como legislação específica. No entanto, essas alternativas devem caminhar lado a lado com a proteção de dados, num processo mutuamente informativo – e não como substituição de uma pela outra.

Um exemplo claro desta abordagem foi visível nas discussões da Cimeira sobre a supervisão democrática das autoridades de aplicação da lei e sobre os mecanismos alternativos que lidam com questões de segurança nacional. Essa supervisão tem uma forte componente de proteção de dados, mas é do interesse da própria proteção de dados procurar apoio adicional para garantir mecanismos de controlo e equilíbrio – especialmente em tempos em que a fronteira entre aplicação da lei e segurança nacional se torna cada vez mais difusa.

Para concluir: a proteção de dados precisa de evoluir. Costumo dizer que as Autoridades de proteção de dados também precisam de evoluir. Ou evoluímos, ou tornamo-nos obsoletos. Esta evolução deve ser deliberada e conscientemente orientada. Os próximos anos apenas irão amplificar os desafios e as dificuldades da proteção de dados. Os nossos sucessos ao longo dos últimos vinte, trinta anos em Portugal, terão, gradualmente, menos impacto.

Como já expressou o meu antecessor, Giovanni Buttarelli, no seu manifesto: o RGPD é um padrão de excelência, mas a comunidade europeia de proteção de dados deve preparar-se para a próxima década. Cinco anos após a perda de Giovanni, o seu apelo continua mais relevante do que nunca.

Por isso, mais uma vez, os meus parabéns a Portugal e à Comissão Nacional de Proteção de Dados pelos seus 30 anos de trabalho. Agradeço a cooperação nos programas práticos e espero que possamos dar continuidade às ações que temos vindo a desenvolver até agora.

Wojciech Wiewiórowski
European Data Protection Supervisor

DATA PROTECTION AND DEMOCRACY
REFLECTIONS FROM THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

Mr. Vice-Chair of the Commission for the Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament,

Ms President, dear Paula Meira Lourenço,

Ladies and gentlemen, dear friends.

We are sometimes too fixed or to focused on the dates and the numbers. While 30th anniversary is a wonderful holiday, what actually matters is the maturity, experience and reliability of the Data Protection Authority in Portugal. I have to say that whenever the European Data Protection Supervisor try to think about the allies, that we can start some difficult subject with, Portugal appears as one of the first. A very good example of that was in 2022 when we decided to make the first coordinated action of supervision of the European Public Prosecutors Office and Portugal was the National Data Protection Authority that was the best prepared to perform the supervising role on the national level and to check how the prosecutors were implementing the rules about European Public Prosecutors Office. And it also drives me then directly to thanking the person whose name had already appeared today, Clara Guerra, for the cooperation in this field.

Coincidently, a few days ago the European Data Protection Supervisor was celebrating its 20th anniversary and once again, while for the people of my country of origin, Poland, 2004 was the date of the accessing of the European Union, for us, in the EDPS, it is the date of the birth of our institution.

It was not that long ago. I don´t know if you realize that in the 2004 European Championship in football Cristiano Ronaldo was already present as a player.

So, while technically speaking, we already did turn 20 in January, last week we celebrated it with a special conference titled: "The European Data Protection Summit: Rethinking Data in Democratic Societies". Today I therefore have an opportunity to share with you the ideas from the summit and reflect with you on the roles the privacy and the data protection plays in the democracies. Our host – Paula – asked me to address in my today's presentation the most important aspects of the discussion we had in Brussels last Thursday.

But let me start by explaining what is the role of the European Data Protection Supervisor, which may not be that obvious for all the people here in the room. The European Data Protection Supervisor is the supervisory institution and data protection authority (DPA) for the EU institutions, bodies and agencies. So, we are not supervising the market, but we are supervising the institutions. If you come to Brussels, and you have problems with data protection in the shop or in the hotel, you go to the Belgian Authority. But when you have these problems with the European Parliament, the European Commission, or the Council or any EU agency that exists in Europe, then you go to the European Data Protection Supervisor. So, we have also two islands of our jurisdiction here in Portugal with EMSA (European Maritime Safety Agency) and European Union Drug Agency that will win a new name from July 1st this year. As EDPS we are also the main adviser in the legislative process in the European Union and we are providing the secretariat to the European Data Protection Board which Anu Talus is the Chair of.

As EDPS we have this specific perspective that comes from the specific mandate limited to advising and supervising exclusively public authorities. What this does, if I may for the sake of the argument, consider European Institutions as mirroring the state functions, is therefore very much of interest of EDPS for more than 20 years now, and that is something that we scrutinize carefully. In my opening remarks in the Summit last Thursday I pointed at examples of horrifying phenomena in terms of data processing by the state actors. We very well know them: use of intrusive spyware, attempts to break encryption, increasing interoperability going across different areas and state roles. The interoperability itself is not the problem, the problem is what it makes us, enabling the reuse of data not in the natural environment for them.

But at the Summit we did not discuss these very dangers, instead we turn into data protection as a discipline, to see how effective it is, worried that too often it is rather helpless when it comes to societal challenges emerging from the state role. We turn into data protection believing also that understanding the application of data protection in the context of public authorities can serve as a gateway to broader reflection on data protection and in general.

Data protection should be understood as a discipline that goes beyond the remit of the General Data Protection Regulation (GDPR) and beyond the scope of its direct application. At the EDPS, we believe that the entire discipline — despite the incredible successes achieved so far, exemplified by the GDPR as landmark legislation — can do better. It can have a more profound impact on how democracy functions.

How to make data protection useful for democracy? This was the underlying theme of the Summit, accompanied by a hint of self-criticism: data protection sometimes tends to be only about itself.

In her opening statement, the Vice-President of the European Commission, Vera Jourová, placed privacy in a broader context of crucial issues that will increasingly dominate public debate – such as security and the economy. It is not only up to the security sector to be mindful of privacy and data protection concerns; it is equally important for data protection to understand the so-called "big picture" and decide how it wants to engage with these interests. Only then can conscious policymaking be achieved.

This call for stronger awareness of the interdisciplinary context was also reflected in interventions that pointed to specific tracks within that landscape, showing greater awareness than others. Birgit Sippel, Member of the European Parliament, urged data protection authorities to be more political — in the sense of sharing her post-election concerns about the direction the EU may take in the upcoming institutional cycle.

Prof. Joe Cannataci – the former United Nations Special Rapporteur on the right to privacy – predecessor of Ana Brian, who is with us today – pointed out that simply having authorities in place does not guarantee genuine protection of fundamental rights. He warned that the gap between the promises made and the practices of public authorities is, sadly, also present in Europe.

What was striking, however, was how rapidly multiple worrying phenomena – emerging from both public and private entities – were identified and linked to proposals for solutions that go beyond traditional data protection institutions. Algorithmic bias, advertising recommendation systems, to name a few, were mentioned as examples of the struggles data protection laws and authorities face in providing meaningful answers.

At the same time, the broader data protection community is best placed to identify such threatening data practices. It shows that experts, advocates, and enthusiasts of data protection are able to see the problems. And if we fail to address them, we should not shy away from contemplating alternative methods, such as targeted legislation. However, such alternatives should go hand in hand with data protection, in a process that is mutually informative – rather than replacing one with the other.

An example of this approach was clearly visible in the Summit's discussions on democratic oversight of law enforcement authorities and the supervision of alternative mechanisms dealing with national security matters. Such oversight has a strong data protection component, but it is in the interest of data protection itself to seek support from additional mechanisms to ensure checks and balances – especially in times when the line between law enforcement and national security becomes increasingly blurred.

To conclude: data protection needs to evolve. I often say that data protection authorities also need to evolve. We will either evolve or we will get extinct. Our evolution should be specially and consciously directed. The coming years will only amplify the challenges and the struggles of data protection. While our successes over past, twenty, thirty years in Portugal will gradually means less.

As my predecessor, Giovanni Buttarelli, already expressed in his manifesto: the GDPR is a gold standard, but the EU data protection community must prepare for the next decade. Five years since the loss of Giovanni, his call remains more relevant than ever.

So once again, my congratulations to Portugal, and to the Portuguese DPA for these 30 years of work. I would like to thank you for the cooperation in practical programmes, and I hope we will be able to build on the actions we have undertaken so far.

SESSÃO DA TARDE
AFTERNOON SESSION


CONFERÊNCIA
INTERNACIONAL
INTERNATIONAL
CONFERENCE
24 JUN 2024
PROTEÇÃO DE DADOS PESSOAIS
QUE FUTURO
ESTAMOS
A CONSTRUIR?

Ana Brian Nougrères
Relatora Especial da ONU para o Direito à Privacidade

Ana Brian Nougrères é doutora em Direito e Jurisprudência pela Faculdade de Direito da Universidade da República, Professora de Direito, Privacidade e TIC na Escola de Engenharia (desde 2014) e na Licenciatura em Ciência de Dados para Empresas (desde 2022), da Universidade de Montevidéu. Também leciona Direito, Proteção de Dados e TIC na Faculdade de Direito da Universidade da República (desde 2000) e é membro fundador do Instituto de Direito da Informática da Faculdade de Direito da Universidade da República (2000). Advogada (1986-2024) e consultora jurídica no Parlamento uruguaio (1992-2019). Consultora em proteção de dados com sede em Montevidéu, Uruguai.

Em julho de 2021, o Conselho dos Direitos Humanos das Nações Unidas nomeou a Doutora Brian Nougrères Relatora Especial para o Direito à Privacidade, tendo esta iniciado o seu mandato em 1 de agosto de 2021.

Escreveu mais de uma centena de artigos relacionados com a privacidade e a proteção de dados e a interseção entre tecnologia e direito, incluindo, em 2008, o livro «Data Protection in Uruguay» [Proteção de dados no Uruguai]. Entre 2022 e 2024, a Relatora Especial para o Direito à Privacidade apresentou cinco relatórios temáticos ao Conselho dos Direitos Humanos (CDH) e à Assembleia Geral (AG).

Ana Brian Nougrères is doctor in law and jurisprudence by the School of Law of Universidad de la República, Professor of Law, Privacy and ICT at the School of Engineering (since 2014), and at the Degree in Data Science for Business (since 2022), of Universidad de Montevideo. She also teaches Law, Data Protection and ICT at the School of Law of Universidad de la República (since 2000) and is Founding Member of the Computer Law Institute at the School of Law, Universidad de la República (2000). Practicing Attorney-at-law (1986-2024) and legal advisor at the Uruguayan Parliament (1992-2019). Consultant on data protection based in Montevideo, Uruguay.

In July 2021, the Human Rights Council appointed Dr. Brian Nougrères as the Special Rapporteur on the Right to Privacy and she took up the mandate on 1 August 2021.

She has written more than one hundred papers related to privacy and data protection and the intersection between technology and law, including in 2008 the book on "Data Protection in Uruguay". Between 2022 and 2024 the Special Rapporteur on privacy has presented five thematic reports to the Human Rights Council (HRC) and the General Assembly (GA).

EL USO DE LA TECNOLOGÍA COMO FORMA DE DISCRIMINACIÓN DE GRUPOS MINORITARIOS

¡Muy buenas tardes para todos!

Es un honor para mí estar aquí hoy con ustedes y poder invitarles a la reflexión sobre un tema de gran relevancia para la cohesión y bienestar en la sociedad de la información y del conocimiento.

En primer lugar, me gustaría agradecer a los organizadores por la invitación que me fuera cursada, y también a ustedes todos por su presencia e interés en este tema tan sensible. Vivimos en una era donde la tecnología juega un papel central en casi todos los aspectos de nuestras vidas. Desde la forma en que nos comunicamos, trabajamos y aprendemos, hasta cómo interactuamos socialmente, la tecnología tiene un impacto profundo y omnipresente.

Sin embargo, este poder transformador de la tecnología también conlleva un riesgo significativo: el potencial de reforzar y exacerbar las desigualdades y las discriminaciones existentes.

Es que la tecnología, más aún cuando hablamos de sistemas de inteligencia artificial, nos ofrece ventajas inconmensurables en materias como empleo, sociedad, cultura, y estos sistemas siguen avanzando más aún: leen cuentos para nuestros niños, organizan las comandas en lugares de comida rápida, ayudan a componer videos musicales… Lo que importa es que debemos tener la certeza de que los beneficios son muy mayores comparativamente con los riesgos.

Desde sus albores, la tecnología, en su desarrollo y aplicación, ha tenido un impacto significativo en la vida de las personas. Pero no todas las innovaciones tecnológicas han beneficiado por igual a todos los grupos sociales, sino que hemos visto cómo en algunos casos han sido utilizadas para perpetuar desigualdades y discriminar a grupos minoritarios.

En el siglo XIX, por ejemplo, cuando se introdujeron tecnologías en el ámbito laboral, como la mecanización en fábricas, afectó de manera desproporcionada a los trabajadores de minorías étnicas y a las mujeres, quienes a menudo eran relegados a los trabajos más peligrosos y peor remunerados. Además, las tecnologías de comunicación, como el telégrafo y posteriormente el teléfono, no estuvieron inicialmente al alcance de todos, ampliando la brecha entre los ricos y los pobres.

Con el advenimiento de la era digital, las desigualdades se manifestaron de nuevas formas. Los primeros sistemas informáticos y de automatización, desarrollados en las décadas de 1960 y 1970, reflejaban los sesgos de sus creadores, lo que llevó a la exclusión de minorías raciales y de minorías de género, así como de oportunidades en el ámbito laboral y educativo. A medida que la tecnología ha avanzado, también lo han hecho las posibles formas de discriminación.

En la actualidad, la discriminación tecnológica se manifiesta de diversas formas y afecta a múltiples aspectos de la vida de las personas. La introducción de la inteligencia artificial y de los algoritmos ha exacerbado algunos de estos problemas. Los algoritmos, a menudo considerados imparciales, en realidad reflejan y amplifican los prejuicios presentes en los datos con los que son entrenados. Esto ha llevado a generar situaciones donde personas de minorías étnicas y raciales reciben sentencias judiciales más severas, tienen menos probabilidades de ser contratadas para trabajos y son más propensas a ser vigiladas por la policía.

A su vez, los avances en la tecnología de vigilancia, por ejemplo, han permitido una vigilancia masiva sin precedentes, que a menudo se dirige desproporcionadamente a las comunidades minoritarias. El uso de tecnologías de reconocimiento facial ha sido particularmente problemático, ya que numerosos estudios han demostrado que estas tecnologías tienen mayores tasas de error cuando se trata de identificar a personas de piel oscura, mujeres y jóvenes.

Otro ejemplo contemporáneo es la brecha digital, que sigue siendo un problema significativo. A pesar de los avances en la accesibilidad de la tecnología, muchas comunidades minoritarias, especialmente en áreas rurales y en países en desarrollo, siguen teniendo un acceso limitado a internet y a dispositivos tecnológicos. Esto no solo afecta su capacidad para comunicarse y acceder a información, sino que también limita sus oportunidades educativas y laborales.

En el ámbito de la discapacidad, como ya dijimos, la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad subraya la importancia de garantizar que dichas personas puedan disfrutar de todos los derechos humanos y libertades fundamentales en igualdad de condiciones con los demás.

Aún así, la tecnología a menudo no es accesible para las personas con discapacidades, lo que, sumado a las mencionadas oportunidades educativas y laborales, perpetúa su exclusión social y económica. En lugar de ser una herramienta de inclusión, se convierte en un mecanismo de exclusión en base a una discapacidad.

DE QUÉ FORMA SE PRESENTA LA DISCRIMINACIÓN TECNOLÓGICA?

Una de las formas más insidiosas y menos visibles de discriminación tecnológica hoy en día es, sin dudas, la discriminación algorítmica. Los algoritmos, que son conjuntos de reglas y procedimientos para resolver problemas, están cada vez más integrados en nuestras vidas. Se utilizan en una variedad de aplicaciones, desde la selección de candidatos para empleos hasta la determinación de sentencias en el sistema judicial. Sin embargo, estos algoritmos pueden perpetuar y amplificar los sesgos presentes en los datos con los que son entrenados.

CONSTITUYEN EJEMPLOS DE DISCRIMINACIÓN TECNOLÓGICA:

1. En los casos de reclutamiento y empleo

El sistema de contratación automatizado de Amazon, que fue utilizado entre 2014 y 2017, mostró un sesgo contra las mujeres. El algoritmo penalizaba los currículums que contenían palabras relacionadas con el género femenino, como "capitana" o "equipo femenino". Los algoritmos de contratación también pueden discriminar a candidatos de minorías raciales y étnicas si los datos históricos de contratación reflejan un sesgo hacia ciertos grupos.

2. En los casos de justicia penal

El sistema de evaluación de riesgo COMPAS, utilizado en el sistema judicial de EE.UU., ha demostrado tener un sesgo racial. Los estudios han demostrado que este sistema sobreestima el riesgo de reincidencia de los afroamericanos mientras subestima el de los blancos. Las decisiones basadas en estos algoritmos pueden llevar a sentencias más largas y a condiciones de libertad condicional más estrictas para minorías raciales.

3. En los casos de tecnologías de vigilancia

Que se han desarrollado rápidamente en las últimas décadas, se permite una supervisión sin precedentes de las actividades individuales. Estas tecnologías, aunque a menudo justificadas en nombre de la seguridad pública, tienden a dirigirse desproporcionadamente hacia comunidades minoritarias. Las tecnologías de reconocimiento facial, utilizadas por la policía y otras agencias gubernamentales, han mostrado mayores tasas de error en la identificación de personas de piel oscura, mujeres y jóvenes.

Un estudio del Instituto Nacional de Estándares y Tecnología de EE.UU. encontró que muchos algoritmos tienen tasas de falsos positivos mucho más altas para personas de ciertos grupos raciales y étnicos. Estas tecnologías se utilizan con mayor

frecuencia en barrios y comunidades con alta concentración de minorías, aumentando el riesgo de vigilancia excesiva y detenciones injustas.

4. En los casos de patrullaje de las fuerzas policiales basado en datos

Los sistemas de policía predictiva utilizan datos históricos para identificar áreas de alta criminalidad y dirigir recursos policiales a esas zonas. Sin embargo, si los datos históricos están sesgados, el sistema simplemente perpetúa esos sesgos. Estas prácticas pueden llevar a una vigilancia excesiva en barrios de minorías, exacerbando la desconfianza y las tensiones entre la policía y dichas comunidades.

5. En los casos de discriminación de minorías consecuencia de brecha digital

En efecto, la brecha digital se refiere a las disparidades en el acceso a la tecnología y a internet, que a menudo siguen líneas de clase socioeconómica, geografía, etaria y de raza. Esta brecha tiene implicaciones significativas para la participación en la vida moderna. En muchas áreas rurales e indígenas, el acceso a internet de alta velocidad sigue siendo limitado o inexistente. Lo anterior impide que estas comunidades participen plenamente en la economía digital, accedan a servicios de educación y salud en línea, y se beneficien de las oportunidades de conectividad.

Aún más, a pesar de los avances en la tecnología accesible, muchas personas con discapacidades enfrentan todavía barreras significativas para acceder a la tecnología. Esto incluye software que no es compatible con tecnologías de asistencia, como lectores de pantalla, y dispositivos físicos que no están diseñados teniendo en cuenta la accesibilidad.

En cuanto a derechos de primera línea, como es el caso de la educación, la falta de acceso a la tecnología puede limitar las oportunidades educativas para estudiantes de comunidades desfavorecidas. Durante la pandemia de COVID-19, esta brecha se hizo aún más evidente, ya que muchos estudiantes no podían participar en el aprendizaje en línea.

La brecha digital también afecta las oportunidades laborales, ya que muchas ofertas de empleo y recursos para la búsqueda de trabajo están disponibles principalmente en línea. Las personas sin acceso adecuado a internet están en desventaja competitiva.

EN QUÉ GRUPOS ESPECÍFICOS SE PRODUCE EL IMPACTO?

Son varios los grupos minoritarios que pueden verse afectados por el mal uso de las herramientas tecnológicas tan características del siglo XXI. La discriminación tecnológica tiene un impacto significativo y a menudo desproporcionado en las comunidades étnicas y raciales. Las tecnologías, que incluyen algoritmos de inteligencia artificial y sistemas de vigilancia, reflejan los prejuicios de la sociedad en la que se desarrollan.

Las minorías religiosas también enfrentan formas específicas de discriminación tecnológica, que afectan su capacidad para practicar su fe libremente y participar plenamente en la sociedad. En varios países, la vigilancia y el perfilado se han centrado desproporcionadamente en las comunidades musulmanas. Los programas de vigilancia masiva justifican estas prácticas en nombre de la seguridad nacional, pero resultan en la violación de derechos fundamentales y la estigmatización de estas comunidades. A su vez, las minorías religiosas son a menudo blanco de discursos de odio y acoso en línea. Lamentablemente, las plataformas sociales no siempre responden de manera efectiva para moderar este contenido, lo que contribuye a un entorno hostil para estas comunidades.

