CEBRI

CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS

NÚCLEO EUROPA

Foco breve na Europa

Setembro, 2021

TRANSFORMAÇÃO DIGITAL E PROTEÇÃO DE DADOS:

O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGDP) DA UE E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) BRASILEIRA

EUROPE PROGRAM

Brief focus on Europe

September, 2021

DIGITAL TRANSFORMATION AND DATA PROTECTION:

THE EU GENERAL DATA PROTECTION REGULATION (GPDR) AND THE BRAZILIAN GENERAL PERSONAL DATA PROTECTION LAW (LGPD)

ISSN 2318-3713

FICHA TÉCNICA
TECHNICAL INFORMATION

Autoras
Authors

Ana Paula Tostes

Yasmin Renni

Coordenação Editorial
Editorial Coordination

Julia Dias Leite
Diretora-Presidente / *CEO*

Luciana Gama Muniz
Diretora de Projetos / *Director of Projects*

Hugo Bras Martins da Costa
Coordenador de Projetos / *Project Coordinator*

Design Gráfico
Graphic Design

Presto Design

ISSN 2318-3713

CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

Rua Marquês de São Vicente, 336 – Gávea
Rio de Janeiro / RJ - CEP: 22451-044
Tel + 55 21 2206-4400 - cebri@cebri.org.br
www.cebri.org

CEBRI

CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS

#2 Think Tank

América do Sul e Central

South and Central America

University of Pennsylvania's Think Tanks and Civil Societies Program 2020 Global Go To Think Tank Index Report

O Centro Brasileiro de Relações Internacionais (CEBRI) é um think tank independente e plural, que há mais de vinte anos se dedica à promoção do debate propositivo sobre a política externa brasileira.

O CEBRI é uma instituição sem fins lucrativos, com sede no Rio de Janeiro e reconhecida internacionalmente, que propõe soluções pragmáticas e inovadoras para alavancar a inserção internacional positiva do país dentro do contexto global.

Formado por figuras proeminentes na sociedade brasileira, o Conselho Curador é parte fundamental da rede apartidária, diversa e plural do CEBRI, composta por mais de 100 especialistas de diversas áreas de atuação e de pensamento.

The Brazilian Center for International Relations (CEBRI) is an independent think tank that contributes to building an international agenda for Brazil. For over twenty years, the institution has engaged in promoting a pluralistic and proposal-oriented debate on the international landscape and Brazilian foreign policy.

In its activities, CEBRI prioritizes themes with the greatest potential to leverage the country's international insertion into the global economy, proposing pragmatic solutions for the formulation of public policies.

It is a non-profit institution, headquartered in Rio de Janeiro and internationally recognized. Today, its circa 100 associates represent diverse interests and economic sectors and mobilize a worldwide network of professionals and organizations. Moreover, CEBRI has an active Board of Trustees composed of prominent members from Brazilian society.

PENSAR
DIALOGAR
DISSEMINAR
INFLUENCIAR

THINKING
DIALOGUING
DISSEMINATING
INFLUENCING

www.cebri.org

NÚCLEO EUROPA

O Núcleo EUROPA tem o objetivo de ampliar a reflexão e o debate sobre dimensões de interesse e pesquisa na Europa que impactam as relações internacionais, a política externa e as políticas públicas brasileiras. A proximidade histórica e cultural entre Brasil e Europa perpassa relações político-diplomáticas e econômico-comerciais de alto valor para nossa sociedade. O Núcleo visa aprofundar o diálogo e a troca de ideias, envolvendo setores público e privado no desenvolvimento de caminhos possíveis para uma relação mais densa e profícua entre o Brasil e a Europa, com foco na União Europeia e países europeus selecionados.

EUROPE PROGRAM

The EUROPE Program aims to broaden the reflection and debate on dimensions of interest and research in Europe that impact international relations, foreign policy and Brazilian public policies. The historical and cultural proximity between Brazil and Europe permeates political-diplomatic and economic-commercial relations of high value to our society. The Program aims to deepen the dialogue and exchange of ideas, involving the public and private sectors in the development of possible paths for a more solid and more fruitful relationship between Brazil and Europe, with a focus on the European Union and selected European countries.

CONSELHEIRO
TRUSTEE

Ronaldo Veirano

Sócio fundador do escritório de advocacia Veirano Advogados; Coordenador do Comitê de Governança e Nomeação do Instituto Brasileiro de Governança Corporativa (IBGC) e membro do Conselho Consultivo do Instituto Brasil do Woodrow Wilson Center em Washington, DC.

Founding partner of the law firm Veirano Advogados; Coordinator of the Governance and Nominating Committee of the Brazilian Institute of Corporate Governance (IBGC) and member of the Advisory Board of the Brazil Institute at the Woodrow Wilson Center in Washington, D.C.