La tecnología también afecta de manera desproporcionada a las comunidades LGBT y a las mujeres, perpetuando estereotipos de género y contribuyendo a la discriminación. Las mujeres y las personas LGBTQ+ enfrentan sesgos en los algoritmos de contratación. Los algoritmos que analizan currículums y perfiles de candidatos a menudo penalizan características asociadas con

estos grupos. Las tecnologías de vigilancia pueden ser utilizadas para rastrear y acosar a personas LGBTQ+, especialmente en regiones donde la homosexualidad es criminalizada o estigmatizada.

Las mujeres a menudo son blanco de acoso en línea y de seguimiento no consentido utilizando tecnologías de geolocalización y redes sociales. Además, las mujeres en muchas partes del mundo tienen menos acceso a la educación tecnológica y a recursos en línea, limitando sus oportunidades de desarrollo profesional y empoderamiento económico.

En cuanto a personas con discapacidades, las mismas enfrentan barreras significativas en el acceso y uso de tecnologías, lo que limita su participación plena en la sociedad. Las personas con discapacidades a menudo tienen menos acceso a internet y a dispositivos tecnológicos adecuados, lo que restringe su capacidad para acceder a servicios en línea, educación y oportunidades laborales. Los algoritmos, utilizados en procesos de selección de empleo y educación pueden discriminar implícitamente contra personas con discapacidades, al no considerar adecuadamente sus capacidades y necesidades específicas.

CUÁLES SON LAS REPERCUSIONES DE ESTOS FENÓMENOS? CUÁLES SON SUS CONSECUENCIAS?

Las consecuencias sociales y psicológicas de la discriminación tecnológica son profundas y multifacéticas.

Las personas de grupos minoritarios que enfrentan discriminación tecnológica pueden experimentar una variedad de efectos negativos que impactan en su bienestar y calidad de vida.

1. Pueden sufrir de aislamento social

- Exclusión digital: la falta de acceso a tecnologías modernas y a internet puede resultar en un aislamiento social significativo. Las personas sin acceso adecuado no pueden participar plenamente en las interacciones sociales en línea, lo que puede llevar a sentimientos de aislamiento y exclusión.
- Estigma y marginación: la vigilancia excesiva y el perfilado algorítmico pueden estigmatizar a ciertos grupos, aumentando la desconfianza y marginación dentro de la sociedad.

2. Impacto en la Salud Mental

- Ansiedad y estrés: las personas que son objeto de discriminación algorítmica y vigilancia constante pueden experimentar altos niveles de ansiedad y estrés. La sensación de ser constantemente monitoreado puede tener efectos perjudiciales en la salud mental.
- Baja autoestima: la discriminación en plataformas digitales y el acoso en línea pueden erosionar la autoestima de las personas afectadas, particularmente en comunidades vulnerables como la LGBTQ+ y las personas con discapacidades.

Asimismo, la discriminación tecnológica puede tener repercusiones económicas negativas significativas, en tanto afecta el empleo, en especial oportunidades de acceso al trabajo, de desarrollo profesional, promociones laborales, limitando el crecimiento profesional por consecuencia de sesgos en las evaluaciones algorítmicas de desempeño.

3. Desigualdad en el Empleo:

- Acceso al Trabajo: Los algoritmos sesgados en los procesos de contratación pueden impedir que las personas de grupos minoritarios accedan a oportunidades laborales equitativas. Esto perpetúa la desigualdad económica y limita el crecimiento profesional.

- Promociones y Desarrollo Profesional: Incluso cuando las personas de grupos minoritarios logran obtener empleo, pueden enfrentar barreras en el desarrollo profesional y promociones debido a sesgos en las evaluaciones de desempeño algorítmicas.

A su vez, temas relacionados con brecha digital, como la falta de acceso a internet de alta velocidad y a tecnologías modernas, puede limitar las oportunidades de acceder a recursos financieros, préstamos, servicios bancarios en línea, exacerbando la desigualdad económica. También, si pensamos en emprendedores de comunidades minoritarias, podemos apreciar que muchas veces enfrentan barreras adicionales al intentar establecer sus negocios, o hacerles crecer, debido a la falta de acceso a tecnología y a plataformas de comercio digital.

Son igualmente perjudiciales las consecuencias legales y políticas derivadas del mal uso de la tecnología, que plantean desafíos significativos para la protección de los derechos humanos y la promoción de la justicia social.

La discriminación tecnológica también se relaciona con la protección de datos y la privacidad.

Por un lado, la vigilancia masiva y el uso de tecnologías de reconocimiento facial nos muestran a comunidades minoritarias como las más afectadas por estas prácticas invasivas, que afectan los derechos humanos. La falta de marcos regulatorios robustos para abordar la discriminación algorítmica y la privacidad de los datos deja a muchas personas vulnerables a abusos y violaciones de sus derechos, en tanto no siempre las víctimas de discriminación tecnológíca poseen los conocimientos ni los recursos necesarios para procurar la justicia por los medios legales. De ahí que decimos que es necesario mejorar el acceso a la asistencia legal y a la educación en derechos digitales.

La opacidad en el funcionamiento de los algoritmos de inteligencia artificial dificulta la identificación y la corrección de los sesgos. De ahí la trascendencia de implementar políticas que exijan transparencia y rendición de cuentas en el uso de tecnologías algorítmicas.

CUÁLES SON LAS SOLUCIONES POSIBLES?

Para mitigar la discriminación tecnológica, exhortamos a que la tecnología sea diseñada y desarrollada con la inclusión y la equidad en mente desde el diseño.

Exhortamos a las EMPRESAS TECNOLÓGICAS a esforzarse por crear equipos diversos e inclusivos, en tanto la diversidad en el personal de desarrollo ayuda a identificar y corregir sesgos que podrían pasar desapercibidos en equipos homogéneos. A su vez, la implementación de programas de capacitación en sesgos inconscientes para desarrolladores y diseñadores también ayuda a reducir la introducción de prejuicios en los algoritmos y en los sistemas tecnológicos. Exhortamos asimismo a adoptar principios de diseño universal que consideren las necesidades de todas las personas, incluidas aquellas con discapacidades. De esta manera, se procura garantizar que los productos tecnológicos sean accesibles para usuarios con diferentes capacidades.

Seguir normas y directrices internacionales, (como las Pautas de Accesibilidad al Contenido en la Web, que son pautas de una organización internacional que adoptan varios países como España y Argentina), puede ayudarnos a asegurar que las tecnologías sean accesibles y utilizables por todos.

Por otra parte, la opacidad en el funcionamiento de los algoritmos puede perpetuar la discriminación. Por ello, exhortamos a implementar prácticas de transparencia y rendición de cuentas, así como realizar auditorías independientes de los algoritmos para identificar y corregir sesgos. Estas auditorías deben ser realizadas por terceros imparciales y expertos en la materia. No basta con auditar los algoritmos una vez: las evaluaciones deben ser continuas para asegurar que los sistemas sigan siendo justos y equitativos a medida que evolucionan. Se deben desarrollar algoritmos que sean explicables, que puedan proporcionar explicaciones comprensibles de cómo se toman las decisiones.

Esto es crucial para asegurar la rendición de cuentas y la confianza de las personas. Se deben publicar los informes sobre el uso de algoritmos y los resultados de las auditorías como una forma de promover la transparencia y permitir la supervisión pública.

Los GOBIERNOS, así como los ORGANISMOS REGULADORES tienen un papel crucial en la promoción de la equidad tecnológica a través de políticas y regulaciones efectivas. Exhortamos, para el bienestar de la sociedad, que se establezcan y refuercen leyes que prohíban la discriminación algorítmica y tecnológica. Estas leyes deben incluir sanciones claras para las violaciones y mecanismos de aplicación robustos.

Exhortamos, a su vez, promover y proteger los derechos digitales de los ciudadanos, asegurando que todos tengan acceso equitativo a la tecnología y una robusta protección contra abusos. Es vital también implementar programas e iniciativas que permitan cerrar la brecha digital. Esto incluye proporcionar acceso a internet de alta velocidad en áreas rurales y comunidades desfavorecidas, y ofrecer formación en competencias digitales.

A su vez, la SOCIEDAD CIVIL tiene un papel crucial en la promoción de la equidad tecnológica y en la lucha contra la discriminación. Es necesario apoyar a organizaciones que aboguen por los derechos de los grupos minoritarios y que trabajen para prevenir la discriminación tecnológica. Estas organizaciones pueden proporcionar recursos, educación y apoyo legal a las personas afectadas.

Exhortamos a fomentar la colaboración multistakeholder, entre las organizaciones de la sociedad civil, los estados, la comunidad técnica, la academia y las empresas tecnológicas para desarrollar soluciones inclusivas y equitativas. A su vez, muchas veces la implementación de campañas de sensibilización para educar a las personas sobre los riesgos de la discriminación tecnológica y la importancia de la equidad digital brindan resultados muy positivos.

Ofrecer formación en derechos digitales a comunidades minoritarias y a grupos vulnerables para empoderarlos a defender sus derechos y utilizar la tecnología de manera segura y efectiva, también es recomendable. A su vez, las empresas tecnológicas y otras organizaciones pueden liderar el camino adoptando buenas prácticas e innovaciones que promuevan la equidad.

Otra forma es desarrollando y compartiendo kits de herramientas y recursos que ayuden a las empresas a evaluar y mitigar el sesgo en sus tecnologías. Estos recursos pueden incluir guías de mejores prácticas, software de auditoría y plantillas de políticas. La creación de redes y consorcios de innovación inclusiva donde las empresas puedan compartir conocimientos es otra buena iniciativa para colaborar en el desarrollo de tecnologías equitativas.

Establecer programas de mentoría y de capacitación que apoyen a grupos subrepresentados en el sector tecnológico puede ayudar a promover una mayor diversidad en la fuerza laboral, así como también realizar evaluaciones de impacto social para todos y cada uno de los nuevos desarrollos tecnológicos, asegurando que se consideren los efectos potenciales en todos los grupos sociales.

Abordar la discriminación tecnológica requiere un enfoque multifacético que incluya diseño inclusivo, transparencia algorítmica, políticas públicas robustas, participación de todas las partes involucradas en el desarrollo tecnológico y de la red. Implementar estas soluciones y prácticas puede ayudar a crear una sociedad más equitativa y justa, donde la tecnología sirva como un catalizador para la inclusión y el empoderamiento, en lugar de perpetuar las desigualdades existentes.

CONCLUSIÓN

A modo de conclusión, hemos explorado la profunda y multifacética intersección entre la tecnología y la discriminación de grupos minoritarios. Hemos examinado cómo la tecnología, aunque prometedora en su potencial para mejorar vidas y aumentar la eficiencia, puede también perpetuar y amplificar las desigualdades existentes. Desde la discriminación algorítmica hasta la vigilancia dirigida, y desde la brecha digital hasta la inaccesibilidad tecnológica, las repercusiones son vastas y significativas.

Es crucial reafirmar los principios fundamentales de derechos humanos y dignidad que deben guiar el desarrollo y uso de tecnologías. La Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad, en tal sentido, subraya la importancia de la inclusión, la accesibilidad y la no discriminación, principios que deben ser aplicados universalmente en el contexto tecnológico.

Es imperativo realizar un llamado a la acción.

A los gobiernos a efectos de formular y aplicar políticas que promuevan la equidad y la inclusión en el ámbito tecnológico, así como implementar programas que cierren la brecha digital, proporcionando acceso equitativo a internet y tecnología para todos, especialmente en comunidades desfavorecidas.

A las empresas tecnológicas a efectos de adoptar principios éticos en el diseño y en el desarrollo de sus productos, así como de ser transparentes en cómo operan sus algoritmos y sistemas de datos, permitiendo evaluaciones independientes y publicando resultados de auditorías para mantener la confianza del público.

A las organizaciones de la sociedad civil, a efectos de continuar su labor de defensa y activismo, trabajando para proteger los derechos de los grupos minoritarios y presionando por políticas y prácticas más equitativas en el uso de la tecnología. Es crucial educar a las personas sobre los riesgos y repercusiones de la discriminación tecnológica, así como sobre sus derechos digitales, empoderandolas para que puedan defenderse de manera efectiva.

La lucha contra la discriminación tecnológica y la promoción de la equidad es un desafío global que requiere una colaboración transnacional. La ONU y otras organizaciones internacionales tienen un papel crucial en facilitar el diálogo, compartir mejores prácticas y coordinar esfuerzos globales. La tecnología tiene el potencial de transformar nuestras vidas de manera positiva, pero solo si se desarrolla y utiliza con un firme compromiso con la equidad y la justicia. Debemos trabajar juntos para asegurar que la tecnología beneficie a todos, sin importar su origen étnico, género, religión, discapacidad u orientación sexual.

Sólo a través de un esfuerzo colectivo y sostenido, podemos construir un futuro donde la tecnología sea una herramienta de inclusión y empoderamiento, promoviendo así una sociedad más justa y equitativa para todos.

¡Muchas gracias!

Ana Brian Nougrères
UN Special Rapporteur on the Right to Privacy OHCHR

THE USE OF TECHNOLOGIES AS A WAY OF DISCRIMINATION

Good afternoon to everyone!

I am honoured to be here with you today and be able to invite you to reflect on a topic of great relevance for cohesion and well-being in the information and knowledge society.

First of all, I would like to thank the organisers for your invitation, and also to thank you for your presence and interest in this sensitive topic. We live in an era where technology plays a central role in almost every aspect of our lives. From the way we communicate, work and learn, to how we interact socially, technology has a profound and ubiquitous impact.

However, this transformative power of technology also carries a significant risk: the potential to strengthen and exacerbate existing inequalities and discrimination.

Technology, even more so when we talk about artificial intelligence systems, offers us immeasurable benefits in areas such as employment, society, culture, and these systems are making further progress: read stories for our children, organise orders in fast food places, help compose music videos... What matters is that we must be sure that the benefits are much higher compared to the risks.

Since its inception, technology, in its development and application, has had a significant impact on people's lives. But not all technological innovations have benefited all social groups equally, but we have seen how in some cases they have been used to perpetuate inequalities and discriminate against minority groups.

In the 19th century, for example, when technologies were introduced in the workplace, such as mechanisation in factories, it disproportionately affected ethnic minority workers and women, who were often relegated to the most dangerous and low-paid jobs. In addition, communication technologies, such as telegraph and later the phone, were initially not available to everyone, widening the gap between the rich and the poor.

With the advent of the digital age, inequalities manifested themselves in new ways. The first IT and automation systems, developed in the 1960s and 1970s, reflected the biases of their creators, leading to the exclusion of racial and gender minorities, as well as opportunities in the field of work and education. As technology has progressed, this has also been done by possible forms of discrimination.

Technological discrimination now manifests itself in various forms and affects multiple aspects of people's lives. The introduction of artificial intelligence and algorithms has exacerbated some of these problems. Algorithms, often considered to be impartial, actually reflect and amplify the prejudices present in the data with which they are trained. This has led to situations where people from ethnic and racial minorities receive more severe court rulings, are less likely to be recruited for work and are more likely to be monitored by the police.

In turn, advances in surveillance technology, for example, have enabled unprecedented mass surveillance, which often targets minority communities disproportionately. The use of facial recognition technologies has been particularly problematic, as many studies have shown that these technologies have higher error rates when it comes to identifying people with dark skin, women and young people.

Another contemporary example is the digital divide, which remains a significant problem. Despite advances in technology accessibility, many minority communities, especially in rural areas and developing countries, still have limited access to the Internet and technological devices. This not only affects their ability to communicate and access information, but also limits their educational and employment opportunities.

In the area of disability, as we have already said, the UN Convention on the Rights of Persons with Disabilities underlines the importance of ensuring that persons with disabilities can enjoy all human rights and fundamental freedoms on an equal basis with others.

Still, technology is often not accessible to people with disabilities, which, in addition to the above mentioned educational and employment opportunities, perpetuates their social and economic exclusion. Instead of being an inclusion tool, it becomes a disability-based exclusion mechanism.

HOW IS TECHNOLOGICAL DISCRIMINATION PRESENTED?

One of the most insidious and less visible forms of technological discrimination today is undoubtedly algorithmic discrimination. Algorithms, which are sets of rules and procedures to solve problems, are increasingly integrated into our lives. They are used in a variety of applications, from the selection of candidates for jobs to the determination of judgements in the judicial system. However, these algorithms can perpetuate and amplify the biases present in the data with which they are trained.

EXAMPLES OF TECHNOLOGICAL DISCRIMINATION ARE:

1. In the case of recruitment and employment

Amazon's automated recruitment system, which was used between 2014 and 2017, showed a bias against women. The algorithm penalised CVs containing words related to the female gender, such as 'captain' or 'female team'. Recruitment algorithms may also discriminate against candidates from racial and ethnic minorities if historical recruitment data reflect a bias towards certain groups.

2. In criminal justice cases

The COMPAS risk assessment system, used in the US judicial system, has proven to have a racial bias. Studies have shown that this system overestimates the risk of reoffending by Afro-American while underestimating that of whites. Decisions based on these algorithms can lead to longer sentences and stricter conditions of conditional release for racial minorities.

3. In the case of surveillance technologies

Which have developed rapidly in recent decades, unprecedented monitoring of individual activities is allowed. These technologies, although often justified in the name of public safety, tend to target disproportionately minority communities. Facial recognition technologies, used by police and other government agencies, have shown higher error rates in identifying dark skin people, women and young people.

A study by the US National Institute of Standards and Technology found that many algorithms have much higher false positive rates for people from certain racial and ethnic groups. These technologies are more frequently used in neighbourhoods and communities with a high concentration of minorities, increasing the risk of excessive surveillance and unfair arrests.

4. In cases of data-driven patrols of police forces

Predictive police systems use historical data to identify areas of high crime and direct police resources to these areas. However, if historical data are biased, the system simply perpetuates those biases. These practices can lead to excessive surveillance in neighbourhoods of minorities, exacerbating mistrust and tensions between police and minority communities.

5. In cases of discrimination against minorities as a result of the digital divide

Indeed, the digital divide refers to disparities in access to technology and the Internet, which often follow socio-economic, geography, ethnicity and race lines. This gap has significant implications for participation in modern life. In many rural and indigenous areas, access to high-speed Internet remains limited or non-existent. This prevents these communities from fully participating in the digital economy, from accessing education and e-health services, and from benefiting from connectivity opportunities.

Moreover, despite advances in accessible technology, many people with disabilities still face significant barriers to access technology. This includes software that is not compatible with assistive technologies, such as screen readers, and physical devices that are not designed with accessibility in mind.

In terms of frontline rights, such as education, lack of access to technology can limit educational opportunities for students from disadvantaged communities. During the COVID-19 pandemic, this gap became even more evident, as many students were unable to participate in e-learning.

The digital divide also affects job opportunities, as many job offers and job-search resources are mostly available online. People without adequate Internet access are at a competitive disadvantage.

IN WHICH SPECIFIC GROUPS THE IMPACT OCCURS?

Several minority groups may be affected by the misuse of technological tools so characteristic of the 21st century. Technological discrimination has a significant and often disproportionate impact on ethnic and racial communities. Technologies, including artificial intelligence algorithms and surveillance systems, reflect the prejudices of the society in which they are developed.

Religious minorities also face specific forms of technological discrimination, which affect their ability to practise their faith freely and participate fully in society. In several countries, surveillance and profiling have disproportionately focused on Muslim communities. Mass surveillance programmes justify these practices in the name of national security, but result in the violation of fundamental rights and stigmatisation of these communities. In turn, religious minorities are often targets of hate speech and harassment online. Unfortunately, social platforms do not always respond effectively to moderate this content, which contributes to a hostile environment for these communities.

Technology also disproportionately affects LGBT communities and women, perpetuating gender stereotypes and contributing to discrimination. Women and LGBTQ + people face bias in recruitment algorithms. Algorithms analysing CVs and candidate profiles often penalise characteristics associated with these groups. Surveillance technologies can be used to track and harass LGBTQ + people, especially in regions where homosexuality is criminalised or stigmatised.

Women are often targets of online harassment and non-consensual tracking using geolocation technologies and social media. In addition, women in many parts of the world have less access to technological education and online resources, limiting their opportunities for professional development and economic empowerment.

For people with disabilities, they face significant barriers in accessing and using technologies, limiting their full participation in society. People with disabilities often have less access to the Internet and appropriate technological devices, restricting their ability to access online services, education and job opportunities. Algorithms, used in job selection and education processes, may implicitly discriminate against persons with disabilities by not properly considering their specific skills and needs.

WHAT ARE THE IMPACTS OF THESE PHENOMENA? WHAT ARE THE CONSEQUENCES?

The social and psychological consequences of technological discrimination are profound and multifaceted.

People from minority groups facing technological discrimination may experience a variety of negative effects impacting their well-being and quality of life.