SENIOR FELLOW

Ana Paula Tostes

Professora Associada no Departamento de Relações Internacionais da Universidade do Estado do Rio de Janeiro (UERJ), e Pesquisadora Prociência da FAPERJ. Possui Doutorado em Ciência Política pelo IUPERJ (atual IESP/UERJ) e Mestrado em Direito pela PUC/RJ.

Ph.D. in Political Science from IUPERJ (currently IESP/UERJ), and a Master's degree in Law from PUC/RJ. Associate Professor at the Department of International Relations of the State University of Rio de Janeiro (UERJ), and Prociência Researcher at FAPERJ.

PESQUISADORA ASSOCIADA
ASSOCIATED RESEARCHER

Yasmin Renni

Doutoranda em Relações Internacionais (Universidade NOVA de Lisboa). Formada em Economia (UFRJ) e mestre em Relações Internacionais (UERJ). É especialista em Negócios Internacionais (IBMEC), com experiência em projetos de internacionalização de empresas.

Associated Researcher at CEBRI. PhD candidate (NOVA University Lisbon). Graduate in Economics (UFRJ) and master in International Relations (PPGRI/UERJ). Specialized in International Business (IBMEC), with experience in companies' internationalization projects.

ÍNDICE

TABLE OF CONTENTS

CEBRI
CENTRO BRASILEIRO DE RELACÕES INTERNACIONAIS

NÚCLEO EUROPA

Foco breve na Europa

TRANSFORMAÇÃO DIGITAL E PROTEÇÃO DE DADOS:

O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGDP) DA UE E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) BRASILEIRA

Setembro, 2021

Transição digital na UE

O mundo está mudando e a esfera digital ganhou muito espaço nas últimas décadas, criando, assim, mais uma camada de complexidade nas relações humanas e nos direitos humanos. O século 21 trouxe mudanças de magnitude. As tecnologias digitais estão transformando nosso mundo: acesso móvel à internet, mídia social, comércio eletrônico (*e-Commerce*), segurança na internet, serviços em nuvem e habilidades digitais — é o início da Era Digital trazida pela Revolução Digital. A difusão das tecnologias digitais está presente em quase todos os negócios, sociedades e mundo do trabalho, e a pandemia do Covid-19 funcionou como um ponto de inflexão na aceleração da transformação digital em uma escala sem precedentes.

Face às mudanças trazidas pelas tecnologias digitais, a União Europeia (UE) vem adaptando o seu mercado único para o adequar à era digital, criando normas e condições de concorrência equitativas para as atividades neste novo domínio. A primeira Agenda Digital Europeia (ADE) da Comissão foi criada em meio ao mandato de José Manuel Durão Barroso na Presidência da Comissão da UE (2004-2014) e centrou-se no fornecimento de amplo acesso à infraestrutura de banda larga, especialmente para as regiões rurais e subdesenvolvidas, tendo aumentado o volume de comércio eletrônico (*e-Commerce*) transfronteiriço, que era excepcionalmente baixo[1].

A ADE tinha um escopo limitado, mas definiu o pano de fundo para a criação da estratégia do Mercado Único Digital (MUD). Adotada em maio de 2015, a estratégia MUD é uma das dez prioridades da Comissão Europeia[2]. A estratégia visava melhorar o acesso de indivíduos e empresas ao mundo *online*, criando condições equitativas para as redes e serviços digitais, a fim de maximizar o potencial de crescimento da economia digital na União[3].

O MUD foi desenvolvido com base em várias medidas legislativas, como diretivas e regulamentos, que iremos delinear neste artigo e, em particular, o Regulamento Geral de Proteção de Dados da UE (RGPD). O RGPD influenciou o Brasil e vários outros países, tais como Japão, Coreia do Sul, Chile e Argentina, na adoção de conceitos e regras similares, reforçando a habilidade da UE em difundir normas e atuar como um ator regulatório global.

---

1. MAKOWSKA, Marta. 2020. The Challenges of Making the EU fit for the Digital Age. PISM Policy Paper n. 4 (179) The Polish Institute of International Affairs. Disponível em: The Challenges of Making the EU Fit for the Digital Age

2. Para mais detalhes, cf: EUROPEAN COMMISSION: EUROSTAT: Overview - Digital economy and society - Eurostat

3. EUROPEAN COMMISSION, 2021. Shaping Europe's digital future, Disponível em: Shaping Europe's digital future | Shaping Europe's digital future

A existência de um mercado único digital põe em causa a forma tradicional de se pensar suas quatro liberdades fundamentais. A importância da livre circulação de bens, capitais, pessoas e serviços pode ser melhor compreendida quando desvendamos as implicações detalhadas das regulamentações e da harmonização jurídica entre os Estados-Membros. O impacto na região é grandioso, incluindo o controle de fronteiras, a inovação institucional e a vida econômica dos cidadãos que vivem no novo mercado interno — de caráter regional. A garantia das quatro liberdades dependerá mais da transição digital do que das limitações físicas à circulação nos Estados-Membros. Isto se dá porque as barreiras atuais não são mais físicas, mas de conhecimento, habilidades e tecnologia. O futuro da UE dependerá do seu potencial para transformar seu mercado único e torná-lo apto para a era digital. Segundo analistas, além de criar milhares de empregos, tal transformação contribuiria para a economia da UE com 415 bilhões de euros por ano[4]. Para a UE manter o seu papel internacional de poder regulatório também em matéria de desenvolvimento tecnológico e transformação digital, alinhada com os valores europeus, foi estratégico considerar a transição digital uma prioridade.

Uma economia digital e a nova ambição de criar o MUD envolvem claramente os direitos democráticos e as liberdades das pessoas. Devido à fragmentação dos impactos deste tipo de mercado no quotidiano dos cidadãos europeus, tais como o novo local de trabalho, o direito à privacidade, a utilização de mecanismos de comércio eletrônico (*e-commerce*), etc., vemos uma relação direta com a proteção de direitos individuais. Isto não é apenas válido para os cidadãos europeus que já fazem parte do Mercado Único da UE, mas também para os indivíduos que podem circular ou integrar atividades relacionadas com o MUD à distância — o que é característico da fluidez da era digital na vida social.

4. BOBAN, M. 2016. "Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world". Economic and social development. 16 International Scientific Conference on Economic and Social Development. The Legal Challenges of Modern World. 1-2 September, 2016, p.191.

Por que informação importa?

Uma distinção importante precisa ser esclarecida: a diferença entre dados e informação. Não sem antes lembrar que *Big Data* se refere a um volume muito grande de dados acumulados em computadores, nuvens ou qualquer outra forma de armazenamento de dados por meio digital.

Dados são informações não processadas ou tratadas. Geralmente estão armazenados em um computador, nuvem ou outra fonte de estocagem de dados. A informação, neste contexto, refere-se aos dados processados, que se tornam conhecidos, seja por classificação, organização ou documentação. Assim, a proteção de dados pessoais torna-se tão ou mais relevante do que a proteção e o acesso às informações pessoais[5].

Em ambiente tecnológico e com grande capacidade computacional, a expansão dos instrumentos de processamento de dados traz uma nova preocupação com o acúmulo e possibilidade de coleta e processamento desses dados.

A transformação tecnológica que agora permite o manuseio e processamento de *Big Data*, associada ao aumento de situações em que consumidores acessam mecanismos de comércio virtual ou simplesmente utilizam computadores e plataformas que registram dados pessoais, gera riscos para os proprietários desses dados, além de novas formas antiéticas ou uso ilegal de dados pessoais por outras pessoas.

A relevância da proteção de dados atinge debates sobre economia e democracia. A economia digital permeia dois níveis de direitos e demandas de proteção: de um lado, as elites econômicas com seus interesses empresariais, e de outro, os indivíduos, que são cidadãos e consumidores. O tema tem referência ao exercício dos direitos individuais sobre dados, reputação, anonimato, privacidade, liberdade e proteção da informação para os consumidores.

5. TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (Eds). 2019. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters. Revista dos Tribunais.

Economia Digital

A Revolução Digital alterou os padrões de produção e comportamento, assim como a Revolução Industrial, que mudou a lógica da indústria tradicional baseada na escassez de recursos para uma economia baseada na informação, informatização e conhecimento. Sob essas novas regras e comportamentos vigentes no campo do armazenamento e tratamento de dados, com a informação e o conhecimento abundantes, o desafio é de otimização: utilizá-los de maneira relevante. A era digital traz uma mudança de escopo, fronteiras e desafios para indivíduos, empresas e a economia como um todo.

A difusão das tecnologias digitais nas diferentes esferas de nossas vidas levou à criação de uma economia digital. A economia digital consiste na atividade econômica de bilhões de conexões *online* diárias entre pessoas, empresas, processos, dispositivos e dados[6]. A mudança na economia e nos negócios, porém, está no contexto de uma transformação das sociedades, nas relações, na construção de preferências e opiniões, na busca pela informação, na comunicação e, mais recentemente — ou seja, no contexto da pandemia do Covid-19, uma mudança no mundo do trabalho. Compreender essa transformação leva tempo e conhecimento.