1. They may suffer from social isolation

- Digital exclusion: lack of access to modern technologies and the Internet can result in significant social isolation. People without adequate access cannot fully participate in online social interactions, which can lead to feelings of isolation and exclusion.
- Stigma and margination: excessive surveillance and algorithmic profiling can stigmatise certain groups, increasing mistrust and marginalisation within society.

2. Impact on mental health

- Anxiety and stress: people subject to algorithmic discrimination and constant surveillance may experience high levels of anxiety and stress. The feeling of being constantly monitored can have detrimental effects on mental health.
- Low self-esteem: discrimination on digital platforms and online harassment can erode the self-esteem of affected people, particularly in vulnerable communities such as LGBTQ + and people with disabilities.

Technological discrimination can also have significant negative economic impacts, as it affects employment, including opportunities for access to work, career development, job promotions, limiting professional growth as a result of bias in algorithmic performance assessments.

3. Inequality in employment:

- Access to work: biased algorithms in recruitment processes can prevent people from minority groups from accessing fair job opportunities. This perpetuates economic inequality and limits professional growth.
- Promotions and career development: even when people from minority groups succeed in obtaining employment, they may face barriers in career development and promotions due to bias in algorithmic performance assessments.

In turn, topics related to the digital divide, such as the lack of access to high-speed Internet and modern technologies, can limit opportunities to access financial resources, loans, online banking services, exacerbating economic inequality. Also, if we think of entrepreneurs from minority communities, we can see that they often face additional barriers when trying to establish or grow their business due to a lack of access to technology and digital trading platforms.

The legal and political consequences of the misuse of technology, which pose significant challenges to the protection of human rights and the promotion of social justice, are equally detrimental.

Technological discrimination also relates to data protection and privacy.

On the one hand, mass surveillance and the use of facial recognition technologies show us minority communities such as those most affected by these invasive practices, which affect human rights. The lack of robust regulatory frameworks to address algorithmic discrimination and data privacy leaves many people vulnerable to abuse and violations of their rights, as long as victims of technological discrimination do not always have the knowledge and resources to seek justice through legal means. This is why we say that better access to legal care and education on digital rights is needed.

Opacity in the functioning of AI algorithms makes it difficult to identify and correct bias. Hence the importance of implementing policies that require transparency and accountability in the use of algorithmic technologies.

WHAT ARE THE POSSIBLE SOLUTIONS?

To mitigate technological discrimination, we call for technology to be designed and developed with inclusiveness and fairness by design.

We urge TECHNOLOGY COMPANIES to strive to create diverse and inclusive teams, while diversity in development staff helps to identify and correct biases that could go unnoticed in homogeneous teams. In turn, the implementation of unconscious bias training programmes for developers and designers also helps to reduce the introduction of prejudices in algorithms and technology systems. We also urge the adoption of universally designed principles that consider the needs of all people, including those with disabilities. In this way, efforts are made to ensure that technological products are accessible to users with different capabilities.

Following international standards and guidelines (such as the Web Content Accessibility Guidelines, which are guidelines of an international organisation adopted by several countries such as Spain and Argentina), can help us to ensure that technologies are accessible and usable by all.

Moreover, opacity in the functioning of algorithms can perpetuate discrimination. We therefore call for transparency and accountability practices, as well as independent audits of algorithms to identify and correct biases. These audits should be carried out by impartial third parties and experts in the field. It is not enough to audit algorithms once: evaluations should be continuous to ensure that systems remain fair and equitable as they evolve. Algorithms should be developed that are explicable, which can provide understandable explanations of how decisions are made.

This is crucial to ensure people's accountability and trust. Reports on the use of algorithms and audit results should be published as a way to promote transparency and enable public oversight.

The GOVERNMENTS, as well as the REGULATORY BODIES, have a crucial role to play in promoting technological fairness through effective policies and regulations.

We call, for the well-being of society, for the establishment and strengthening of laws prohibiting algorithmic and technological discrimination. These laws should include clear sanctions for violations and robust enforcement mechanisms.

We urge, in turn, to promote and protect citizens' digital rights, ensuring that everyone has equal access to technology and robust protection against abuse. It is also vital to implement programmes and initiatives to close the digital divide. This includes providing access to high-speed Internet in rural areas and disadvantaged communities, and providing training in digital skills.

In turn, CIVIL SOCIETY has a crucial role to play in promoting technological fairness and fighting discrimination. There is a need to support organisations advocating the rights of minority groups and working to prevent technological discrimination. These organisations can provide resources, education and legal support to those affected.

We encourage multi-stakeholder collaboration between civil society organisations, states, the technical community, academia and technology companies to develop inclusive and equitable solutions. In turn, the implementation of awareness-raising campaigns to educate people about the risks of technological discrimination and the importance of digital fairness often yield very positive results.

Providing training on digital rights to minority communities and vulnerable groups to empower them to defend their rights and use technology safely and effectively is also recommended. In turn, technology companies and other organisations can lead the way by adopting good practices and innovations that promote equity.

Another way is to develop and share toolkits and resources to help companies assess and mitigate bias in their technologies. These resources may include best practice guides, audit software and policy templates. Creating networks and inclusive innovation consortia where companies can share knowledge is another good initiative to collaborate in the development of equitable technologies.

Establishing mentoring and capacity building programmes that support under-represented groups in the technology sector can help promote greater diversity in the workforce, as well as carrying out social impact assessments for each and every new technological development, ensuring that potential effects on all social groups are considered.

Addressing technological discrimination requires a multi-faceted approach that includes inclusive design, algorithmic transparency, robust public policies, involvement of all parties involved in technological and network development. Implementing these solutions and practices can help create a fair society, where technology serves as a catalyst for inclusion and empowerment, rather than perpetuating existing inequalities.

CONCLUSION

In conclusion, we have explored the deep and multifaceted intersection between technology and discrimination against minority groups. We have examined how technology, while promising in its potential to improve lives and increase efficiency, can also perpetuate and amplify existing inequalities. From algorithmic discrimination to targeted surveillance, and from the digital divide to technological inaccessibility, the impacts are vast and significant.

It is crucial to reaffirm the fundamental principles of human rights and dignity that should guide the development and use of technologies. The UN Convention on the Rights of Persons with Disabilities, in this regard, underlines the importance of inclusiveness, accessibility and non-discrimination, principles that should be universally applied in the technological context.

It is imperative to make a call to action.

Governments should formulate and implement policies that promote fairness and inclusion in technology, as well as implement programmes that close the digital divide, providing equal access to the Internet and technology for all, especially in disadvantaged communities.

Technology companies should adopt ethical principles in the design and development of their products, as well as be transparent in how their algorithms and data systems operate, enabling independent assessments and publishing audit results to maintain public trust.

Civil society organisations should, for the purpose of continuing their advocacy and activism work, work to protect the rights of minority groups and press for more equitable policies and practices in the use of technology. Educating people on the risks and impacts of technological discrimination, as well as on their digital rights, is crucial to empower them to defend themselves effectively.

Combating technological discrimination and promoting equity is a global challenge that requires transnational collaboration. The UN and other international organisations have a crucial role to play in facilitating dialogue, sharing best practices and coordinating global efforts. Technology has the potential to transform our lives positively, but only if it is developed and used with a strong commitment to fairness and justice. We must work together to ensure that technology benefits everyone, regardless of their ethnic origin, gender, religion, disability or sexual orientation.

Only through a collective and sustained effort can we build a future where technology is a tool for inclusion and empowerment, thus promoting a more just and equitable society for all.

Thank you very much!

Josefina Román Vergara

Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) do México, que detém a Presidência da Rede Ibero-Americana de Proteção de Dados

Román Vergara é atualmente Comissária do INAI para o período 2019-2026.

Em 2013, foi nomeada Comissária do Instituto para a Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais do Estado do México e dos seus Municípios, onde um ano depois foi eleita Comissária Presidente, cargo que ocupou até 2017.

De novembro de 2015 a novembro de 2016, foi a primeira Coordenadora do Sistema de Órgãos de Supervisão das Entidades Federativas do Sistema Nacional de Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais. Em 2018, foi Secretária Técnica da Secretaria Executiva do Sistema Anticorrupção do Estado do México e seus Municípios.

É licenciada em Direito pela Faculdade de Direito da Universidade do Estado do México, Mestre em Direito das Sociedades pela Faculdade de Direito da Universidad Anahuac e Doutorada em Direito pelo Centro de Pós-Graduação em Direito.

Ms. Román Vergara is currently a Commissioner of INAI for the 2019 – 2026 period.

In 2013, she was appointed Commissioner of the Institute of Transparency, Access to Public Information and Protection of Personal Data of the State of Mexico and its Municipalities, where a year later, she was elected as the President Commissioner, a position she held until 2017. From November 2015 to November 2016, she was the first Coordinator of the System of Supervisory Bodies of the Federative Entities of the National System of Transparency, Access to Public Information and Protection of Personal Data. In 2018, she was the Technical Secretary of the Executive Secretariat of the Anticorruption System of the State of Mexico and its Municipalities.

She holds a Law Degree from the Universidad del Estado de México's Law School, an LLM in Corporate Law from Universidad Anahuac Law School and a Ph.D in Law from the Centre for Postgraduate Studies in Law.

EL FORTALECIMIENTO DE LA PROTECCIÓN DE DATOS EN EL CONTEXTO DIGITAL: LOS ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS

Muy buen día, tengan todas y todos, celebro y agradezco la oportunidad de dirigirme ante ustedes en este espacio a nombre de las Comisionadas y el Comisionado Presidente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de México, autoridad que actualmente preside la Red Iberoamericana de Protección de Datos.

Asimismo, aprovecho este espacio para saludar a las personalidades y expertos que nos acompañan este día, para abordar la importancia del fortalecimiento de la protección de datos en el contexto digital, tema que ha ocupado la agenda tanto de las autoridades que nos encargamos de velar por este derecho, como de otras autoridades regulatorias en cada uno de nuestros países, así como de terceros interesados como grupos de la sociedad civil organizada, organismos internacionales y, por supuesto, representantes del sector privado.

Antes de iniciar con mi intervención también quiero saludar a las expertas y expertos que me acompañan en esta sesión y que son las voces que nos invitarán a reflexionar sobre uno de los documentos referentes de la protección de datos en la región iberoamericana que todos conocemos y son los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

En primer lugar, permítanme expresar mi más sincero agradecimiento por esta invitación a participar en esta sesión a los organizadores y anfitriones de este evento. Para el INAI, participar en el desarrollo y promoción de estas actividades es de suma importancia, somos autoridades nacionales de protección de datos personales, por lo que difundir y fortalecer la garantía de estos derechos fundamentales es una de nuestras atribuciones.

Tenemos una misión y visión clara, ya sea de manera individual o compartida en el espacio que conformamos como Red, por lo que está por demás señalar que estamos comprometidos con proteger la privacidad y los datos personales no solo de nuestros ciudadanos sino de toda la población que forma parte de Iberoamérica.

El día de hoy me toca abordar uno de los grandes logros que se han concretado en el marco de la Red Iberoamericana de Protección de Datos y me refiero, por supuesto, a los Estándares de Protección de Datos para los Estados Iberoamericanos, instrumento con el que podemos afirmar que por primera vez en la región contamos con una base normativa común para la protección de datos.

En 2017, las autoridades que conformamos la Red Iberoamericana de Protección de Datos, en el marco del XV Encuentro Iberoamericano aprobamos estos Estándares, dando cumplimiento así a un objetivo largamente anhelado por todas las entidades que integran esta Red.

Los antecedentes inmediatos para la aprobación de estos Estándares datan de 2016 como parte de uno de los acuerdos adoptados en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, relacionado con solicitar a esta Red la elaboración de una propuesta para la cooperación efectiva relacionada con la protección de datos personales y privacidad.

No podemos olvidar que también uno de los principales impulsores de estos Estándares se remonta hacia 2007 con ocasión del V Encuentro de la Red, en donde se adoptaron las Directrices para la "Armonización de la Protección de Datos en la Comunidad Iberoamericana". Primer instrumento con el que se pretendía establecer un "marco armonizado" de referencia para las legislaciones que surgieran en la región.

Por otro lado, también se tomaron en cuenta los llamados "Estándares de Madrid" de 2009, que fueron aprobados mediante resolución derivada de la entonces Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, hoy mejor conocida como Asamblea Global de Privacidad.

Asimismo, el impulsó final que se dio para la aprobación de este texto, vino acompañado de uno de los ejes de la estrategia acordada por la Red en noviembre de 2016, plasmada en el documento "RIPD 2020", consistente en "impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetro para futuras regulaciones o para la revisión de las existentes".

Por lo que los Estándares Iberoamericanos se constituyeron como un conjunto de directrices orientadoras para contribuir a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no contaban con estos ordenamientos, o en su caso, para ser un instrumento referente en la modernización y actualización de sus legislaciones vigentes.

Quiero retomar la referencia original a los objetivos que están plasmados en estos Estándares Iberoamericanos y que destaco a continuación:

- Uno. Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.
- Dos. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.
- Tres. Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.
- Cuatro. Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia.

A siete años de la aprobación de los Estándares, y luego de ver que ya la mayoría de los países que integran la región Iberoamericana cuentan con legislaciones vigentes en materia de protección de datos personales y privacidad, e incluso que algunas de estas nuevas legislaciones ya contienen elementos de los instrumentos internacionales de referencia como el Reglamento General de Protección de Datos Personales de la Unión Europea, es necesario que volvamos a replantearnos los alcances que enmarcamos en este instrumento, ya que la innovación tecnológica no cesa y en los últimos años nos hemos enfrentado a una avalancha de nuevas tecnologías y sistemas de inteligencia artificial que representan un nuevo desafío para las autoridades de protección de datos.

Si bien en su origen los Estándares se caracterizaban por:

- Responder a las necesidades y exigencias nacionales e internacionales, en una sociedad donde las tecnologías cobran mayor relevancia.
- Incluir las mejores prácticas nacionales e internacionales.
- Proponer una serie de estándares tan flexibles que faciliten su adopción entre los Estados Iberoamericanos, sin contravenir de ninguna manera su derecho interno, con la finalidad de ser un documento de viable adopción en la región.
- Garantizar un nivel adecuado de protección de los datos personales y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas.
- Y finalmente, y no menos importante, reforzar la posición de la Red en el ámbito internacional.

Estoy convencida hoy más que nunca requerimos estándares más fuertes que nos permitan reforzar las atribuciones de las autoridades de protección de datos, ante el tratamiento masivo de datos personales, en medio de una coyuntura donde el mundo está hiperconectado y los flujos de datos, principalmente en el sector económico, vayan más allá de nuestras fronteras.

Por lo anterior, debemos comenzar a plantearnos como Red el posible trazo de diversas estrategias que nos permitan llegar a consensos que contemplen los desafíos que plantean estas nuevas tecnologías, y enriquezcamos las bases normativas de nuestras legislaciones con las mejores prácticas internacionales que obedezcan al contexto actual que estamos viviendo.

Para lograr ese objetivo, sin duda nos enfrentamos a diversas barreras ya que si bien es cierto que son muchos los países que cuentan con regulación es inevitable que existan diferencias en cuanto a la prioridad y aplicación de estas normas en cada país, pues no debe perderse de vista que cada jurisdicción cuenta con particularidades específicas que debe mantener, sobre todo porque en muchos lugares, como en México, la privacidad y la protección de datos personales son considerados como derechos fundamentales; no obstante, existen países donde este tipo de derechos van encaminados más a la protección del consumidor, desde una óptica comercial.

Para ello y retomando uno de los objetivos que están enmarcados dentro de estos Estándares, destaco la importancia de establecer una base mínima para la cooperación internacional entre las autoridades de protección de datos de la región, con la finalidad de favorecer y facilitar la aplicación de la legislación en la materia y garantizar una protección efectiva de los titulares.

La cooperación interinstitucional, nacional o internacional, es una herramienta indispensable para el intercambio de conocimientos, experiencias y herramientas en diversos aspectos vinculados con la protección de datos personales, a través de esta vía podemos impulsar la adopción de nuevos principios y estándares que vayan en línea con los riesgos ya identificados y asociados a la conexión digital en la que nos desenvolvemos.

En los últimos años hemos sido testigos de considerables esfuerzos en diversas regiones del mundo, respecto al desarrollo de mecanismos de cooperación internacional y asistencia mutua para facilitar la aplicación efectiva de los diferentes marcos regulatorios para la protección de datos personales y con ello coadyuvar a la interoperabilidad entre los mismos.

Ante este escenario, los Estándares exponen de manera clara la importancia de la cooperación internacional entre las autoridades miembro y establecen en su décimo capítulo el establecimiento de mecanismos de cooperación internacional, señalando que:

Los Estados Iberoamericanos podrán adoptar mecanismos de cooperación internacional que faciliten la aplicación de las legislaciones nacionales aplicables en la materia, los cuales podrán comprender, de manera enunciativa más no limitativa:

a. El establecimiento de mecanismos que permitan reforzar la asistencia y cooperación internacional en la aplicación de las respectivas legislaciones nacionales en la materia.
b. La asistencia entre las autoridades de control a través de la notificación y remisión de reclamaciones, la asistencia en investigaciones y el intercambio de información.
c. La adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

El INAI, al presidir la Red Iberoamericana de Protección de Datos, ha sido testigo del interés de las autoridades miembros por abarcar nuevos temas que son razón de preocupación y en conjunto con el Comité Ejecutivo hemos generado acciones necesarias para articular y avanzar en la creación de estándares comunes, difusión de estrategias y buenas prácticas en favor del derecho a la protección de datos personales tal como la reciente Guía de "Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales".

Esta Guía, así como otros trabajos desarrollados desde el seno de la Red, han tenido su fundamento en los apartados y artículos que forman parte de los Estándares, denotando la necesidad de contar con reglas homogéneas para facilitar el flujo de datos y con ello obtener beneficios económicos y a su vez que den certeza y garantía del tratamiento de datos personales, ya sea entre los propios países de la Red, como terceros que realicen transferencia de datos personales a esta región.

Asimismo, en 2023, las autoridades que integramos la Red, iniciamos una labor de supervisión y coordinación conjunta por primera vez, sobre el servicio de inteligencia artificial ChatGPT, ya que se advirtió que éste podía conllevar riesgos para los derechos y libertades de los usuarios en relación con el tratamiento de sus datos personales, inclusive en el mes de abril, se instalaron mesas de trabajo en las que se abordó el estado actual de investigaciones iniciadas a propósito de la actividad de empresas desarrolladoras de inteligencia artificial y su incidencia sobre los datos personales, resaltando la importancia de la IA para el desarrollo económico y social, sin dejar de reconocer el fuerte impacto que su uso no regulado puede tener para los derechos y libertades de los ciudadanos y en concreto para el derecho fundamental a la protección de sus datos personales. Abogamos por una regulación equilibrada que fomente la necesaria innovación y desarrollo de esta tecnología y al tiempo proteja los derechos de protección de datos y los aspectos éticos asociados.

Por otro lado, también hemos destacado la vulnerabilidad de los menores en el mundo digital, ya que se encuentran sujetos a numerosos riesgos por el uso temprano y su sobreexposición, lo que les puede provocar, entre otros, adicciones, acceso a contenido inapropiado, perfilado de su comportamiento desde la niñez, así como trastornos cerebrales y de sueño, problemas de psicomotricidad, de alimentación, autolesiones, ansiedad, suicidios, acoso sexual (grooming), etc.

Un tema de creciente relevancia son las neurotecnologías en tanto que advertimos un impacto potencial en la privacidad y la protección de datos personales de sus usuarios. Destacamos la importancia de los neuroderechos para proteger la privacidad y la autonomía frente a la manipulación y comercialización de datos cerebrales, abogando por la necesidad de regular el uso de los neurodatos para salvaguardar la privacidad mental individual, integrando esta regulación con la de protección de datos y con otras áreas normativas, de forma que se promueva una mayor transparencia en su tratamiento.

La exposición de datos personales e información en la era digital ha conllevado una creciente preocupación por el cumplimiento y garantía de los derechos de protección de datos personales y privacidad. Más que nadie, las autoridades de protección de datos personales somos testigos del valor que representa garantizar estos derechos, como activos en la sociedad actual y del riesgo que implica para su titular.

Mantener resguardados los datos y proteger la privacidad es una preocupación constante, por lo que es necesario que se pueda garantizar el cumplimiento de nuestras normativas a fin de garantizar un tratamiento ético y legal y enfrentar los riesgos sobre la privacidad y datos personales que se presenten.

No quiero concluir esta intervención sin reafirmar, como lo he venido señalando, que nos encontramos en un contexto ideal para que como Red y como región, establezcamos nuevos objetivos que vayan en sintonía con las innovaciones tecnológicas, no se trata de restringir o prohibir el desarrollo y uso de nuevas tecnologías, sino más bien de garantizar que haya un respeto a los derechos fundamentales de los titulares de los datos personales.

Por lo que me congratula compartir con ustedes que, en mayo durante el Encuentro de la Red, celebrado en Cartagena, Colombia, las autoridades hemos dado los primeros pasos hacia la actualización de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

Esta actualización viene de la mano con el trabajo que se ha empezado a desarrollar en los grupos de trabajo de la Red y tiene como objetivo centrarse, como ya he mencionado, en el fortalecimiento del derecho a la protección de datos personales ante el uso sistemas de inteligencia artificial y las neurotecnologías; fomentar la protección de menores en ecosistemas digitales y por último, pero no menos relevante, es imperativo robustecer el marco normativo y dotar de mayores atribuciones y recursos a las autoridades de protección de datos personales para que puedan, de manera eficiente, dar atención oportuna al ejercicio de estos derechos.

A medida que la tecnología avanza, debemos asegurarnos de que la privacidad y la protección de datos sigan siendo una prioridad en nuestros esfuerzos legislativos y regulatorios.

Agradezco su atención y su compromiso con la protección de datos personales. Espero que estas ideas sirvan como base para futuras discusiones y acciones concretas en nuestros países. Juntos, podemos enfrentar los desafíos del futuro y asegurar un entorno seguro y respetuoso de la privacidad para todos.

Josefina Román Vergara
Commissioner of Mexico's National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), which holds the presidency of the Ibero-American Data Protection Network

THE STRENGTHENING DATA PROTECTION IN THE DIGITAL CONTEXT
THE STANDARDS FOR PERSONAL DATA PROTECTION FOR IBERO-AMERICAN STATES

Good morning, everyone. I am delighted and grateful for the opportunity to address you here on behalf of the Commissioners and the President of Mexico's National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), the Authority that currently chairs the Ibero-American Data Protection Network.

I would also like to take this opportunity to welcome the distinguished guests and experts who are with us today to discuss the importance of strengthening data protection in the digital context, an issue that has been on the agenda of both the authorities responsible for safeguarding this right and other regulatory authorities in each of our countries, as well as interested third parties such as organised civil society groups, international organisations and, of course, representatives of the private sector.

Before beginning my presentation, I would also like to welcome the experts who are joining me in this session and who will invite us to reflect on one of the reference documents on data protection in the Ibero-American region that we are all familiar with: the Personal Data Protection Standards for Ibero-American States.

First of all, let me express my sincere thanks for this invitation to take part in this session to the organisers and hosts of this event. For INAI, being involved in the development and promotion of these activities is of the utmost importance, we are national personal data protection authorities, so disseminating and strengthening the guarantee of these fundamental rights is one of our powers.

We have a clear mission and vision, either individually or shared in the space we form as a Network, so we are committed to protecting the privacy and personal data not only of our citizens but of the entire population that is part of Ibero-America.

Today, I have to address one of the great achievements that have been made in the framework of the Ibero-American Data Protection Network and, of course, I refer to the Data Protection Standards for Ibero-American States, an instrument with which we can say that for the first time in the region we have a common legal basis for data protection.

In 2017, the authorities forming the Ibero-American Data Protection Network, in the framework of the fifteenth Ibero-American meeting, approved these standards, thus fulfilling a long standing objective of all the entities making up this network.

The immediate background for the approval of these standards dates back to 2016 as part of one of the agreements adopted at the XXV Ibero-American Summit of Heads of State and Government, relating to requesting this Network to draw up a proposal for effective cooperation related to the protection of personal data and privacy.

It should not be forgotten that one of the main drivers of these standards also dates back to 2007 at the Fifth Network Meeting, at which the Guidelines for 'Harmonisation of Data Protection in the Ibero-American Community' were adopted.

On the other hand, account was also taken of the so-called "Madrid Standard" of 2009, which were approved by a resolution stemming from the then International Conference of Data Protection and Privacy Authorities, which is now better known as the Global Privacy Assembly.

The final impetus given to the adoption of this text was also accompanied by one of the axes of the strategy agreed by the Network in November 2016, set out in the document 'RIPD 2020', which consists of 'encouraging and contributing to the strengthening and adaptation of regulatory processes in the region, by drawing up guidelines to serve as a parameter for future regulations or for the revision of existing regulations'.

The Ibero-American standards were therefore established as a set of guiding guidelines to help issue regulatory initiatives for the protection of personal data in the Ibero-American region of those countries that did not yet have these laws, or, where appropriate, to be a reference instrument for modernising and updating their existing legislation.

I would like to reiterate the original reference to the objectives set out in these Ibero-American standards and which I would like to highlight below:

- One. Establish a set of common principles and rights for the protection of personal data that the Ibero-American States can adopt and develop in their national legislation, with the aim of having uniform rules in the region.
- Two. Ensure the effective exercise and protection of the right to the protection of personal data of any natural person in the Ibero-American States by establishing common rules to ensure the proper processing of their personal data.
- Three. Facilitate the flow of personal data between the Ibero-American States and beyond, with the aim of contributing to the economic and social growth of the region.
- Four. Encourage international cooperation between the supervisory authorities of Ibero-American States, with other non-regional supervisory authorities and international authorities and bodies in this area.

Seven years after the adoption of the Standards, and now that most of the countries that integrate the Ibero-American region already have legislation in force on the protection of personal data and privacy, and even that some of these new laws already contain elements of international reference instruments such as the General Data Protection Regulation of the European Union, we need to rethink the scope of this instrument, as technological innovation is continuing and in recent years we have faced an avalanche of new technologies and artificial intelligence systems that represent a new challenge for data protection authorities.

Standards were originally characterised by:

- Responding to national and international needs and requirements, in a society where technologies are most relevant.
- Include national and international best practices.
- Propose such flexible standards as to facilitate their adoption among Ibero-American States, without in any way infringing their domestic law, with the aim of being a viable document for adoption in the region.
- Ensure an adequate level of protection of personal data and thus promote commercial activities between the region as well as with other economic regions.
- And last but not least, to strengthen the Network's position at international level.

I am convinced more than ever that we need stronger standards to enable us to strengthen the powers of data protection authorities, given the massive processing of personal data, amid a situation where the world is hyperconnected and data flows, mainly in the economic sector, go beyond our borders.

In view of the above, we must begin to consider as a Network the possible outline of various strategies that will enable us to reach consensus on the challenges posed by these new technologies, and we enrich the regulatory bases of our legislation with the best international practices that reflect the current context we are experiencing.

In order to achieve this objective, we certainly face various barriers, since although many countries have regulation, it is inevitable that there are differences in the priority and application of these rules in each country, since it should not be forgotten that each jurisdiction has specific features that it must maintain, not least because in many places, such as Mexico, privacy and the protection of personal data are regarded as fundamental rights; however, there are countries where such rights are more aimed at protecting consumers, from a commercial point of view.

To this end, I would like to stress the importance of establishing a minimum basis for international cooperation between the data protection authorities of the region, with the aim of promoting and facilitating the implementation of the relevant legislation and ensuring effective protection of data subjects.

Interinstitutional cooperation, whether national or international, is an indispensable tool for exchanging knowledge, experience and tools in various aspects related to the protection of personal data, through this route we can encourage the adoption of new principles and standards that are in line with the risks already identified and associated with the digital connection in which we operate.

In recent years, we have witnessed considerable efforts in various regions of the world to develop international cooperation and mutual assistance mechanisms to facilitate the effective implementation of the different regulatory frameworks for the protection of personal data and thereby contribute to the interoperability between them.

Against this backdrop, the standards clearly set out the importance of international cooperation between the member authorities and set out in their tenth chapter the establishment of international cooperation mechanisms, noting that:

The Ibero-American States may adopt international cooperation mechanisms to facilitate the application of the applicable national laws, which may include, but are not limited to:

a. The establishment of mechanisms to strengthen international assistance and cooperation in the implementation of the respective national laws in this area.
b. Assistance between supervisory authorities through notification and referral of complaints, assistance in investigations and exchange of information.

c. The adoption of mechanisms aimed at knowledge and exchange of best practices and experiences on the protection of personal data, including on conflicts of jurisdiction with third countries.

In chairing the Ibero-American Data Protection Network, INAI has witnessed the interest of the member authorities in covering new issues of concern and together with the Executive Committee we have generated necessary actions to articulate and advance the creation of common standards, dissemination of strategies and good practices in favour of the right to the protection of personal data, such as the recent Guide to "Model Contractual Clauses for the International Transfer of Personal Data".

This Guide, as well as other work carried out from within the Network, has been based on the paragraphs and articles that form part of the Standards, stressing the need for uniform rules to facilitate the flow of data and thus to obtain economic benefits and, in turn, to provide certainty and guarantee the processing of personal data, either between the Network's own countries and third parties transferring personal data to this region.

In addition, in 2023, the authorities involved in the Network launched joint monitoring and coordination work for the first time on the artificial intelligence service ChatGPT, as it was noted that it could pose risks to the rights and freedoms of users in relation to the processing of their personal data. Including in April, working tables were set up to discuss the current state of investigations initiated in relation to the activity of companies developing artificial intelligence and its impact on personal data, underlining the importance of AI for economic and social development, while recognising the strong impact that its unregulated use can have on citizens' rights and freedoms and in particular on the fundamental right to the protection of their personal data. We call for a balanced regulation that fosters the necessary innovation and development of this technology while protecting data protection rights and associated ethical aspects.

On the other hand, we have also highlighted the vulnerability of minors in the digital world, as they are subject to many risks due to early use and overexposure, which can lead to, among other things, addiction, access to inappropriate content, profiling of their behaviour from childhood, as well as brain and sleep disorders, psychomotor problems, eating disorders, self-harm, anxiety, suicide, grooming, etc.

A topic of growing relevance is neurotechnologies as we warn of a potential impact on the privacy and protection of personal data of their users. We stress the importance of neurorights to protect privacy and autonomy from the manipulation and commercialisation of brain data, advocating the need to regulate the use of neurodata to safeguard individual mental privacy, integrating this regulation with data protection and other regulatory areas, so as to promote greater transparency in their processing.

The exposure of personal data and information in the digital age has led to growing concerns about the enforcement and enforcement of personal data protection and privacy rights. Rather than anyone, the personal data protection authorities witness the value of guaranteeing these rights, as assets in today's society and the risk it entails for the data subject.

Keeping data secure and protecting privacy is a constant concern and it is therefore necessary that compliance with our regulations can be ensured in order to ensure ethical and legal processing and to address the risks to privacy and personal data presented.

I do not want to conclude this intervention without reaffirming, as I have pointed out, that we are in the ideal context for the Network and as a region to set new objectives that are in line with technological innovations, not to restrict or prohibit the development and use of new technologies, but rather to ensure that the fundamental rights of the data subjects are respected.

I am therefore pleased to share with you that during the Network Meeting in Cartagena, Colombia, in May, the authorities took the first steps towards updating the Personal Data Protection Standards for Ibero-American States.

This update goes hand in hand with the work that has started to be developed in the Network's working groups and aims to focus, as I have already mentioned, on strengthening the right to protection of personal data from the use of artificial intelligence systems and neurotechnologies; promoting the protection of minors in digital ecosystems, and last but not least, it is imperative to strengthen the regulatory framework and provide more powers and resources to personal data protection authorities so that they can, in an efficient manner, give timely attention to the exercise of these rights.

As technology progresses, we need to make sure that privacy and data protection remain a priority in our legislative and regulatory efforts.

Thank you for your attention and commitment to the protection of personal data. I hope these ideas will serve as a basis for future discussions and concrete actions in our countries. Together, we can face the challenges of the future and ensure a safe and privacy-friendly environment for all.

Bruno Martins
Investigador e Professor Associado do Instituto Superior Técnico da Universidade de Lisboa

Bruno Martins é Professor Associado do Instituto Superior Técnico da Universidade de Lisboa, investigador do Laboratório de Tecnologias da Linguagem Humana do INESC-ID, e membro da Unidade ELLIS em Lisboa (LUMLIS). O seu trabalho de investigação foca-se em problemas relacionados com as áreas de recuperação de informação, análise de texto, e ciências da informação geográfica. Destaca-se no seu trabalho o envolvimento em vários projetos de investigação relacionados com aspetos geo-espaciais no acesso e recuperação de informação, tendo ele acumulado uma experiência significativa na abordagem de problemas que intersetam a recuperação de informação, o processamento de linguagem natural, e a aprendizagem automática.

Bruno Martins is an Associate Professor at Instituto Superior Técnico of the University of Lisbon, a researcher at the Human Language Technologies Lab of INESC-ID, and a member of the Lisbon ELLIS Unit (LUMLIS). He works on problems related to the general areas of information retrieval, text mining, and the geographical information sciences. Bruno has specifically been involved in several research projects related to geospatial aspects in information access and retrieval, and he has accumulated a significant expertise in addressing challenges at the intersection of information retrieval, natural language processing, and machine learning.

PROTEÇÃO DE DADOS PESSOAIS NA ERA DA INTELIGÊNCIA ARTIFICIAL GENERATIVA

A minha intervenção hoje vai abordar o que no meu entender é um dos tópicos mais fascinantes e transformadores da era atual, nomeadamente a inteligência artificial generativa e os modelos de linguagem de grande escala ("large language models" – LLM), como o ChatGPT. É indiscutível que a inteligência artificial tem avançado a passos muito largos, impactando diversas áreas do conhecimento e diversos sectores da economia. Em particular, temos assistido à disponibilização de ferramentas que se destacam pela sua capacidade de criar conteúdos novos e originais (reforço aqui a palavra original, pois é algo que vou voltar a abordar na minha intervenção) a partir de dados preexistentes, imitando padrões humanos de linguagem e criação, por forma a gerar textos, imagens e vídeos, música, ou mesmo código de software, ampliando o horizonte do que consideramos possível.

A minha intervenção vai-se focar em três aspetos principais relacionados com os modelos de linguagem de grande escala, pois muito embora existam outros exemplos e aplicações, penso que seja esta a tecnologia atualmente com maior impacto. Em primeiro lugar, vou tentar explicar um pouco do que está na base desta tecnologia. De seguida, procurarei discutir o que são atualmente as principais potencialidades e limitações. Finalmente, darei alguns exemplos do impacto destas ferramentas especificamente no que se relaciona com a temática da proteção de dados. O meu objetivo com esta palestra é informar, pois acredito que algum conhecimento sobre o funcionamento destas ferramentas (em particular das suas limitações) é essencial para a sua boa utilização, e espero que uma melhor compreensão possa também ajudar no vislumbrar de novas oportunidades de utilização, ao mesmo tempo suportando uma reflexão sobre o impacto destas tecnologias na sociedade.

Em primeiro lugar, penso que seja importante referir que muito embora estejamos a assistir nos últimos anos a avanços muito rápidos, estas tecnologias não surgiram de um "vazio" e na realidade constroem sobre muitas décadas de trabalho em diferentes subáreas da inteligência artificial. Coisas como o aumento significativo da quantidade de informação disponível de forma digital, associado à crescente utilização da Web, ou o aumento da capacidade de computação associado a melhorias contínuas no hardware, fizeram com que se tornasse possível revisitar algumas ideias já com bastantes anos, agora com uma escala muito maior.

Em particular, na base dos modelos GPT (a sigla na realidade significa Generative Pre-Training) está uma ideia muito simples, relacionada com modelos probabilísticos para entender e prever padrões em linguagem natural, introduzidos por Claude Shannon nos anos 50, que consiste em prever qual a continuação mais adequada, ou seja, prever qual a próxima palavra, num determinado texto. O que estes modelos fazem na realidade resume-se a isto: dada uma representação para uma determinada sequência de palavras, correspondente a um exemplo de um texto, prever qual a probabilidade da palavra seguinte ser uma determinada entrada do dicionário. Por si só é uma ideia muito simples, mas quando associada ao conceito de "grande escala" é incrivelmente poderosa. Grande escala aqui significa que o modelo que estima estas probabilidades tem uma grande capacidade, envolvendo muitos parâmetros, e por outro lado significa também que a quantidade de exemplos de texto, usada para aprender a distribuição de probabilidade, é enorme e corresponde essencialmente a uma porção muito significativa de toda a informação publicada na Web.

Seguindo esta receita, torna-se possível desenvolver sistemas que, muito embora não tenham um "entendimento" profundo do significado da linguagem humana, geram continuações plausíveis, tal como expressas em documentos reais. A capacidade de criar estas imitações é já por si muito útil e interessante, mas os sistemas mais modernos (dos quais o ChatGPT é um exemplo) introduzem ainda uma melhoria sobre esta ideia, por forma a melhor aproximar os resultados produzidos de um diálogo natural entre pessoas, envolvendo instruções e a geração de respostas a essas instruções. Quando exposto a uma pergunta, por exemplo, um sistema treinado apenas para prever continuações possíveis com base em textos da Internet vai provavelmente responder com uma outra pergunta no mesmo tópico, em lugar da resposta. Assim, por forma a melhor alinhar os sistemas com as expectativas dos utilizadores humanos, o modelo pré-treinado com os dados da Web é exposto a exemplos de instruções em linguagem natural, e é ajustado por forma a gerar continuações para essas instruções que correspondam a respostas adequadas e preferidas por humanos. Além do significado "Generative Pre-Training", a sigla GPT

é também associada ao conceito de "General Purpose Technology", e a ideia de alinhar os resultados dos modelos de acordo com preferências de humanos é o que permite estas capacidades, ao mesmo tempo procurando evitar a geração de conteúdos que façam uso de uma linguagem ofensiva ou discriminatória, tal como existe na Internet.

De uma forma muito resumida, focando no conceptual e sem entrar nos muitos detalhes de engenharia que são fundamentais para o desenvolvimento de sistemas de grande escala, é esta a forma como funcionam os modelos de linguagem como o ChatGPT. Os resultados são verdadeiramente surpreendentes, e são muitas as tarefas que estes sistemas conseguem automatizar com uma proficiência incrível. Tarefas relacionadas com a produção de texto plausível, com base noutra informação textual fornecida como entrada, são ótimos candidatos a automatização com estas ferramentas. Exemplos são por exemplo: (a) expandir para um artigo desde um conjunto de pontos principais, ou condensar informação numa lista de pontos principais; (b) responder a perguntas com base num dado texto; ou (c) reescrever um texto de acordo com um determinado estilo.

A questão da originalidade dos textos produzidos penso que seja particularmente difícil de aferir, e se por um lado existe a opinião de que estes sistemas são pouco mais do que "papagaios estocásticos" que se limitam a repetir, de forma ligeiramente diferente, informação que já existe na Internet, por outro lado também é verdade que estes sistemas geram realmente novos textos diferentes, por vezes misturando conceitos de uma forma que se pode considerar como original. É muito difícil compreender realmente estes sistemas, e diria até que na realidade sabemos muito pouco sobre eles. Esta afirmação é um pouco estranha, pois tratam-se de sistemas desenhados e construídos por humanos, cuja engenharia é perfeitamente conhecida. Sabemos quais os componentes, sabemos individualmente quais os cálculos que são efetuados em cada um dos módulos que compõem estes sistemas. No entanto, a escala destes sistemas (ou seja, os vários biliões de parâmetros envolvidos, e os dados de treino à escala de toda a Internet) levam a que as interações entre os componentes gerem resultados difíceis de prever, sendo que o estudo destes sistemas se assemelha ao que acontece noutras áreas do conhecimento como a física ou a biologia, em que os objetos de estudo são muito complexos.

Se é verdade que os resultados são verdadeiramente surpreendentes, também existem ainda muitas limitações na utilização destes sistemas. Eles produzem geralmente texto fluido e gramaticalmente correto, correspondente a continuações muito plausíveis para as entradas, com conteúdo que parece certo, mas que pode estar errado. Isto deve-se ao facto de os sistemas serem treinados com informação limitada (e.g., dados da Web, ou seja, multilingues, mas principalmente em Inglês, e por vezes contendo informação enviesada ou mesmo factualmente errada), particularmente no que se refere a tópicos mais específicos ou eventos recentes. Devido à forma como estes sistemas funcionam, os mesmos são muito limitados na verificação de factos, na execução de raciocínio lógico, ou realização de cálculos. Por vezes as respostas apresentadas por estes sistemas chegam a apresentar citações e ligações para conteúdos que não existem. Não podemos dizer definitivamente o que estes modelos "sabem e o que não sabem", e não sabemos quando estes modelos expressam com confiança afirmações que estão incorretas.

Temos visto (e continuaremos a ver nos próximos anos) um progresso muito rápido e melhorias contínuas nestes sistemas. Algumas das limitações que acabei de referir serão provavelmente ultrapassadas nas próximas versões destes sistemas (por exemplo através da combinação destes sistemas com outros, como por exemplo calculadoras para expandir a capacidade de execução de cálculos, ou motores de busca como forma de aceder a informação mais atualizada), mas dificilmente o problema será completamente resolvido e é assim necessário espírito crítico na utilização destes sistemas. Diria que um dos desafios que se coloca com a crescente utilização destes sistemas passará por treinar as pessoas no uso adequado destas ferramentas.