A hiperconectividade já era percebida como a espinha dorsal da economia digital. Embora a UE conduza a sua política digital há muitos anos, é mais conhecida como uma superpotência regulatória do que como uma economia de alta tecnologia. No caso dos Estados Unidos (EUA), o potencial de alta tecnologia é notório, e podemos encontrar pesquisas que buscam um melhor entendimento da nova era digital que está impactando a sociedade e a força de trabalho norte-americanas.

Um relatório publicado pela Brookings Institution[7] apresenta uma análise detalhada das mudanças no conteúdo digital de 90 por cento da força de trabalho dos EUA em todos os setores entre 2001-2017. A pesquisa categorizou as ocupações em empregos que exigem habilidades digitais altas, médias ou baixas e rastreou os impactos das mudanças rápidas. Uma das conclusões interessantes é a falta de informações suficientes sobre a difusão da adoção digital no mundo do trabalho, o que ajudaria a mapear o nível de transformação e um

6. DELOITTE. 2021. What is digital economy? Unicorns, transformation and the internet of things. 2021 Malta Technology Leadership Survey. Disponível em: What is digital economy?

7. Para mais detalhes, cf: Brookings Report Digitalization and the American workforce

grau de mudança mais preciso. O relatório conclui, entre outras coisas, que a digitalização requer melhorias significativas na educação digital e altas habilidades.

Na verdade, a educação e a formação digitais são uma das áreas que a UE tem visado desde 2015, ao mesmo tempo que cria novos desafios de acesso baseados na raça e no gênero. Sob a nova Presidência e no contexto da situação pandêmica, a Comissão publicou um novo Plano de Ação para a Educação Digital (2021-2027), que é uma iniciativa política renovada da UE para apoiar a adaptação sustentável e eficaz dos sistemas de educação e formação dos Estados-Membros da UE à era digital. As duas áreas prioritárias do Plano de Ação são a promoção do desenvolvimento de um ecossistema de educação digital de alto desempenho e o aprimoramento das habilidades e competências digitais para a transformação digital[8].

Os parlamentares brasileiros também entenderam que a alfabetização digital e a formação são o caminho certo a seguir neste século 21. Um projeto de lei foi proposto em setembro de 2020 para uma Política Nacional de Educação Digital[9]. A proposta compreende iniciativas em educação, mas também inclusão digital, qualificação do mercado de trabalho, aumento da empregabilidade e pesquisa digital.

No âmbito da prioridade da agenda digital da UE, a União criou o *Digital Economy and Society Index* (DESI). É um índice que visa monitorar o desempenho digital geral da Europa e acompanhar o progresso dos países da UE em termos de competitividade digital. O índice tem **cinco dimensões** em sua estrutura para avaliar os aspectos gerais da digitalização: **conectividade**; **capital humano**; **uso da internet**; **integração de tecnologia digital**; **serviços públicos digitais**[10]. A **conectividade** diz respeito à infraestrutura digital, o acesso a uma conexão de banda larga rápida e confiável, tanto fixa como móvel. É a chave para a prestação de serviços sociais e econômicos em uma economia digital. O **capital humano** diz respeito ao conjunto de competências necessárias para acesso ao mundo digital e é a espinha dorsal da sociedade digital: para o engajamento em atividades digitais, desde o agendamento de uma consulta, realização de compras ou para trabalhar, é necessário possuir competências para tal.

O **uso da internet** refere-se ao uso da internet por pessoas físicas, que vem crescendo desde 2015. Já no caso das empresas, a **integração de tecnologias digitais** diz respeito às empresas que se tornam digitais em sua forma de trabalho, comunicação e venda (como é o caso do comércio eletrônico). Por fim, os **serviços públicos digitais** referem-se à qualidade e utilização de recursos e soluções digitais na prestação de serviços públicos. O recente cenário de pandemia destacou a importância de garantir a continuidade da prestação de serviços públicos, apesar do distanciamento social e das medidas de confinamento. No entanto, de acordo com o relatório DESI 2020, houve uma melhoria na qualidade e no uso dos serviços públicos digitais em 2019, antes da pandemia e como consequência da estratégia MUD[11].

---

8. Para mais detalhes, cf: EUROPEAN COMMISSION, 2021, see: Digital Education Action Plan (2021-2027) | Education and Training

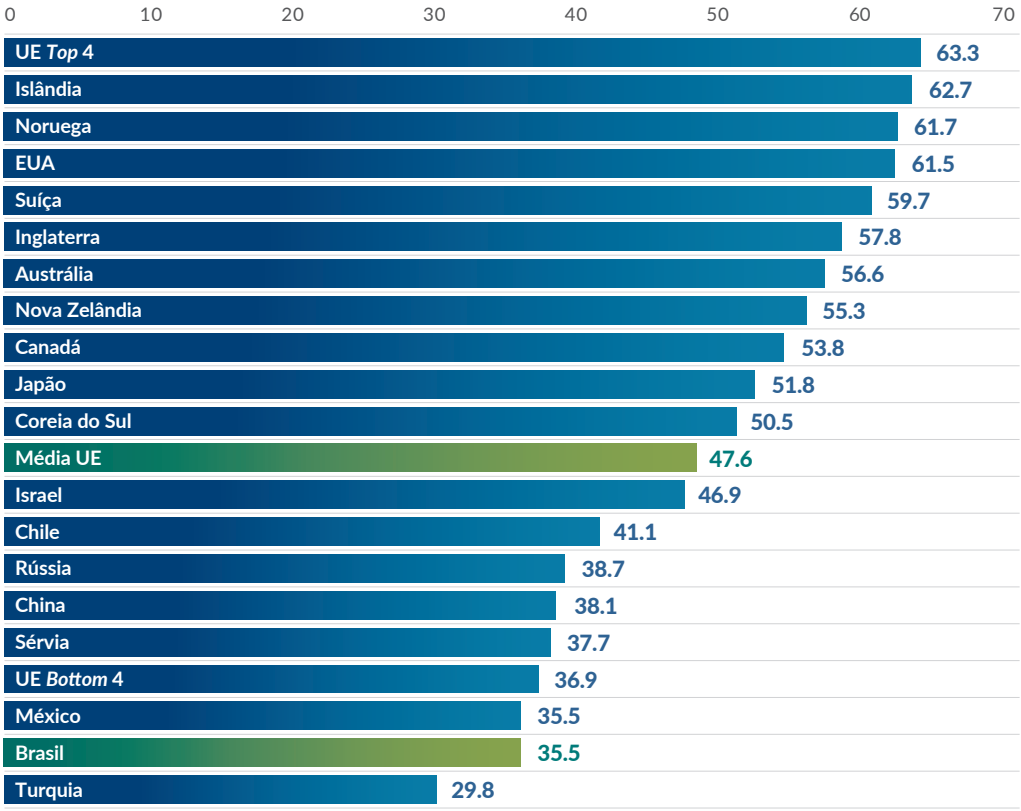
9. LEGISLATIVE PROPOSAL PL 4513/20, cf.: Projeto institui Política Nacional de Educação Digital - Notícias

10. EUROPEAN COMMISSION, 2020. The Digital Economy and Society Index. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/desi

11. Idem.

Em geral, a adoção digital aumentou notavelmente desde a adoção da estratégia do MUD em 2015. No entanto, existem discrepâncias entre os Estados-Membros e evidências de desigualdades na União, como mostra a figura 1. Ao comparar os 4 *top scored* da UE com a média, há uma diferença de mais de 15 pontos no índice, diferença ainda mais significativa se os 4 *bottom scored* da UE forem considerados. Ainda assim, os 4 Estados-Membros da UE de mais baixo *score*, tiveram uma pontuação melhor do que o Brasil, segundo a avaliação I-DESI de 2018.

FIGURA 1 - PONTUAÇÃO DO ÍNDICE DE ECONOMIA E SOCIEDADE DIGITAL (2018)



Fonte: Comissão Europeia, 2020[12].

12. EUROPEAN COMMISSION, 2020a. Shaping Europe's digital future REPORT. I-DESI 2020. Disponível em: I-DESI 2020: How digital is Europe compared to other major world economies? | Shaping Europe's digital future

O impulso na transição digital sob a Comissão de Juncker

Nas últimas décadas, a tecnologia e a internet transformaram o mundo cada vez mais rapidamente. A existência de barreiras *online* afeta diretamente os Estados-Membros da UE por se configurar falta de acesso a bens e serviços para os seus cidadãos, uma limitação para o desenvolvimento de novas empresas de alta tecnologia e a impossibilidade de colher certos benefícios da internet para empresas e governos. O problema foi mapeado pela Comissão de Barroso (2004-2014), com a criação de uma agenda digital inédita na União. Esta agenda se concentrou no amplo acesso à infraestrutura de banda larga e no aumento do volume de comércio eletrônico (*e-commerce*) transfronteiriço.

Diante disso, como presidente da Comissão Europeia de 2014 a 2019, Jean-Claude Juncker continuou a avançar com duas agendas de transição que já estavam ganhando vida internacional antes de sua chegada: a agenda verde e a digital. Juncker fazia promessas para revolucionar a economia e o mercado antes de iniciar seu mandato, dizendo que a economia deveria se tornar verde e o mercado digital. Num momento em que os países ainda se recuperavam da crise financeira e da dívida europeia, a criação de um MUD não foi encarada como uma questão urgente até que surgiram escândalos internacionais relacionados com a expansão da esfera digital[13] nos anos finais da Comissão de Juncker.