No contexto particular do ensino, a introdução destas tecnologias tem sido particularmente transformadora, com aspetos positivos e negativos. Acho que esta é uma área concreta de aplicação que ilustra bem o desafio, potencialidades e problemas introduzidos pelo uso destas ferramentas. É inegável que a utilização de sistemas como o ChatGPT pode ser muito útil aos estudantes e docentes, funcionando como uma espécie de "tutores" sempre disponíveis, que podem ajudar a resumir informação, ou gerar perguntas que ajudam a verificar as aprendizagens. No entanto, existe o problema da integridade académica, em particular a preocupação de que os estudantes possam usar ferramentas como o ChatGPT sem o conhecimento dos professores, entregando relatórios gerados automaticamente como se fossem textos da sua autoria. Este é um problema de difícil (talvez até impossível) resolução, dado que as ferramentas atuais para deteção de texto gerado automaticamente não

funcionam, e dificilmente existirão ferramentas que oferecem garantias de deteção correta. No mundo académico penso que existe um consenso alargado sobre a importância da consciência ética da utilização destas ferramentas, por oposição a proibição, sendo que os docentes e as instituições devem procurar ter uma política clara sobre a utilização destas ferramentas, indicando em que casos a sua utilização é (ou não é) aceitável.

Sistemas como o ChatGPT trazem também várias preocupações no contexto da proteção de dados pessoais, alguns semelhantes ao que acontece com outros serviços disponíveis na Web, e outras talvez um pouco mais diferentes e particulares. Existem por exemplo preocupações relacionadas com a recolha e o armazenamento dos dados que suportam o treino destes sistemas, quer sejam dados disponibilizados na Web quer sejam as interações com o sistema, que podem ser armazenadas para fins de melhoria. Estes dados podem incluir informações pessoais, e já existe um enquadramento regulatório que indica o que estes sistemas podem ou não fazer. Para poderem operar, estes sistemas devem estar em conformidade com regulamentações de proteção de dados existentes, e são garantidos aspetos como o direito dos utilizadores à portabilidade dos seus dados, o direito ao esquecimento e à transparência sobre como seus dados são usados, o direito ao consentimento explicito e informado para que os dados sejam utilizados. No entanto, a escala a que estes sistemas operam coloca muitas dificuldades no garantir que a informação da Web que é usada para o treino destes modelos esteja realmente em conformidade com as obrigações que acabei de descrever, ou que esteja isenta de conteúdos ofensivos ou vieses. Este é um desafio essencialmente técnico, que irá requerer ainda muito trabalho na área.

Um outro aspeto particularmente relevante, relacionado com a proteção de dados pessoais, passa pelo uso destes sistemas para a realização de ataques de "phishing" e de engenharia social. Sistemas como o ChatGPT podem ser usados de forma muito eficaz para imitar o indivíduo e assim criar mensagens de phishing muito convincentes, facilitando ataques de engenharia social que visam roubar informações pessoais. Este é mais do que um desafio técnico, sendo que é difícil antecipar qual o impacto societal que a crescente utilização dos sistemas para estes fins virá a ter. Se por um lado importa adequar os mecanismos regulatórios e de combate à atividade criminosa, por forma a lidar com estes casos, estou convencido que será pela via da sensibilização e educação das pessoas, pelo reforço da ética no ensino (por exemplo, no ensino da engenharia e no treino dos profissionais que desenvolvem estas ferramentas) que poderemos ter um maior impacto.

Para terminar, queria deixar-vos a mensagem de que devemos não antecipar o futuro, mas sim considerar a situação presente onde o uso de ferramentas de Inteligência Artificial como ChatGPT é comum e omnipresente. É esta a realidade atual, sendo que é importante termos cidadãos informados sobre as potencialidades e limitações destas ferramentas.

Bruno Martins
Researcher and Associate Professor at the Instituto Superior Técnico of the University of Lisbon

PERSONAL DATA PROTECTION IN THE ERA OF GENERATIVE ARTIFICIAL INTELLIGENCE

My intervention today will address what in my view is one of the most fascinating and transformative topics of the current era, namely generative artificial intelligence and large-scale language models such as ChatGPT. There is no doubt that artificial intelligence has progressed very widely, impacting various areas of knowledge and various sectors of the economy. In particular, we have seen the availability of tools that stand out for their ability to create new and original content (reinforcing here the "original" word, as it is something I will discuss again in my intervention) from pre-existing data, imitating human patterns of language and creation, in order to generate texts, images and videos, music, or even software code, extending the horizon of what we consider possible.

My intervention will focus on three main aspects related to large-scale language models, as while there are other examples and applications, I think this technology is the most impactful today. First, I will try to explain a little of what underpins this technology. I will then try to discuss what are currently the main potentials and limitations. Finally, I will give some examples of the impact of these tools specifically on data protection issues. My aim with this lecture is to inform you, as I believe that some knowledge about the functioning of these tools (in particular their limitations) is essential for their good use, and I hope that a better understanding can also help to see new opportunities for use, while supporting a reflection on the impact of these technologies on society.

First, I think it is important to note that while we are witnessing very rapid advancements in recent years, these technologies have not emerged from a "vacuum" and they actually build on many decades of work in different sub-areas of artificial intelligence. Things such as the significant increase in the amount of information available digitally, coupled with the increasing use of the

web, or the increase in computing capacity associated with continuous hardware improvements, have made it possible to revisit some long-standing ideas, now on a much larger scale.

In particular, on the basis of the GPT models (the acronym in reality means Generative Pre-Training) is a very simple idea, linked to probabilistic models for understanding and predicting natural language patterns, introduced by Claude Shannon in the 50s, which is to predict the most appropriate continuation, i.e. to predict what next word in a given text. What these models actually do can be summarised as follows: given a representation for a particular sequence of words, corresponding to an example of a text, predict the probability of the next word being a given dictionary entry. It is in itself a very simple idea, but when linked to the concept of 'large scale' it is undeniably powerful. Large scale here means that the model that estimates these probabilities has a high capacity, involving many parameters, and also means that the amount of text examples used to learn the probability distribution is huge and essentially corresponds to a very significant portion of all information published on the web.

Following this recipe, it is possible to develop systems which, although they do not have a deep "understanding" of the meaning of human language, generate plausible continuations, as expressed in actual documents. The ability to create these imitations is already very useful and interesting, but more modern systems (of which ChatGPT is an example) still introduce an improvement on this idea, so as to bring the results produced closer to a natural dialogue between people, involving instructions and the generation of responses to such instructions. When exposed to a question, for example, a system trained only to predict possible continuations based on internet texts is likely to answer another question on the same topic instead of the answer. Thus, in order to better align systems with human users' expectations, the pre-trained model with web data is exposed to examples of instructions in natural language, and is adjusted to generate continuations for such instructions that correspond to appropriate and human-preferred responses. In addition to the meaning 'Generative Pre-Training', the acronym GPT is also associated with the concept of General Purpose Technology, and the idea of aligning the results of models according to human preferences is what enables these capabilities, while seeking to avoid the generation of content that uses offensive or discriminatory language, as it exists on the Internet.

In a very summarised way, focusing on conceptual and without entering into the many engineering details that are fundamental to the development of large-scale systems, this is how language models such as ChatGPT work. The results are truly surprising, and there are many tasks that these systems can automate with an incredible proficiency. Tasks related to the production of plausible text, based on other textual information provided as input, are excellent candidates for automation with these tools. Examples include: (a) expand to an article from a number of main points, or condense information into a list of main points; (b) answer questions on the basis of a given text; or (c) rewrite a text according to a particular style.

The question of the originality of the texts produced seems to me to be particularly difficult to assess, and whether, on the one hand, there is the view that these systems are slightly more than 'stochastic parrots' which merely repeat, in a slightly different manner, information which already exists on the internet; on the other hand, it is also true that these systems actually generate new, different texts, sometimes mixing concepts in a way that can be regarded as original. It is very difficult to really understand these systems, and I would say that in reality we know very little about them. This statement is somewhat strange, since they are human-made and human-made systems whose engineering is well known. We know which components, we know individually which calculations are made in each of the modules that make up these systems. However, the scale of these systems (i.e. the various trillions of parameters involved, and web-wide training data) means that interactions between the components generate results that are difficult to predict, and the study of these systems is similar to what happens in other areas of knowledge such as physics or biology, where study objects are very complex.

While it is true that the results are truly surprising, there are still many limitations in the use of these systems. They usually produce fluid and grammatical text, corresponding to very plausible continuations for entries, but with content that seems certain but may be wrong. This is because the systems are trained with limited information (e.g. web data, i.e. multilingual, but mainly in English, and sometimes containing biased or even factually wrong information), particularly for more specific topics or recent events. Due to the way these systems work, they are very limited in fact-checking, performing logical reasoning, or performing calculations. Sometimes the answers submitted by these systems even show quotes and links to content that does not exist. We cannot definitively say what these models 'know and what they don't know', and we do not know when these models are confident expressing statements that are incorrect.

We have seen (and will continue to see in the coming years) very rapid progress and continuous improvements in these systems. Some of the limitations I have just mentioned will probably be overcome in the next versions of these systems (e.g. by combining these systems with others, such as calculators to expand the ability to perform calculations, or search engines as a way to access more up-to-date information), but the problem will hardly be completely solved and critical thinking is therefore needed in the use of these systems. I would say that one of the challenges of the increasing use of these systems will be to train people in the proper use of these tools.

In the particular context of education, the introduction of these technologies has been particularly transformative, with positive and negative aspects. I think it will be a concrete area of application that illustrates the challenge, potential, and problems brought about by the use of these tools. It is undeniable that the use of systems such as ChatGPT can be very useful for students and teachers, acting as a kind of always available "tutors" who can help summarise information, or generate questions that help check apprenticeships. However, there is the problem of academic integrity, in particular the concern that students can use tools such as ChatGPT without the teachers' knowledge, delivering automatically generated reports as if they were texts authored by them. This is a difficult (perhaps even impossible) problem to resolve, as the current tools to detect automatically generated text do not work, and there will be hardly any tools that offer guarantees of correct detection. In the academic world I think there is a broad consensus on the importance of ethical awareness of the use of these tools, as opposed to the ban, and teachers and institutions should seek to have a clear policy on the use of these tools, indicating in which cases their use is (or is not) acceptable.

Systems such as ChatGPT also raise several concerns in the context of personal data protection, some similar to other web services, and others perhaps a bit more different and private. For example, there are concerns related to the collection and storage of data supporting the training of these systems, be it data made available on the web or interactions with the system, which can be stored for improvement purposes. These data may include personal information, and there is already a regulatory framework indicating what these systems can or may not do. In order to operate, these systems must comply with existing data protection regulations, and aspects such as users' right to data portability, the right to be forgotten and transparency about how their data are used, the right to explicit and informed consent for data to be used are guaranteed. However, the scale on which these systems operate poses many difficulties in ensuring that the web information that is used to train these models is actually in line with the obligations I have just described, or that it is free of offensive or biased content. This is essentially a technical challenge, which will still require a lot of work in the field.

Another particularly relevant aspect, related to the protection of personal data, is the use of these systems for phishing and social engineering attacks. Systems such as ChatGPT can be used very effectively to imitate the individual and thus create very convincing phishing messages, facilitating social engineering attacks to steal personal information. This is more than a technical challenge and it is difficult to anticipate what societal impact the increasing use of systems for these purposes will have. If, on the one hand, regulatory and anti-criminal mechanisms need to be adapted in order to deal with these cases, I am convinced that it will be through awareness raising and education, by strengthening ethics in education (e.g. engineering education and training for those developing these tools) that we can have a greater impact.

Finally, I wanted to give you the message that we should not anticipate the future, but rather consider the present situation where the use of AI tools like ChatGPT is common and omnipresent. This is the current reality, and it is important that people are informed about the potential and limitations of these tools.

SESSÃO DE ENCERRAMENTO
CLOSING SESSION

Paula Meira Lourenço
Presidente da Comissão Nacional de Proteção de Dados

PROTEÇÃO DE DADOS PESSOAIS
QUE FUTURO ESTAMOS A CONSTRUIR

Permitam-me que cumprimente todos Vós na pessoa de Sua Excelência o Presidente da Assembleia da República, e que, em meu nome, e em nome da Comissão Nacional de Proteção de Dados, reitere o agradecimento que fiz na Sessão de Abertura, a Sua Excelência o Presidente da Assembleia da República, ao Senhor Secretário-Geral da Assembleia da República, e às Senhoras e Senhores Deputados da Nação, a disponibilidade e a gentileza em receber-nos na Casa da Democracia, no ano em que celebramos o 30.º aniversário ao serviço de Portugal, lembrando que esta é também a Casa da Comissão Nacional de Proteção de Dados — porquanto a Comissão é uma Entidade independente que funciona junto da Assembleia da República —, e a Casa de todos nós, enquanto cidadãos.

Coincidentemente, assinala-se também este ano o 50.º aniversário do 25 de abril de 1974 e o 20.º aniversário da Autoridade Europeia para a Proteção de Dados (EDPS) – pelo que aproveito esta oportunidade para congratular Wojciech Wiewiórowsi, a Autoridade Europeia para a Proteção de Dados, pelas duas décadas de missão em sede de proteção de dados pessoais.

A Comissão Nacional de Proteção de Dados é, há 30 anos, a Autoridade Administrativa independente que assegura o respeito pelo direito fundamental à proteção de dados pessoais, como tal previsto no n.º 1, do artigo 8.º, da Carta dos Direitos Fundamentais da União Europeia (CDFUE), no n.º 1, do artigo 16.º, do Tratado de Funcionamento da União Europeia (TFUE) e no artigo 35.º da Constituição da República Portuguesa (CRP), o qual deve ser conjugado com outros princípios e direitos fundamentais conexos, como seja os princípios da igualdade e não discriminação em razão de ascendência, sexo, raça, etnia, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual (artigo 13.º da CRP), o direito à reserva da intimidade da vida privada, à identidade pessoal, à identidade genética do ser humano, ao desenvolvimento da personalidade, ao bom nome, à reputação e à imagem (artigo 26.º da CRP), e

bem assim o direito à liberdade (artigo 27.º da CRP) – direitos, liberdades e garantias constitucionais que assumem particular relevância em ambiente digital.

Trata-se de direitos humanos fundamentais que emergiram há cerca de 50 anos com a democracia, com o eclodir do Estado de direito democrático, e que desde 1976 têm assento na Constituição da República Portuguesa, tendo Portugal sido pioneiro a nível mundial na sua consagração formal como direito fundamental.

Em 2018, porém, com o RGPD, assistimos a uma mudança de paradigma em sede de regulação, pois passámos de um modelo de heteroregulação, para um modelo de autorregulação, baseado na avaliação do risco e na tomada de medidas para a sua mitigação por parte dos responsáveis pelo tratamento dos dados, paradigma mais condicente com o dinamismo e a flexibilidade que a permanente desadequação de soluções normativas impõe, com a análise do risco e da complexidade decorrente das particularidades do caso concreto de cada área e sector (financeiro, económico, saúde, etc..).

Como a filosofia subjacente à autorregulação é mais responsabilizante para as organizações (públicas e privadas), que são as responsáveis pelo tratamento dos dados e os seus subcontratantes, assistimos desde 2018 à reorganização das instituições, que tiveram de se reinventar para corresponder aos objetivos da autorregulação, tendo designado os seus Encarregados de Proteção de Dados e os seus Responsáveis de Segurança da Informação (ou CISO – chief information security officer).

Desde 2018, a CNPD é a Autoridade Nacional de Controlo, a Autoridade administrativa independente que tem por atribuição controlar e fiscalizar o cumprimento do RGPD e da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD, e a sua missão revela-se na sua atividade de regulação (*ex ante*, ou seja, centrada no controlo prévio: o responsável pelo tratamento tem de consultar a CNPD, antes de proceder ao tratamento, quando a avaliação de impacto sobre a proteção de dados indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar os riscos), regulamentação, na emissão de pareceres relativamente a iniciativas legislativas da AR e Governo, e regulamentares, na supervisão, fiscalização, aplicação de medidas corretivas e sancionatórias (processos de contraordenação, ou a suspensão de tratamento de dados – definitiva ou provisória), e bem assim na divulgação de informação e emissão de Orientações e o reforço da cooperação nacional e internacional.

Em 2023, abrimos 2.656 processos, dos quais 1.818 foram processos de averiguação, o que representa um acréscimo de cerca de 2% face ao ano anterior.

No que se refere a notificações de violações de dados pessoais, nos últimos 3 anos, a CNPD registou um aumento de 36% de violações de dados: em 2021 recebemos 453 participações, em 2022 tivemos 560, e em 2023 houve 618 reportes, tendo em 2023 sido abertos 409 processos (destes, 303 provieram de entidades privadas e 106 de entidades públicas).

Nos processos de violação de dados pessoais (data breach), foram adotadas 197 deliberações, tendo a CNPD feito em todas elas recomendações específicas no sentido de as organizações melhorarem o nível de segurança dos seus tratamentos de dados, através da adoção de medidas adequadas à situação concreta.

Realço ainda as sanções aplicadas, em especial a aplicação de coimas por infrações à legislação. No ano de 2023, a CNPD aplicou o maior número de coimas: 90 coimas, no valor de perto de 560 mil euros. Foram sobretudo casos de violação das regras de videovigilância, envio de marketing em violação das regras legais (spam) e por violação do RGPD.

Não posso deixar de fazer uma referência especial à inspeção efetuada à recolha de dados biométricos pela WorldCoin Foundation, pelo impacto público que provocou, e que resultou na decisão de suspensão, por 90 dias, desta atividade, em nome da salvaguarda do direito à proteção de dados pessoais, especialmente de menores.

Mas mais do que enunciar o passado e o presente, queremos que o nosso 30.º aniversário seja ancorado numa visão prospetiva, face aos desafios e oportunidades mais prementes que se colocam aos cidadãos, enquanto titulares dos dados pessoais, onde a CNPD seja conquistadora, e não herdeira, audaz, e não saudosista, e que participe, de forma proativa, na resolução dos desafios que o futuro nos coloca.

Foi por isso, que no início do meu mandato, em maio de 2023, propus à CNPD a aprovação de um Plano Estratégico para o triénio de 2024-2026, e após uma consulta pública (teve lugar pela primeira vez na história da CNPD, em julho de 2023), a CNPD aprovou o seu 1.º Plano Estratégico trienal.

Temos metas muito concretas, que definimos em 3 grandes objetivos e 20 vinte ações estratégicas. E, não obstante o plano ter como horizonte temporal 2026, 16 dessas ações iniciaram-se já em 2024, porque não há tempo a perder, o mundo vive em acelerada mudança e temos de recorrer a todos os mecanismos para que, com ambição e com o melhor conhecimento e meios disponíveis, possamos assegurar o estrito cumprimento da lei à velocidade que estes novos tempos nos impõem.

Sinteticamente, gostaria de partilhar convosco esses objetivos, que nos guiarão até 2026.

Em primeiro lugar, o reforço da proteção dos dados pessoais dos cidadãos, assegurando uma maior divulgação ao público da missão da CNPD e dos direitos dos titulares dos dados, porque, sem conhecimento, sem informação, nenhum cidadão poderá defender os seus direitos.

A este propósito, dou-vos nota de que, em 2023, recebemos 7.874 pedidos de informação e de participação, sobretudo de cidadãos, através dos canais disponibilizados pela CNPD no seu sítio da Internet. Entre as matérias reportadas destacam-se as comunicações eletrónicas não solicitadas (spam), a videovigilância no local de trabalho e no contexto das relações de vizinhança e a garantia de direitos perante os responsáveis pelo tratamento.

No que se refere ao segundo grande objetivo do nosso Plano, queremos aumentar a capacidade de observação estratégica dos riscos e oportunidades colocados pela aceleração da inovação tecnológica e pela segurança das práticas e dos processos emergentes. Isto consegue-se através de um maior aprofundamento de conhecimentos no domínio tecnológico e da inovação característicos da Era digital, promovendo um enquadramento regulatório que previna e sancione más práticas. Para tal, é essencial o permanente diálogo com os meios académicos, científicos e empresariais.

O 3.º objetivo estratégico da CNPD visa reforçar e fortalecer a regulação dos dados pessoais em Portugal, através de mecanismos colaborativos e de cooperação com entidades nacionais e internacionais. Neste domínio, a partilha de informação e de conhecimento é absolutamente essencial para alcançarmos a eficiência dos meios e recursos indispensáveis à prossecução da atividade da CNPD, com respeito pela sua independência, autonomia e isenção.