Além disso, um processo judicial na Corte de Justiça da União Europeia (CJUE) sobre o uso não autorizado de *cookies* de usuários pelo Facebook em 2015, com base em uma reclamação da Autoridade de Proteção de Dados da Bélgica, reforçou a urgência da agenda. A decisão da CJUE estendeu-se a outros gigantes da tecnologia como Twitter, Google e Apple e destacou como a Diretiva Europeia de Proteção de Dados existente (Diretiva 95/46 CE) de 1995 estava desatualizada e não abrangia a realidade trazida pela transformação digital e o crescimento da economia digital.

Juncker lançou um documento sobre a estratégia da UE para a transição digital. Tratou-se de um projeto em concordância com os valores e regras europeias para acompanhar a transformação digital em curso, visando prover uma internet aberta, justa, inclusiva e *people-centric*. Além disso, esta estratégia da Comissão teve como objetivo buscar soluções digitais como forma de criar novas oportunidades econômicas e de negócios em consonância com uma transição verde.

13. Como o escândalo da *Cambridge Analytica*.

Intitulada *Shaping Europe's digital future*, a estratégia é definida em três pilares como suporte de sua extensão: tecnologia que funciona para as pessoas; uma economia digital justa e competitiva; e uma sociedade aberta, democrática e sustentável[14]. A estratégia abrangia uma vasta gama de questões relativas à digitalização das sociedades europeias, mas a questão principal era a melhoria do *e-commerce* transfronteiriço na UE[15]. Na verdade, o novo documento repetiu objetivos previamente definidos em documento estratégico anterior, a ADE, mas cujos resultados estavam longe de ser satisfatórios. Essa estratégia deu origem ao MUD. De acordo com a Comissão, um MUD seria "aquele em que a livre circulação de pessoas, serviços e capitais é garantida e onde os indivíduos e empresas podem acessar e se envolver em atividades *online* em condições de concorrência leal e de um alto nível de proteção de dados pessoais e dos consumidores, independentemente da nacionalidade ou do local de residência"[16]. A estratégia foi construída sobre três pilares: acesso, meio ambiente e economia & sociedade.

Uma avaliação no meio termo da estratégia de MUD, em 2017, indicou várias realizações. No entanto, era conhecido o objetivo mais amplo da estratégia, ou seja, a consolidação do novo mercado verdadeiramente digital, que ainda não havia sido alcançado. E a realização deste objetivo seria a chave para o estabelecimento das condições propícias para o crescimento das empresas europeias. Naquele contexto, no entanto, o Regulamento da UE sobre Proteção de Dados, conhecido como RGPD (2016/679) foi considerado uma das legislações adotadas mais significativas da Comissão de Juncker, representando um marco nos direitos de privacidade do consumidor[17].

14. Para mais detalhes, cf: EUROPEAN COMMISSION Brussels, 19.2.2020 COM(2020) 67 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT.

15. EUROPEAN PARLIAMENT, 2019 (STUDY PE 631044, January 2019) MARCUS, J.S.; PETROPOULOS, G.; YEUNG, T., cf: Contribution to growth: The European Digital Single Market Delivering economic benefits for citizens and businesses

16. Cf. ref. Nota 3

17. Cf. ref. Nota 17

O RGPD da UE

A Comissão de Juncker teve as agendas digital e verde como prioridades. A criação de um MUD implicou políticas e iniciativas em diferentes frentes, tais como conectividade, compras, cultura, treinamento, inovação, *blockchain*, saúde, serviços públicos e confiança. De fato, para que muitas das iniciativas da estratégia do MUD fossem implementadas, era fundamental garantir a regulamentação da utilização de dados pessoais, definir padrões de privacidade de dados (*e-Privacy*) e lidar com as questões de segurança originadas no mundo digital (segurança cibernética).

Dados pessoais são toda e qualquer informação relacionada a uma pessoa, não apenas nome ou dados relativos ao endereço ou identificação, mas também perfis de usuários da internet, de compras, dados sobre vida financeira ou propriedade. Seja através do uso da internet, da identificação digital, das câmeras e de todo tipo de tecnologia cada vez mais sofisticada, os dados pessoais têm sido coletados e processados sem a devida atenção dos cidadãos ou processados sem a devida cautela por parte de instituições, empresas e até mesmo do poder público. A exposição excessiva de dados absolutamente sensíveis, não apenas pessoais em geral, mas também de saúde e econômicos, tornou-se um novo foco de preocupação e atenção em relação à segurança e economia.

A Diretiva de Proteção de Dados existente de 1995 afirmava o princípio da livre circulação de dados pessoais entre os Estados-Membros da UE, proibindo todos os tipos de restrições[18]. As "boas práticas" e "códigos de conduta" nas regras europeias de proteção de dados datavam da Diretiva, que estava em consonância com o objetivo da UE na década de 1990. No quadro jurídico da UE, as diretivas introduzem parâmetros e princípios a serem regulamentados pelos Estados-Membros. Naquele período, por exemplo, a Alemanha aprovou uma Lei Federal de proteção de dados apenas em 2001. Diversas outras normas estavam sendo aprovadas no país, trazendo algumas incertezas jurídicas sobre o tema. Hoje, os políticos na Alemanha parecem muito mais convencidos da importância da proteção de dados. Uma nova e sofisticada Lei alemã de proteção de dados foi adotada em maio de 2021, em convergência com o novo regulamento da UE e consolidando as regras anteriormente existentes sobre o assunto.

Uma transformação digital que passa a afetar a maneira como vivemos, trabalhamos, produzimos, nos comunicamos e fazemos compras se revelaria como uma nova *commodity* desde 2016. Prova disso foram os escândalos internacionais sobre o uso e transferência

18. CELESTE, Edoardo. 2021. "Cross-Border Data Protection After Brexit. Brexit Institute Working Paper Series, n. 4. Disponível em: Cross-Border Data Protection After Brexit by Edoardo Celeste :: SSRN

de dados pessoais do Facebook para a Cambridge Analytica e as preocupações com o processamento de dados, *e-Privacy* e sua relação com o marketing político[19]. Os dados ganham poder de influenciar eleições, interesses econômicos e elites. Embora tenha havido denúncias em anos anteriores, foi a partir de 2016[20] que a maioria das sociedades e governos ao redor do mundo perceberam que preferências e comportamentos políticos ou privados, influências e relações religiosas ou culturais, detalhes da vida pessoal registrados em fotos e vídeos nas redes sociais etc. foram processados sem o conhecimento de seus detentores. Assim, a garantia de proteção de dados envolve a proteção de direitos sobre a personalidade — considerados direitos fundamentais.

Embora o RGPD tenha começado a ser discutido na UE em 2012, só foi aprovado em 2016, sob a clara urgência de considerar os dados pessoais um novo foco para o Mercado Único Europeu (MUE). Desde 2011, as instituições da UE começaram a adotar iniciativas de governo eletrônico (*e-Government*), com estratégias para desenvolver instrumentos governamentais e políticos para a função da UE em serviços eletrônicos (*e-Services*) transfronteiriços e desenvolver soluções digitais para as formalidades de negócios, informações de segurança social e todos os tipos de potencial eletrônico e digital para *e-Consultation*, *e-Information*, e *e-Decision-making*. Esta ambição também faz parte do *Digital Europe Programme* lançado para o período 2021-2027.

Desde maio de 2018, o novo regulamento da UE entrou em vigor com o objetivo de corresponder ao cenário tecnológico do século 21 e facilitar os negócios, esclarecendo as regras e os direitos fundamentais dos indivíduos em sistemas nacionais de proteção de dados fragmentados na UE. O pacote de proteção de dados adotado em maio de 2016 foi inicialmente concebido para proteger a privacidade das pessoas na UE; ao mesmo tempo, representou melhores condições para continuar a desenvolver o potencial do *e-Government* e da *e-Economy* (governo e economia digitais). A complexidade da transição digital tornou-se rapidamente evidente, e o RGPD entrou em vigor em maio de 2018 para adequar os europeus à era digital. O RGPD inclui um pacote de iniciativas, como a criação de um Comitê Europeu para a Proteção de Dados e uma Autoridade Europeia para a Proteção de Dados, que foram complementares à preparação da era digital do mercado da UE. Os supervisores europeus e locais já vem aplicando multas para controladores e processadores que não cumpram a regulamentação[21].

Hoje em dia, a legislação de proteção de dados da UE permite o fluxo irrestrito de dados pessoais dentro do Espaço Econômico Europeu (EEE),[22] incluindo os Estados-Membros da UE, Noruega, Islândia e Liechtenstein. Ela também descreve as regras e os casos limitados para

19. Para mais detalhes, cf.: Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (Published 2018)

20. O ano da votação do referendo que aprovou o Brexit.

21. Para mais detalhes sobre multas por país membro do EEE, cf.: GDPR Enforcement Tracker - list of GDPR fines

22. O Acordo do EEE, que entrou em vigor em 1994, reúne os países da UE e três países membros do *European Free Trade Agreement* (EFTA). O EFTA inclui a Noruega, Islândia, Liechtenstein e Suíça. Foi criado com o objetivo de estender as disposições de livre comércio do MUE a não membros.

a transferência internacional de dados pessoais. Isto é particularmente importante porque 90% dos dados da União são armazenados fora do continente[23]. Aspectos importantes do RGPD foram os princípios de limitação da finalidade e minimização de dados, referindo-se à coleta de dados para uma finalidade específica, explícita e clara, além de limitada ao que é necessário para os fins em que os dados são processados, conforme estabelecido no artigo 5º do Regulamento.