Estes grandes objetivos têm, depois, tradução em ações concretas, das quais gostaria de destacar o lançamento do Plano Nacional de Formação em Proteção de Dados, em conjunto com os Pais e os Professores, e as crianças e jovens, tendo em vista a melhoria da aplicação e do bom entendimento das leis, envolvendo a Assembleia da República, o Governo (designadamente o Ministério da Educação) e as autarquias locais. Inspirámo-nos na boa experiência do Projeto Dadus, iniciado pelo Presidente da CNPD, Mestre Luís Lingnau da Silveira, e estamos convictos de que este novo Plano é uma peça essencial para a literacia nesta área tão fundamental na vida dos nossos concidadãos.

Planeamos ainda criar um "Canal prioritário de interação" no site da Comissão, que permita aos menores apresentarem as suas queixas online, que terão um tratamento urgente por parte da CNPD, quando se trate de disponibilização na Internet de conteúdos digitais de grande violência, sobretudo contra crianças e jovens mulheres, para que a CNPD possa ordenar a sua imediata eliminação, como medida cautelar (sem prejuízo da coordenação com o Ministério Público e os órgãos de polícia criminal).

A CNPD quer ter um papel proativo na defesa das crianças e jovens em ambiente digital, e irá apresentar à Assembleia da República uma Proposta de Lei que consagre esta solução legislativa, que já provou funcionar em Espanha, onde há um procedimento administrativo cautelar, que vigora há 3 anos, e que tem sido muito eficaz: a Agência Espanhola de Proteção de Dados emite ordens de apagamento dos dados, as quais são cumpridas pelas empresas reguladas em 100% dos casos e dentro do prazo definido – o "Canal prioritário" foi aqui hoje referido pela Diretora da Agência Espanhola de Proteção de Dados, Mar España Martí.

E também ouvimos atentamente as medidas elencadas por Ana Brian Nougrères, Relatora Especial da ONU para o Direito à Privacidade, para fazer face à discriminação online.

Vamos também estabelecer e reforçar canais de diálogo e de cooperação mútua com várias instituições, públicas e privadas, que prosseguem objetivos comuns, designadamente com a Autoridade Nacional de Comunicações, o Centro Internet Segura, o Centro Nacional de Cibersegurança, o Conselho de Fiscalização do Sistema Integrado de Informação Criminal e Conselho de Fiscalização da Base de Dados de Perfis de ADN, instituições do ensino superior e respetivos Centros de Investigação, o Instituto Nacional de Administração, o Instituto Português de Acreditação, o Instituto Português da Qualidade e a Provedoria de Justiça.

No plano internacional, estamos em permanente diálogo com as nossas congéneres e com todos os órgãos, grupos de trabalho e fóruns europeus e internacionais em que a CNPD participa regularmente, desde há muitos anos.

Com efeito, desde 1997, a CNPD viu os seus Presidentes, Membros e representantes serem eleitos para diversos fóruns, como seja a Presidência e/ou a Vice-Presidência da Autoridade de Controlo Comum de Schengen (1997-1999 e após 2003), da Instância Comum de Controlo do Eurojust, da Instância Comum de Controlo da Europol (2008-2013), e após 2019 até muito recentemente, uma representante da CNPD assumiu a Presidência do Comité de Supervisão Coordenada para os sistemas de informação europeus – facto destacado por Anu Talus, Presidente do Comité Europeu para a Proteção de Dados, na sua intervenção na nossa Conferência, no painel da manhã, numa expressa referência à Dra. Clara Guerra e ao seu notável trabalho nessas honrosas e exigentes funções.

Desde 2018, a Comissão Nacional de Proteção de Dados tem participado de forma muito ativa nas reuniões mensais e grupos de trabalho do Comité Europeu para a Proteção de Dados, a par da Autoridade Europeia para a Proteção de Dados, sendo hoje crescente a utilização de instrumentos jurídicos de cooperação (assistência mútua e realização de operações conjuntas) no tratamento de casos transfronteiriços, para facilitar a obtenção de consensos, e bem assim os procedimentos de controlo da coerência, tendo em vista a interpretação e aplicação uniforme dos princípios e normas jurídicas previstas no RGPD.

Relativamente à Rede Ibero-americana de Proteção de Dados, da qual a CNPD foi Membro fundador, em conjunto com a Agência Espanhola de Proteção de Dados, contamos já com 21 anos de profícua cooperação, como bem assinalou na nossa Conferência de hoje Josefina Román Vergara, Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI), que detém a Presidência da Rede Ibero-americana de Proteção de Dados.

É claro que a Comissão Nacional de Proteção de Dados continuará a contribuir para o diálogo global sobre proteção de dados – por exemplo, este ano participei nas reuniões do Comité Europeu para a Protecção de Dados, nas reuniões da Rede Ibero-americana de Proteção de Dados, no Simpósio de Privacidade de Veneza, na ANGOTIC, o maior evento de inovação e comunicações eletrónicas de Angola, e no Outono participarei na Assembleia Global de Privacidade e no Encontro Ibérico, que reavivámos no ano passado, e que este ano terá lugar aqui em Lisboa.

E tendo em vista o reforço da cooperação entre países lusófonos, e em resposta à questão formulada por Faustino Varela Monteiro, Presidente da Comissão Nacional de Proteção de Dados da Cabo Verde, na sua preleção de hoje de manhã, tenho a honra de anunciar que amanhã, na sede da Comissão Nacional de Proteção de Dados, terá lugar a primeira reunião oficial de criação da Rede Lusófona de Autoridades de Proteção de Dados, com a participação dos Presidentes das Autoridades Nacionais de Proteção de Dados de Angola, Brasil, Cabo Verde e São Tomé e Príncipe, para formalizar os laços institucionais que fomos criando ao longo destes 30 anos, e conferir-nos a escala que merecemos, para, em conjunto – e estando abertos à

participação dos 35 Estados que falam a língua portuguesa, em 5 continentes, ou de organizações, no estatuto de Membros ou de Observadores –, termos uma maior capacidade de defender os interesses dos cidadãos, sustentados na defesa dos Direitos Humanos, dos Direitos, Liberdades e Garantias e do Estado de Direito Democrático.

E porque falamos do futuro, é inelutável falarmos da regulação dos dados pessoais em ambiente digital, em especial face à utilização da inteligência artificial (IA), que é uma tecnologia que apresenta muitas vantagens (maior celeridade na execução de tarefas e poupança de encargos administrativos e financeiros), mas também coloca vários riscos em sede de proteção de dados pessoais, alguns dos quais referidos também na Conferência de hoje, pelo Prof. Doutor Bruno Martins, e que não podemos escamotear.

Permitam-me destacar os seguintes riscos: os dados recolhidos poderem ser usados e vendidos sem o consentimento dos titulares dos dados; desinformação (o mundo repleto de ***deepfake*** – alucinações não intencionais dos sistemas de IA generativa); riscos reputacionais (criação intencional de informação falsa e /ou difamatória); roubo de identidade; roubo de segredo de negócio; data breach; treino e algoritmo (dados enviesados, com elevado risco de discriminação em razão do género e da raça /origem) e "desvios" de finalidade (como nos revelou o escândalo "Cambridge Analytics", onde a recolha de dados pessoais no Facebook – "gostos" e "hábitos" –, permitiu a análise, elaboração de perfis e envio de informação selecionada para efeitos de manipulação psicológica, tendo em vista obter um determinado resultado eleitoral nos EUA – eleição de Donald Trump).

Muito recentemente, a UN Women (***United Nations Agency for gender equality and women´s empowerment***) salientou que a IA espelha a discriminação de género: de entre 133 sistemas de IA, em diferentes sectores, 44% apresentam discriminação de género – ex.: escreve uma história entre médicos e enfermeiros: "Era uma vez um médico e uma enfermeira…"

Nos EUA, descontinuou-se um sistema de IA concebido para auxiliar os juízes a avaliar a possibilidade de concessão, ou não, de liberdade condicional, por se ter chegado à conclusão que o sistema só dava parecer favorável a seres humanos de raça branca. Se a informação recolhida é racista, o conteúdo é racista e tende-se a perpetuá-lo, devido à repetição.

Como sabemos, a IA envolve dados pessoais e onde há dados pessoais a CNPD deve estar presente. Por isso, a CNPD está totalmente disponível para assegurar a regulação da IA, pois enquanto Autoridade Nacional independente, que assegura a proteção de direitos fundamentais, temos uma atuação transversal, algo fundamental para se regular uma tecnologia de uso amplo como a IA.

Como bem frisou o Comité Europeu para a Proteção de Dados e a Autoridade Europeia para a Proteção de Dados no seu Parecer conjunto n.º 5/2021, as Autoridades Nacionais de Proteção de Dados de cada Estado-Membro são as Autoridades vocacionadas para receber as competências legais em sede de inteligência artificial.

A utilização da IA envolve riscos quanto à salvaguarda de princípios e direitos fundamentais, éticos, jurídicos que colocam em causa a identidade humana – como YUVAL HARARI bem frisou: *"Não sei se a humanidade pode sobreviver"*.

Senhor Presidente da Assembleia da República

Minhas Senhoras e Meus Senhores,

Numa sociedade em que se assiste a sucessivas vagas de regulamentação – ao RGPD seguiu-se o Regulamento dos Serviços Digitais (Regulamento (UE) n.º 2022/2065, do Parlamento Europeu e do Conselho, de 19 de outubro de 2022), a Diretiva NIS 2 (Diretiva (UE) 2022/2555, de 14 de dezembro de 2022), o Regulamento Dados e o Regulamento da Inteligência Artificial –, ficamos com a sensação que as soluções nascem já desatualizadas relativamente aos problemas que pretendiam resolver.

Tivemos o privilégio de ouvir as reflexões de muitos dos responsáveis de várias destas instituições internacionais, as suas experiências e a forma como têm vencido os enormes desafios com que estamos, coletivamente, confrontados.

Importa encontrar um novo paradigma de proteção de dados pessoais na Era digital, conciliando as novas tecnologias, o uso da inteligência artificial nas organizações, a Internet das Coisas ou o metaverso, e conciliar este "novo mundo" com o bem-estar e o princípio da dignidade da pessoa humana, pilar do Estado de Direito, com a proteção de dados pessoais, essência da identidade do ser humano.

A proteção de dados pessoais é imanente a um Estado de direito democrático, como é a República Portuguesa, e onde a Comissão existe há três décadas.

Perante estes e outros desafios e oportunidades que o futuro nos coloca, e atentas as permanentes tensões entre a proteção de dados pessoais e outros direitos e bens jurídicos, temos de agir e reagir, com sabedoria e com a prudência e a determinação que todas elas exigem, procurando uma solução proporcional e adequada, justa, pois sem a proteção devida aos dados pessoais, nas suas múltiplas conjugações, não há regularidade administrativa ou burocrática, nem economia, nem justiça e nem democracia.

Espero que a comemoração dos 30 anos da CNPD que assinalámos hoje na Casa da Democracia tenha permitido, com confiança e determinação, reafirmar a relevância da proteção do direito fundamental à proteção dos dados pessoais, e direitos fundamentais conexos, que precisa da ação de todas e de todos.

Trata-se de um imperativo de que depende a Humanidade.

Paula Meira Lourenço
President of the Portuguese Data Protection Supervisory Authority

PERSONAL DATA PROTECTION
BUILDING THE FUTURE

Allow me to greet you all in the person of His Excellency the President of the Portuguese Parliament and, on my behalf and on behalf of the Portuguese Data Protection Supervisory Authority express once again our gratitude to His Excellency the President of the Portuguese Parliament, to the Secretary General of the Portuguese Parliament, and to the Honourable Members of Parliament the willingness and kindness to receive us at the House of Democracy, in the year we celebrate the 30th anniversary in the service of Portugal, recalling that this is also the House of the Portuguese Data Protection Supervisory Authority – as the Commission is an independent body working within the Portuguese Parliament – and the House of all of us as citizens.

This year also marks the 50th anniversary of 25 April 1974 and the 20th anniversary of the European Data Protection Supervisor (EDPS) – I take this opportunity to compliment Wojciech Wiewiórowsi, the European Data Protection Supervisor, for the two decades of personal data protection mission.

The Portuguese Data Protection Supervisory Authority has been, for 30 years, the Independent Administrative Authority which ensures respect for the fundamental right to the protection of personal data, provided for in Article 8 (1) of the Charter of Fundamental Rights of the European Union (CFREU), Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) and Article 35 of the Constitution of the Portuguese Republic (CPR), which must be combined with other related principles and fundamental rights, such as the principles of equality and non-discrimination on the grounds of descent, sex, race, ethnicity, language, territory of origin, religion, political or ideological opinion, instruction, economic situation, social condition or sexual orientation (Article 13 CRP), the right to privacy, personal identity, genetic identity, personality development, good name, reputation and image (Article 26 CRP), as well as the right to liberty (Article 27 CRP) – constitutional rights, freedoms and guarantees of particular relevance in the digital environment.

These are fundamental human rights that emerged about 50 years ago from democracy, with the outbreak of the democratic rule of law, and which since 1976 have featured in the Constitution of the Portuguese Republic, and Portugal has been a global frontrunner in its formal establishment as a fundamental right.

In 2018, however, with the GDPR, we saw a paradigm shift in regulation, as we moved from a heteroregulation model to a self-regulatory model, based on risk assessment and mitigation measures by data controllers, a paradigm that is more consistent with the dynamism and flexibility required by the continuing inadequacy of regulatory solutions, with an analysis of the risk and complexity arising from the particularities of each area and sector (financial, economic, health, etc.).

As the underlying philosophy of self-regulation gives more responsability to organisations (public and private), which are data controllers and processors, we have witnessed since 2018 the reorganisation of the institutions, which had to reinvent themselves to meet the objectives of self-regulation and have appointed their Data Protection Officers and their Chief Information Security Officers (CISO).

Since 2018, the CNPD has been the National Supervisory Authority, the independent administrative authority entrusted with the task of monitoring and supervise compliance with the GDPR and Law 58/2019 of 8 August, which implements the GDPR in the internal legal order, and its role is apparent in its regulatory activity (*ex ante*, i.e. focusing on prior control: the controller has to consult the CNPD, prior to processing, when the data protection impact assessment indicates that the processing would result in a high risk in the absence of the measures taken by the controller to mitigate the risks), regulation, by issuing opinions on legislative initiatives of the Parliament and the Government, and regulations, in supervision, monitoring, enforcing corrective and sanctioning measures (infringement proceedings, or suspension of data processing – final or interim), as well as in the disclosure of information and issuing guidelines and the strengthening of national and international cooperation.

In 2023, we opened 2.656 cases, of which 1.818 were investigative procedures, an increase of around 2 % compared to the previous year.

As regards personal data breach notifications, in the last 3 years, the CNPD has seen a 36 % increase in data breaches: in 2021 we received 453 notifications, in 2022 we had 560, and in 2023 there were 618, while in 2023 there were 409 cases opened (of these, 303 were from private entities and 106 from public entities).

In the data breach cases, 197 resolutions were adopted and the CNPD made specific recommendations for organisations to improve the level of security of their data processing by taking measures appropriate to the specific situation.

I would also highlight the sanctions applied, in particular the imposition of fines for infringements of the legislation. In 2023, the CNPD imposed the highest number of fines: 90 fines, amounting to almost EUR 560,000. These were mainly cases of infringements of the rules on videosurveillance, marketing in breach of legal rules (spam) and infringements of the GDPR.

I would like to make a special reference to the inspection of biometric data by the Worldcoin Foundation, for the public impact it has caused, which resulted in the decision to suspend its activity for 90 days, in the name of safeguarding the right to the protection of personal data, especially of minors.

But more than spelling out the past and the present, we want our 30th anniversary to be anchored in a forward-looking vision, in the face of the most pressing challenges and opportunities for citizens, as personal data subjects, where the CNPD is a conqueror, not an heir, bold, rather than nostalgic, and is proactively involved in addressing the challenges that the future brings.

That is why, at the beginning of my mandate in May 2023, I proposed to the CNPD the approval of a Strategic Plan for the three-year period 2024-2026, and after a public consultation (which took place for the first time in the history of the CNPD in July 2023), the CNPD approved its 1st three-year Strategic Plan.

We have very concrete targets, which we set out in 3 headline targets and 20 strategic actions. And although the plan has a time horizon of 2026, 16 of these actions started already in 2024, because there is no time to lose, the world is changing rapidly and

we need to use all mechanisms so that, with ambition and with the best knowledge and means available, we can ensure strict compliance with the law at the speed that these new times demand of us.

In summary, I would like to share these objectives with you, which will guide us until 2026.

First, strengthening the protection of citizens' personal data by ensuring greater dissemination to the public of the CNPD's mission and the rights of data subjects, because without knowledge, without information, no citizen will be able to defend their rights.

In this regard, I will let you know that in 2023 we received 7.874 requests for information and participation, mainly from citizens, through the channels made available by the CNPD on its website. These include unsolicited electronic communications (spam), videosurveillance in the workplace and in the context of neighbourly relations and the guarantee of rights vis-à-vis those controllers.

Regarding the second major objective of our Plan, we want to increase the capacity for strategic observation of the risks and opportunities posed by the acceleration of technological innovation and the security of emerging practices and processes. This is achieved by further deepening technological knowledge and innovation characteristic of the digital Era, promoting a regulatory framework that prevents and penalises bad practices. To this end, continuous dialogue with academic, scientific and business circles is essential.

The CNPD's 3rd strategic objective aims to reinforce and strengthen the regulation of personal data in Portugal through collaborative mechanisms and cooperation with national and international bodies. In this area, the sharing of information and knowledge is absolutely essential in order to achieve the efficiency of the necessary means and indispensable resources for the CNPD to continue its activities, while respecting its independence, autonomy and impartiality.

These major targets are then translated into concrete actions, of which I would like to highlight the launch of the National Data Protection Training Plan, together with parents, teachers, children and young people, with a view to improving the application and good understanding of laws, involving the Portuguese Parliament, the Government (in particular the Ministry of Education) and local authorities. We have drawn inspiration from the good experience of the Dadus Project, initiated by CNPD President Luís Lingnau da Silveira, and we are convinced that this new Plan is an essential part of literacy in this key area in the lives of our fellow citizens.

We are also planning to create a "Priority Channel for Interaction" on the Commission's website, allowing minors to submit their complaints online, which will be dealt with as a matter of urgency by the CNPD when it comes to making digital content of great violence available online, especially against children and young women, so that the CNPD can order its immediate removal as a precautionary measure (without prejudice to coordination with the Public Prosecutor's Office and the criminal police).

The CNPD wants to play a proactive role in defending children and young people in the digital environment, and will submit to the Portuguese Parliament a draft law setting out this legislative solution, which has proved to be operational in Spain, where there has been a precautionary administrative procedure, which has been in place for 3 years, and which has been very effective: the Spanish Data Protection Supervisory Authority issues data erasure orders, which are complied with by regulated companies in 100 % of cases and within the set deadline – the 'Priority Channel' was referred to here today by the Director of the Spanish Data Protection Supervisory Authority, Mar España Martí.

And we also listened closely to the measures listed by Ana Brian Nougères, UN Special Rapporteur on the Right to Privacy, to address online discrimination.

We will also establish and strengthen channels for dialogue and mutual cooperation with various public and private institutions which pursue common objectives, in particular with the National Communications Authority, the Secure Internet Centre, the National Cybersecurity Centre, the Supervisory Council of the Integrated Criminal Information System and the Supervisory Council of the DNA Profile Database, higher education institutions and their research centres, the National Institute of Administration, the Portuguese Institute for Accreditation, the Portuguese Institute of Quality and the Portuguese Ombudsman.

At international level, we are in constant dialogue with our counterparts and with all European and international bodies, working groups and forums in which the CNPD has participated regularly for many years.

Indeed, since 1997, the CNPD has seen its Presidents, Members and representatives elected to various forums, such as the Presidency and /or Vice-Presidency of the Schengen Joint Supervisory Authority (1997-1999 and after 2003), the Joint Supervisory Body of Eurojust, the Europol Joint Supervisory Body (2008-2013), and after 2019 until very recently, a representative of the CNPD took over the Chair of the Coordinated Supervisory Committee for European Information Systems – a fact highlighted by Anu Talus, Chairwoman of the European Data Protection Board, in her intervention at our Conference in the morning panel, in an express reference to Ms. Clara Guerra and her remarkable work in these honourable and demanding roles.

Since 2018, the Portuguese Data Protection Supervisory Authority has been very actively involved in the monthly meetings and working groups of the European Data Protection Board, alongside the European Data Protection Supervisor, and the use of legal instruments for cooperation (mutual assistance and joint operations) in the handling of cross-border cases is increasing to facilitate consensus building and consistency monitoring procedures with a view to the uniform interpretation and application of the principles and legal rules laid down in the GDPR.

With regard to the Ibero-American Data Protection Network, of which the CNPD was a founding member, together with the Spanish Data Protection Supervisory Authority, we already count on 21 years of fruitful cooperation, as pointed out at our conference today by Josefina Román Vergara, Commissioner of the National Institute for Transparency, Access to Information and Personal Data Protection (INAI), which holds the presidency of the Ibero-American Data Protection Network.

It is clear that the Portuguese Data Protection Supervisory Authority will continue to contribute to the comprehensive data protection dialogue – for example, this year I participated in the meetings of the European Data Protection Board, the meetings of the Ibero-American Data Protection Network, the Venice Privacy Symposium, ANGOTIC, Angola's largest innovation and electronic communications event, and in autumn I will participate in the Global Privacy Assembly and in the Iberian Meeting, which we have revived last year, and this year will take place here in Lisbon.

With a view to strengthening cooperation between Portuguese-speaking countries, and in response to the question raised by Mr Varela Monteiro, President of the Data Protection Supervisory Authority of Cape Verde, in his prelection of this morning, I have the honour to announce that tomorrow, at the headquarters of the Portuguese Data Protection Supervisory Authority, the first official meeting will take place to set up the Lusophone Network of Data Protection Authorities, with the participation of the Presidents of the National Data Protection Authorities of Angola, Brazil, Cape Verde and São Tomé and Príncipe, in order to formalise the institutional ties that we have created over these 30 years, and to give us the scale we deserve, together – and being open to the participation of the 35 states speaking Portuguese on 5 continents, or of organisations, with the status of Members or Observers – we have a greater capacity to defend the interests of citizens, based on the defence of human rights, and of rights, freedoms and guarantees and the rule of law.

And since we talk about the future, it is inevitable to talk about the regulation of personal data in the digital environment, in particular in the face of the use of artificial intelligence (AI), which is a technology that has many advantages (faster execution of tasks and saving administrative and financial burdens), but also poses a number of risks for the protection of personal data, some of which was also mentioned at today's Conference by Professor Bruno Martins, and which we cannot hide.

Allow me to highlight the following risks: the data collected can be used and sold without the consent of the data subjects; disinformation (a world full of deepfakes – unintentional hallucinations of generative AI systems); reputational risks (intentional creation of false and /or defamatory information); identity theft; theft of business secrets; data breach; training and algorithm (biased data with high risk of discrimination on grounds of gender and race /origin) and purpose 'deviations' (as revealed by the Cambridge Analytics scandal, where the collection of personal data on Facebook – 'likes' and 'habits' – allowed for analysis,

profiling, and sending of selected information for psychological manipulation with a view to obtaining a certain election result in the US – election of Donald Trump).

Very recently, the UN Women (United Nations Agency for gender equality and women´ s empowerment) pointed out that AI reflects gender discrimination: out of 133 AI systems in different sectors, 44 % have gender discrimination – e.g.: write a story between doctors and nurses: "Once upon a time, a doctor (male) and a nurse (female)..."

In the USA, an AI system intended to assist judges in assessing whether or not to grant parole has been discontinued, as the conclusion has been reached that the system only gave a favourable opinion to white-race humans. If the information collected is racist, the content is racist and tends to perpetuate it due to repetition.

As we know, AI involves personal data, and where there is personal data, the CNPD should be present. Therefore, the CNPD is fully available to ensure the regulation of AI, since, as the independent National Authority which ensures the protection of fundamental rights, we have a cross-cutting action which is crucial for regulating a widely used technology such as AI.

As the European Data Protection Board and the European Data Protection Supervisor rightly pointed out in their Joint Opinion 5/2021, the national data protection authorities of each Member State are the authorities destined to receive legal powers in the field of Artificial Intelligence.

The use of AI involves risks in terms of safeguarding fundamental, ethical, legal principles and rights that undermine human identity – as YUVAL HARARI rightly pointed out: "I don't know if humanity can survive".

Dear President of the Assembly of the Republic /Portuguese Parliament,

Ladies and Gentlemen,

In a society where there are successive waves of regulation – the GDPR was followed by the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022), the NIS 2 Directive (Directive (EU) 2022/2555 of 14 December 2022), the Data Act and the Artificial Intelligence Act – we feel that the solutions are already outdated in relation to the problems they intended to address.

We had the privilege to listen to the reflections of many of the leaders of several of these international institutions, their experiences and how they have met the huge challenges we are collectively facing.

It is important to find a new paradigm of personal data protection in the digital age, reconciling new technologies, the use of artificial intelligence in organisations, the Internet of Things or the metaverse, and to reconcile this 'new world' with the well-being and the principle of human dignity, a pillar of the rule of law, with the protection of personal data, which is the essence of human identity.

The personal data protection is inherent to a democratic state governed by the rule of law, such as the Portuguese Republic, where the Commission has existed for three decades.

In the face of these and other challenges and opportunities that the future poses, and in view of the continuing tensions between the protection of personal data and other rights and legal interests, we must act and react, with wisdom and with the caution and determination they all require, seeking a proportionate and appropriate fair solution, as without the due protection of personal data, in their multiple combinations, there is no administrative or bureaucratic regularity, economy, justice and democracy.

I hope that today's celebration of the 30th anniversary of the CNPD at the House of Democracy has allowed us to reaffirm, with confidence and determination, the importance of protecting the fundamental right to personal data protection, and related fundamental rights, which requires action from everyone.

This is an imperative upon which Humanity depends.

José Pedro Aguiar-Branco
Presidente da Assembleia da República

Exma. Senhora Presidente da Comissão Nacional de Proteção de Dados, Dr.ª Paula Meira Lourenço

Minhas senhoras e meus senhores,

Assinala-se em 2024 os trintas anos da Comissão Nacional de Proteção de Dados.

A todos os que a integram – e a integraram ao longo dos anos – o meu agradecimento e a minha homenagem cívica.

Em 1994, a Internet ainda não se tinha generalizado em Portugal. Estávamos longe de imaginar a importância que haveria de ter.

Mas em 1994 o Parlamento intuiu que era preciso criar os instrumentos adequados para esse novo mundo que nascia. Era preciso preparar o futuro.

Tanto a regulamentação da Comissão, como as outras deliberações que então se fizeram sobre proteção de dados, só puderam ser concretizadas, porque se gerou um amplo consenso parlamentar.

Só se avançou, porque houve conversações. Só se decidiu, porque houve acordo entre os vários partidos.

Também hoje, 30 anos depois, não sabemos como será o futuro. O mundo digital parece cada vez mais vasto, complexo, rico de oportunidades.

Para a cultura, para a democratização do conhecimento, para a economia, para o diálogo social, para a participação cívica.

Mas também esconde novos desafios e novas encruzilhadas.

Para enfrentar o futuro, precisamos novamente de gerar consensos. Temas que, na sociedade, são consensuais não devem, no Parlamento, ser foco de divisões, mais ou menos artificiais. Nem devem ficar bloqueados por falta de diálogo.

Em Espanha discute-se, hoje, um Pacto de Estado para proteger as crianças no uso dos meios digitais.

Fala-se, em particular, de um acesso demasiado precoce a conteúdos pornográficos ou violentos.

Em França, o Governo encomendou um relatório sobre o impacto do computador e do telemóvel na infância.

Os peritos recomendam, entre outras coisas, que sejam criados mecanismos para impedir as crianças de aceder a sites pornográficos.

Fala-se de uma situação de «assimetria de informação» em grau máximo. Pedem-se formas legais de responsabilizar estes sites pela verificação de quem os visita.

Em Portugal, o primeiro contacto com a pornografia acontece, em média, aos onze anos. É cedo, demasiado cedo.

Da mesma forma, a discriminação e a desigualdade nos meios digitais. Se há algum dado que todos os estudos revelam é que as famílias mais carenciadas são também as que têm menos literacia digital.

Famílias em que os filhos sabem mais sobre a Internet do que os próprios pais. E, por isso, não têm mediadores, não têm mestres nem critérios seguros. Estão sozinhos no mundo digital.

Falo também das redes sociais e da forma como estão a impactar a própria democracia.

As redes sociais oferecem-nos novas formas de socialização e de relação. Novas oportunidades de diálogo e de organização política e social.

As redes podem ser o lugar onde os eleitos e os eleitores se reaproximam. Podem ser o palco onde as instituições recuperam importância e medem o pulso à sociedade.

Mas podem ser também um campo aberto à desinformação e ao radicalismo. Para o acicatar das fraturas sociais e das incompreensões mútuas. Para o colapso de todas as mediações e para a fragmentação social.

Também aqui, é preciso uma reflexão de fundo. Concertada, dialogada, atenta aos sinais do mundo.

Minhas senhoras e meus senhores

Volto ao início desta intervenção e à palavra consensos.

Precisamos de criar novos consensos.

Sobre a proteção da infância na internet.

Sobre a literacia digital.

Sobre a privacidade e os direitos que dela decorrem.

Sobre o combate à discriminação nos meios digitais.

Sobre as redes sociais e a democracia, salvaguardando sempre a liberdade de expressão.

Quero saudar, por isso, esta iniciativa de assinalar os trinta anos da Comissão Nacional de Proteção de Dados, não a exaltar o passado, mas a pensar o presente e o futuro.

Uma conferência que nos mostrou novas ideias e boas práticas internacionais e que nos desafia a fazer melhor.

Há trinta anos, o diálogo franco e o consenso alargado permitiram criar a CNPD e fazer a primeira legislação sobre proteção de dados pessoais.

Hoje, com um diálogo sério e uma autêntica procura de consensos, podemos fazer mais para tornar a Internet num espaço seguro.

José Pedro Aguiar-Branco
President of the Portuguese Parliament (called the Assembleia da República)

Dear Ms President of the Portuguese Data Protection Supervisory Authority, Professor Paula Meira Lourenço

Ladies and Gentlemen,

2024 marks the thirty years of the Portuguese Data Protection Supervisory Authority.

To all its members – and to those who have been a part of it over the years – my thanks and civic tribute.

In 1994, the Internet had not yet become widespread in Portugal. We were far from imagining how important it would be.

But in 1994 Parliament made it clear that the right tools had to be put in place for the new world that was born. We needed to prepare for the future.

Both the Commission's rules and the other deliberations that took place at that time on data protection could only be approved because there was a broad parliamentary consensus.

Progress was made only because there were talks. It was only decided because there was an agreement between the various parties.

Also today, 30 years later, we do not know how the future will be. The digital world seems increasingly broad, complex, rich in opportunities.

For culture, for the democratisation of knowledge, for the economy, for social dialogue, for civic participation.

It also hides new challenges and crossroads.

To face the future, we need to build consensus again. Topics that are consensual in society should not be the focus of divisions, whether artificial or not, in Parliament. Nor should they be blocked for lack of dialogue.

Today, Spain is discussing a State Pact to protect children in the use of digital means.

In particular, there is too early access to pornographic or violent content.

In France, the government commissioned a report on the impact of computer and mobile phone on childhood.

The experts recommend, among other things, that mechanisms be put in place to prevent children from accessing pornographic sites.

There is a situation of "information asymmetry" to a maximum degree. Legal ways are being sought to hold these websites accountable for verifying who visits them.

In Portugal, the first contact with pornography takes place on average at eleven years. It is early, too early.

Similarly, discrimination and inequality in digital media. If there is one thing that all studies reveal, it is that the most disadvantaged families are also those with the lowest digital literacy.

Families where children know more about the Internet than their parents themselves. So they do not have intermediaries, they have no masters and no insurance criteria. They are alone in the digital world.

I also talk about social media and how they are impacting democracy itself.

Social media offers us new forms of socialisation and relationships. New opportunities for dialogue and political and social organisation.

Networks can be the place where elected and voters reconnect. This can be the stage where institutions regain importance and measure the wrist to society.

But they can also be an open field for disinformation and radicalism. To spur social fractures and misunderstandings.

For the collapse of all mediations and social fragmentation.

Here too, a substantive reflection is needed. Concerted, dialogued, attentive to world signals.

Ladies and gentlemen,

I return to the beginning of this intervention and to the word consensus.

We need to build new consensus.

On the protection of children on the Internet.

On digital literacy.

On privacy and the rights deriving from it.

On combating discrimination in digital media.

On social media and democracy, always safeguarding freedom of expression.

I would therefore like to welcome this initiative to mark the thirty years of the Portuguese Data Protection Supervisory Authority, not exposing it to the past, but to think of the present and the future.

A conference which showed us new ideas and international best practices, and challenges us to do better.

Thirty years ago, open dialogue and broad consensus enabled the establishment of the CNPD and the first legislation on the protection of personal data.

Today, with serious dialogue and a genuine search for consensus, we can do more to make the Internet a secure space.

Da esquerda para a direita: Bruno Martins, Investigador e Professor Associado do Instituto Superior Técnico da Universidade de Lisboa; Mar España Martí, Diretora da Agência Espanhola de Proteção de Dados; Anu Talus, Presidente do Comité Europeu para a Proteção de Dados; Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados; Wojciech Wiewiórowski, Autoridade Europeia para a Proteção de Dados; Josefina Román Vergara, Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) do México, que detém a presidência da Rede Ibero-americana de Proteção de Dados; Ana Brian Nougrères, Relatora Especial da ONU para o Direito à Privacidade; Faustino Varela Monteiro, Presidente da Comissão Nacional de Protecção de Dados de Cabo Verde

From left to right: Bruno Martins, Researcher and Professor at the Lisbon University; Mar España Martí, Director of the Spanish Data Protection Supervisory Authority; Anu Talus, Chair of the European Data Protection Board; Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority; Wojciech Wiewiórowski, European Data Protection Supervisor; Josefina Román Vergara, Commissioner of the National Institute of Transparency, Access to Information and Personal Data Protection of Mexico (INAI), which holds the Presidency of the Ibero-American Data Protection Network; Ana Brian Nougrères, UN Special Rapporteur for the Rights to Privacy; Faustino Varela Monteiro, President of the Data Protection Supervisory Authority of Cape Verde

Da esquerda para a direita: Paula Meira Lourenço, Presidente da CNPD, com José Carlos Vegar Alves Velho, Maria da Conceição Lourenço Martins Correia Diniz e Ana Paula Pinto Ferreira Lourenço, Vogais da CNPD

From left to right: Paula Meira Lourenço, President of the CNPD, with José Carlos Vegar Alves Velho, Maria da Conceição Lourenço Martins Correia Diniz, and Ana Paula Pinto Ferreira Lourenço, Members of the CNPD

Paula Meira Lourenço, Presidente da CNPD, e Luís Barroso, Vogal da CNPD
Paula Meira Lourenço, President of the CNPD, and Luís Barroso, Member of the CNPD

Paula Meira Lourenço, Presidente da CNPD, e Maria Cândida Guedes de Oliveira, Vogal da CNPD
Paula Meira Lourenço, President of the CNPD, and Maria Cândida Guedes de Oliveira, Member of the CNPD

Paula Meira Lourenço, Presidente da CNPD, com Luís Lingnau da Silveira, antigo Presidente da CNPD (entre 2001 e 2012)
Paula Meira Lourenço, President of the CNPD, with Luís Lingnau da Silveira, former President of the CNPD (between 2001 and 2012)

Paula Meira Lourenço, Presidente da CNPD, e Anu Talus, Presidente do Comité Europeu para a Proteção de Dados
Paula Meira Lourenço, President of the CNPD, and Anu Talus, Chair of the European Data Protection Board

Paula Meira Lourenço, Presidente da CNPD, e Mar España Martí, Diretora da Agência Espanhola de Proteção de Dados
Paula Meira Lourenço, President of the CNPD, and Mar España Martí, Director of the Spanish Data Protection Supervisory Authority

Paula Meira Lourenço, Presidente da CNPD, e Faustino Varela Monteiro, Presidente da Comissão Nacional de Protecção de Dados de Cabo Verde

Paula Meira Lourenço, President of the CNPD, and Faustino Varela Monteiro, President of the Data Protection Supervisory Authority of Cape Verde

Paula Meira Lourenço, Presidente da CNPD, e Wojciech Wiewiórowski, Presidente da Autoridade Europeia para a Proteção de Dados
Paula Meira Lourenço, President of the CNPD, and Wojciech Wiewiórowski, European Data Protection Supervisor

Paula Meira Lourenço, Presidente da CNPD, e Ana Brian Nougrères, Relatora Especial da ONU para o Direito à Privacidade
Paula Meira Lourenço, President of the CNPD, and Ana Brian Nougrères, UN Special Rapporteur for the Rights to Privacy

Paula Meira Lourenço, Presidente da CNPD, e Josefina Román Vergara, Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) do México, que detém a presidência da Rede Ibero-americana de Proteção de Dados

Paula Meira Lourenço, President of the CNPD, and Josefina Román Vergara, Commissioner of the National Institute of Transparency, Access to Information and Personal Data Protection of Mexico (INAI), which holds the Presidency of the Ibero-American Data Protection Network

Paula Meira Lourenço, Presidente da CNPD, e Bruno Martins, Investigador e Professor Associado do Instituto Superior Técnico da Universidade de Lisboa

Paula Meira Lourenço, President of the CNPD, and Bruno Martins, Researcher and Professor at the Lisbon University

Convidados
Guests

Convidados
Guests

Convidados
Guests

Visita à exposição de Vieira da Silva “Nós e a Liberdade” na Assembleia da República
Visit to the Vieira da Silva exhibition “Us and Freedom” at the Portuguese Parliament


QUE FUTURO
ESTAMOS
A CONSTRUIR?

Sessão de Abertura da Conferência Internacional Comemorativa do 30.º aniversário da CNPD - Manuel Magno, Vice-Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, e Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados

Opening Session of the International Conference commemorating the 30th anniversary of the CNPD - Manuel Magno, Vice-Chair of the Commission for the Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament, and Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority

Intervenção de Paula Meira Lourenço, Presidente da CNPD, na sessão de abertura
Intervention by Paula Meira Lourenço, President of the CNPD, at the opening session

Sessão de Abertura da Conferência Internacional Comemorativa do 30.º aniversário da CNPD - Manuel Magno, Vice-Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, e Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados

Opening Session of the International Conference commemorating the 30th anniversary of the CNPD - Manuel Magno, Vice-Chair of the Commission for the Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament, and Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority

Convidados
Guests

Painel da sessão da manhã (mesa da esquerda para a direita): Faustino Varela Monteiro, Presidente da Comissão Nacional de Protecção de Dados de Cabo Verde; Anu Talus, Presidente do Comité Europeu para a Proteção de Dados; Wojciech Wiewiórowski, Autoridade Europeia para a Proteção de Dados; Mar España Martí, Diretora da Agência Espanhola de Proteção de Dados

Morning Session Panel (table from left to right): Faustino Varela Monteiro, President of the Data Protection Supervisory Authority of Cape Verde; Anu Talus, Chair of the European Data Protection Board; Wojciech Wiewiórowski, European Data Protection Supervisor; Mar España Martí, Director of the Spanish Data Protection Supervisory Authority

Painel da sessão da manhã (mesa da esquerda para a direita): Faustino Varela Monteiro, Presidente da Comissão Nacional de Protecção de Dados de Cabo Verde; Anu Talus, Presidente do Comité Europeu para a Proteção de Dados; Wojciech Wiewiórowski, Autoridade Europeia para a Proteção de Dados; Mar España Martí, Diretora da Agência Espanhola de Proteção de Dados

Morning Session Panel (table from left to right): Faustino Varela Monteiro, President of the Data Protection Supervisory Authority of Cape Verde; Anu Talus, Chair of the European Data Protection Board; Wojciech Wiewiórowski, European Data Protection Supervisor; Mar España Martí, Director of the Spanish Data Protection Supervisory Authority

Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados, junto aos convidados da Conferência Internacional
Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority, with guests at the International Conference


CONFERÊNCIA
INTERNACIONAL
INTERNATIONAL
CONFERENCE
24 JUN 2024
PROTEÇÃO DE DADOS PESSOAIS
QUE FUTURO
ESTAMOS
A CONSTRUIR?
BUILDING
THE FUTURE
CNPD

Painel da sessão da tarde (mesa da esquerda para a direita): Josefina Román Vergara, Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) do México, que detém a presidência da Rede Ibero-americana de Proteção de Dados; Ana Brian Nougrères, Relatora Especial da ONU para o Direito à Privacidade; Bruno Martins, Investigador e Professor Associado do Instituto Superior Técnico da Universidade de Lisboa

Afternoon Session Panel (table from left to right): Josefina Román Vergara, Commissioner of the National Institute of Transparency, Access to Information and Personal Data Protection of Mexico (INAI), which holds the Presidency of the Ibero-American Data Protection Network; Ana Brian Nougrères, UN Special Rapporteur for the Rights to Privacy; Bruno Martins, Researcher and Professor at the Lisbon University

Sessão da tarde: Josefina Román Vergara, Comissária do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) do México, que detém a presidência da Rede Ibero-americana de Proteção de Dados; Ana Brian Nougrères, Relatora Especial da ONU para o Direito à Privacidade; Bruno Martins, Investigador e Professor Associado do Instituto Superior Técnico da Universidade de Lisboa

Afternoon session: Josefina Román Vergara, Commissioner of the National Institute of Transparency, Access to Information and Personal Data Protection of Mexico (INAI), which holds the Presidency of the Ibero-American Data Protection Network; Ana Brian Nougrères, UN Special Rapporteur for the Rights to Privacy; Bruno Martins, Researcher and Professor at the Lisbon University

José Pedro Aguiar-Branco, Presidente da Assembleia da República, acompanhado pelo seu Chefe do Gabinete, Rui Clero, e funcionários da Assembleia da República
José Pedro Aguiar-Branco, President of the Portuguese Parliament, accompanied by his Chief of Staff, Rui Clero, and staff of the Portuguese Parliament

Sessão de Encerramento da Conferência Internacional Comemorativa do 30.º aniversário da CNPD com Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados, e José Pedro Aguiar-Branco, Presidente da Assembleia da República

Closing Session of the International Conference commemorating the 30th anniversary of the CNPD with Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority, and José Pedro Aguiar-Branco, President of the Portuguese Parliament

Sessão de Encerramento da Conferência Internacional Comemorativa do 30.º aniversário da CNPD com Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados, e José Pedro Aguiar-Branco, Presidente da Assembleia da República

Closing Session of the International Conference commemorating the 30th anniversary of the CNPD with Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority, and José Pedro Aguiar-Branco, President of the Portuguese Parliament

Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados, e José Pedro Aguiar-Branco, Presidente da Assembleia da República, durante a Sessão de Encerramento da Conferência Internacional Comemorativa do 30.º aniversário da CNPD

Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority, and José Pedro Aguiar-Branco, President of the Portuguese Parliament, during the Closing Session of the International Conference International Conference commemorating the 30th anniversary of the CNPD

José Pedro Aguiar-Branco, Presidente da Assembleia da República
José Pedro Aguiar-Branco, President of the Portuguese Parliament


UTURO
MOS
STRUIR?

Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados, e José Pedro Aguiar-Branco, Presidente da Assembleia da República, durante a Sessão de Encerramento da Conferência Internacional Comemorativa do 30.º aniversário da CNPD

Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority, and José Pedro Aguiar-Branco, President of the Portuguese Parliament, during the Closing Session of the International Conference International Conference commemorating the 30th anniversary of the CNPD

Convidados
Guests

José Pedro Aguiar-Branco, Presidente da Assembleia da República
José Pedro Aguiar-Branco, President of the Portuguese Parliament

Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados, e José Pedro Aguiar-Branco, Presidente da Assembleia da República, durante a Sessão de Encerramento da Conferência Internacional Comemorativa do 30.º aniversário da CNPD

Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority, and José Pedro Aguiar-Branco, President of the Portuguese Parliament, during the Closing Session of the International Conference International Conference commemorating the 30th anniversary of the CNPD


DOS PESSOAIS
TURO
OS
TRUIR?
NAL DATA PROTECTION
BUILDING
E FUTURE

Sessão de Encerramento da Conferência Internacional Comemorativa do 30.º aniversário da CNPD
Closing Session of the International Conference commemorating the 30th Anniversary of the CNPD

Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados, e José Pedro Aguiar-Branco, Presidente da Assembleia da República, durante a Sessão de Encerramento da Conferência Internacional Comemorativa do 30.º aniversário da CNPD

Paula Meira Lourenço, President of the Portuguese Data Protection Supervisory Authority, and José Pedro Aguiar-Branco, President of the Portuguese Parliament, during the Closing Session of the International Conference International Conference commemorating the 30th anniversary of the CNPD


QUE FUTURO
ESTAMOS
A CONSTRUIR?

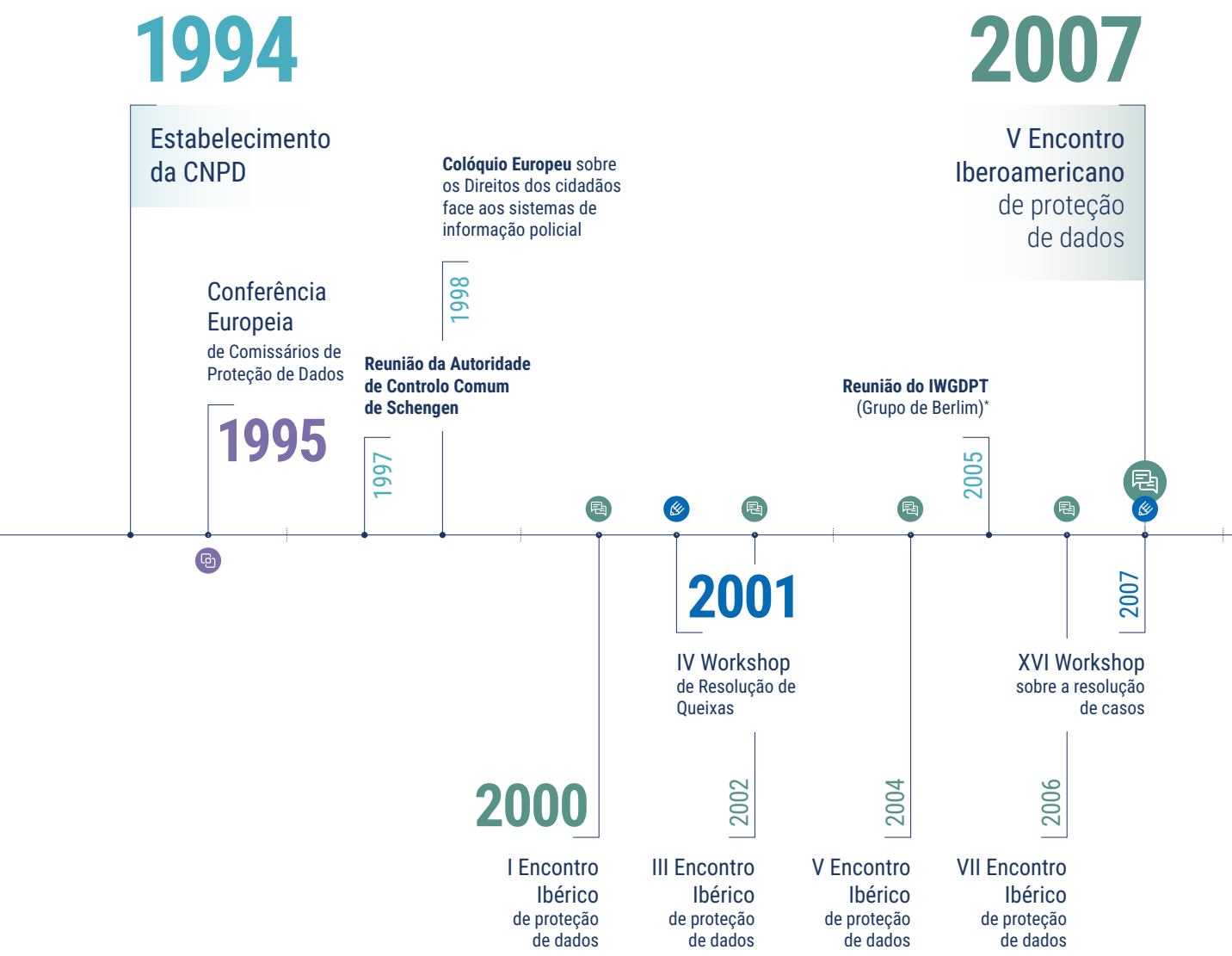
CRONOLOGIA DA CNPD
CNPD TIMELINE

A cooperação internacional sempre foi uma das vertentes principais da atividade da CNPD ao longo dos seus 30 anos. A CNPD promoveu diversas iniciativas e foi anfitriã de importantes fóruns no plano europeu e no plano mais global, incentivando o diálogo, o intercâmbio de experiências e perspetivas e a discussão alargada das matérias de proteção de dados pessoais. Apresenta-se aqui uma linha temporal de alguns dos momentos mais marcantes das últimas três décadas.

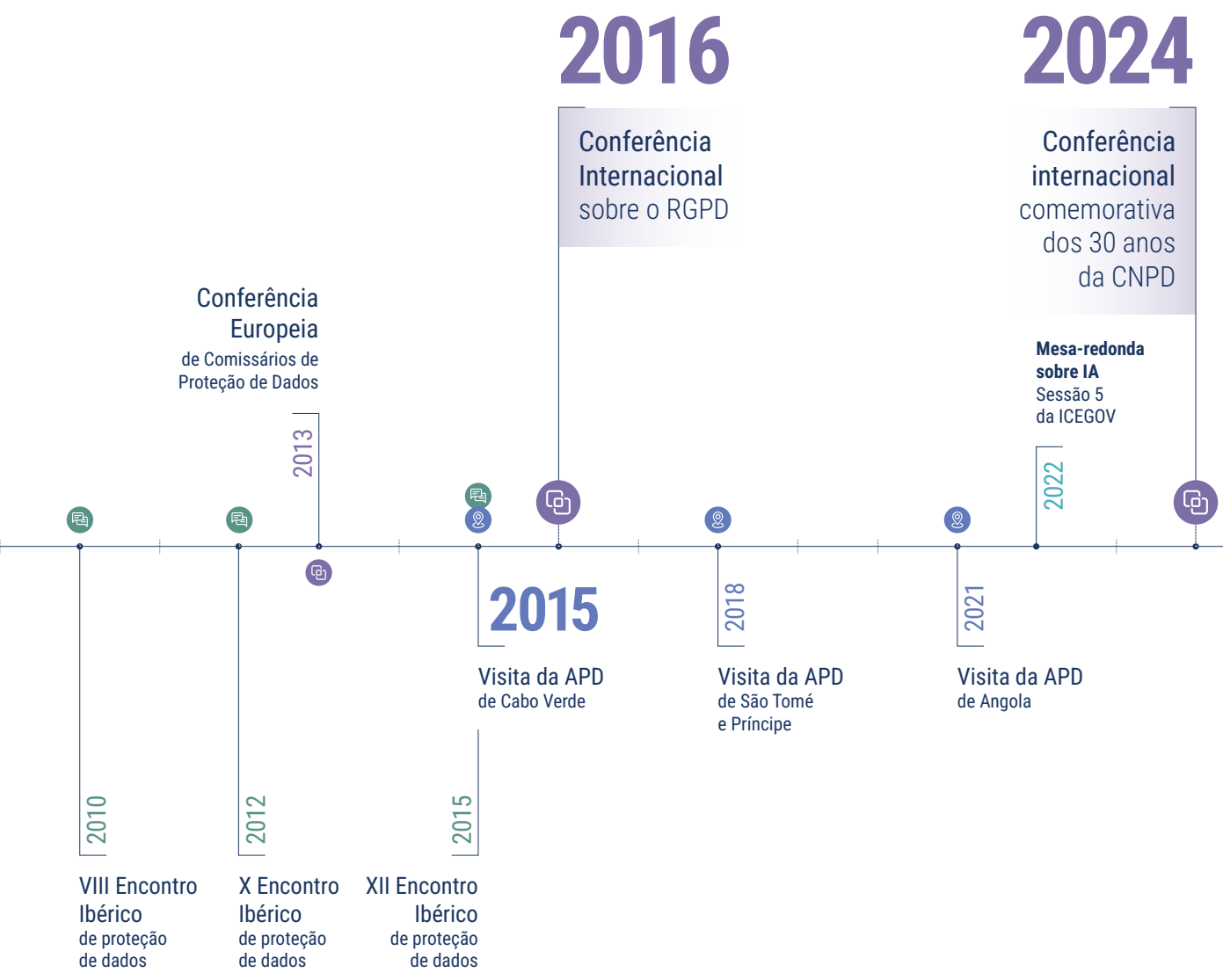
Boa viagem!

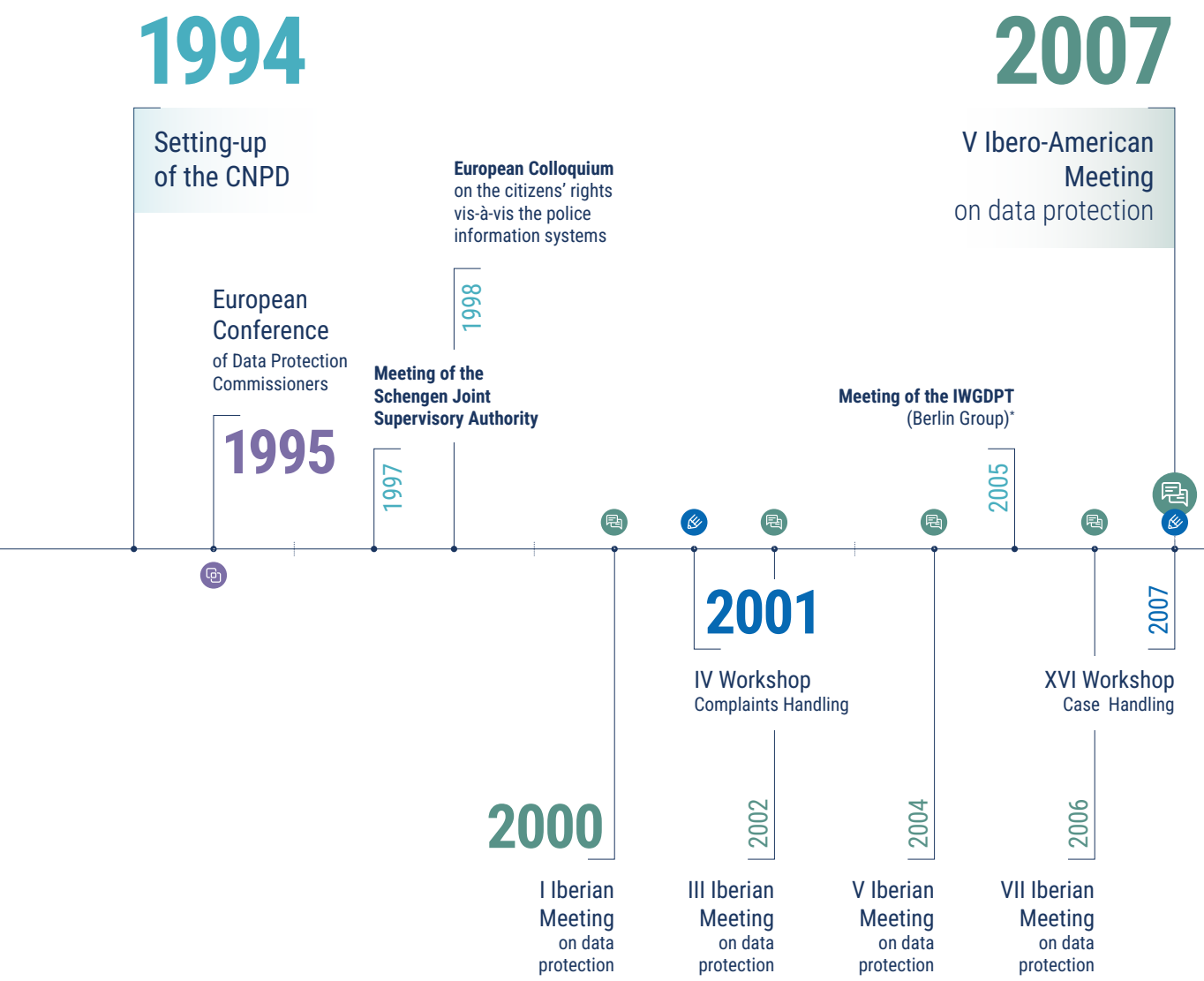
The international cooperation has been always a key-aspect of the CNPD's activity over these 30 years. The CNPD has promoted several initiatives and hosted important forums at European level and worldwide, fostering the dialogue, the exchange of experiences and perspectives and the overall discussion on data protection matters. Here it is presented a timeline with some of the most significant moments of the last three decades.

Enjoy the journey!

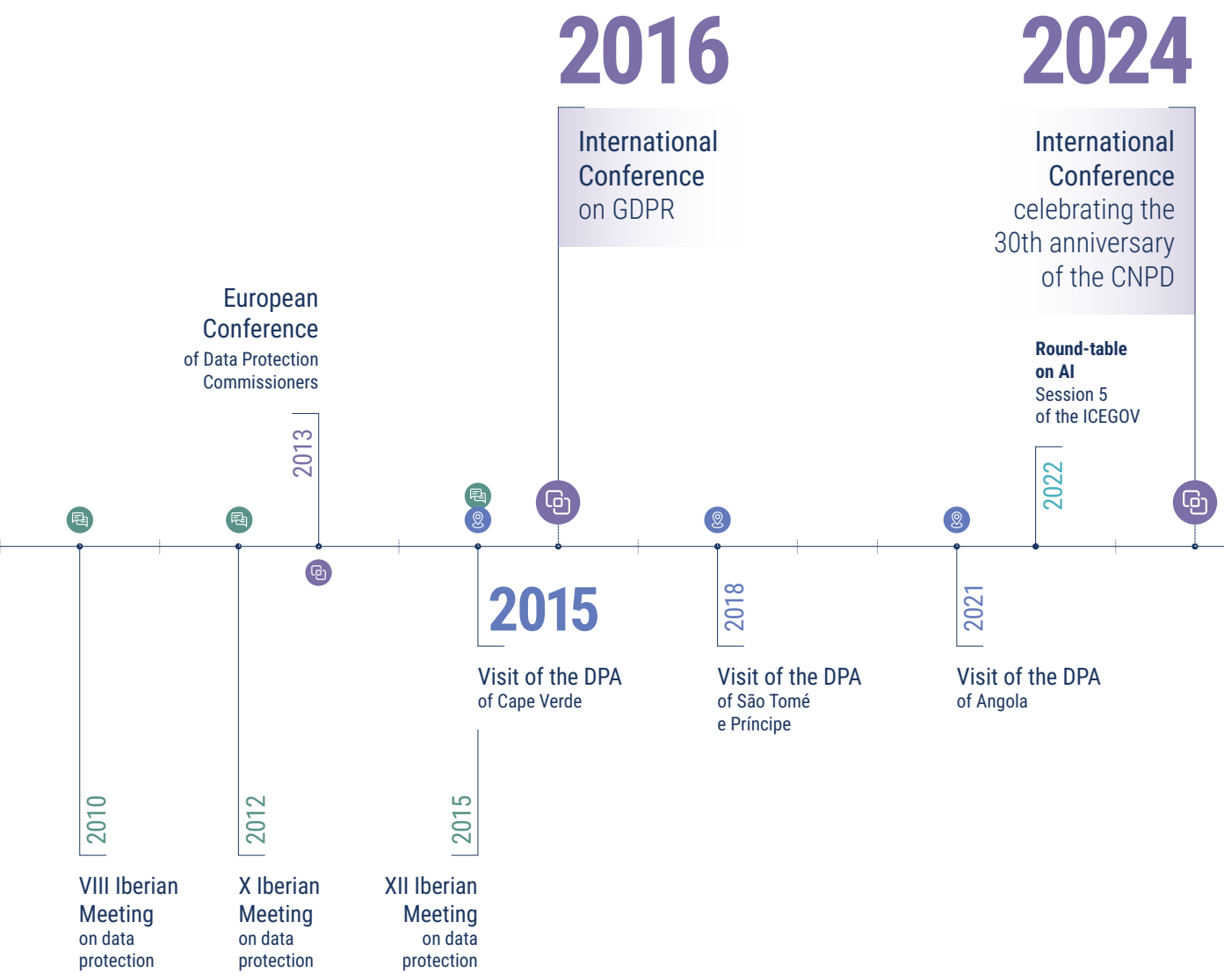


* Grupo de Trabalho Internacional de Proteção de Dados nas Telecomunicações, atualmente designado por Grupo de Trabalho Internacional de Proteção de Dados e Tecnologia


2010
VIII Encontro Ibérico de proteção de dados
2012
X Encontro Ibérico de proteção de dados
2013
Conferência Europeia de Comissários de Proteção de Dados
2015
XII Encontro Ibérico de proteção de dados
2015
Visita da APD de Cabo Verde
2016
Conferência Internacional sobre o RGPD
2018
Visita da APD de São Tomé e Príncipe
2021
Visita da APD de Angola
2022
Mesa-redonda sobre IA Sessão 5 da ICEGOV
2024
Conferência internacional comemorativa dos 30 anos da CNPD



* International Working Group on Data Protection in Telecommunications, now renamed as International Working Group on Data Protection and Technology


2016
International Conference on GDPR
2024
International Conference celebrating the 30th anniversary of the CNPD
European Conference of Data Protection Commissioners
2013
Round-table on AI Session 5 of the ICEGOV
2022
2015
Visit of the DPA of Cape Verde
2018
Visit of the DPA of São Tomé e Príncipe
2021
Visit of the DPA of Angola
2010
VIII Iberian Meeting on data protection
2012
X Iberian Meeting on data protection
2015
XII Iberian Meeting on data protection

COMEMORAÇÃO DO 30.º ANIVERSÁRIO

30TH ANNIVERSARY CELEBRATION

CNPD

Comissão Nacional
de Proteção de Dados