23. Cf. ref. Nota 1

A LGPD brasileira

Na esteira do RGPD, o Brasil abriu uma ampla discussão sobre um arcabouço jurídico brasileiro para o tema. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709 foi aprovada em 14 de agosto de 2018, tendo entrado em vigor em 2020. No entanto, a vigência dos artigos relativos às suas sanções foi adiada, passando a vigorar a partir de 1º de agosto de 2021. A LGPD foi inspirada na legislação da UE, especialmente na definição de "dados pessoais". Atualmente, as atividades privadas e públicas trabalham com a utilização de dados de pessoas jurídicas e privadas, portanto, as bases, definições de expressões e princípios, bem como práticas de aplicação de dados foram determinadas pela legislação nacional.

Historicamente, podemos comentar os avanços brasileiros em proteção de dados antes mesmo da LGPD. A partir de 2010, deu-se início ao tratamento da proteção de dados e surgiram as primeiras legislações relacionadas ao assunto: a Lei de Acesso à Informação (Lei nº 12.527 / 2011) e a Lei Carolina Dieckmann (Lei nº 12.737 / 2012), relacionadas à acesso à informação e criminalização da obtenção de dados pessoais por meio de dispositivos eletrônicos. A aceleração do Marco Civil da Internet com debates públicos sobre o assunto levou à aprovação da Lei n.º 12. 965/2014, que entrou em vigor em junho do mesmo ano.

A LGPD prevê o tratamento de dados pessoais, inclusive em meio digital, por pessoa física ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade de pessoas naturais. Neste contexto, uma das grandes inovações trazidas pelo RGPD, não previstas na anterior Diretiva 95/46 CE, é o denominado "princípio da responsabilização", que também foi incorporado pela LGPD (artigo 6.º). O princípio da responsabilização se refere mais diretamente à possibilidade de um determinado ator ou pessoa ser responsabilizado por sua conduta. A inclusão do princípio visava obrigar os Estados-Membros a atribuir responsabilidades para assegurar *compliance* das atividades do controlador com os demais princípios de proteção de dados estabelecidos.

TABELA 1 - SEMELHANÇAS ENTRE O RGPD DA UE E O LGPD BRASILEIRO NO QUE SE REFERE AOS DIREITOS E À BASE LEGAL DE PROCESSAMENTO DE DADOS

	RGPD	LGPD
DEFINIÇÃO DE DADOS PESSOAIS	ARTIGO 4	ARTIGO 5
	Qualquer informação relativa a uma pessoa natural "identificada" ou "identificável" ('data subject'). Uma pessoa natural "identificável" é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um "identificador", como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos referentes a características física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.	Quaisquer dados relativos a uma pessoa natural que, por si só ou em combinação com outros dados, possam identificar a pessoa ou ser submetido a um processamento/tratamento específico.
DIREITOS DA PESSOAL NATURAL 'DATA SUBJECT'	ARTIGOS 12-23 (CAPÍTULO 3)	ARTIGO 18
	Informação, comunicação e modalidades transparentes para o exercício de seus direitos;	Direito à confirmação da existência do tratamento de dados;
	Quando os dados pessoais do titular são coletados devem existir informações claras sobre a identidade e detalhes de contato do controlador, Autoridade de Proteção de Dados, finalidades de processamento, localização, interesse legítimo e outras informações relacionadas ao processamento de dados;	Direito à informação sobre a possibilidade de negar o consentimento e as consequências dessa negação;
	Quando os dados pessoais não são coletados diretamente do titular de dados, devem existir informações claras sobre a identidade e detalhes de contato do controlador, Autoridade de Proteção de Dados, finalidades de processamento, localização, interesse legítimo e outras informações relacionadas ao processamento de dados;	Direito à informação sobre entidades públicas e privadas com as quais o controlador compartilha dados;
	Direito de acesso da pessoa natural titular dos dados (data subject);	Direito de acesso aos dados;
	Direito à retificação;	Direito de corrigir dados incompletos, imprecisos ou desatualizados;
	Direito de apagar / ser esquecido;	Direito de apagar dados pessoais processados com o consentimento do titular de dados;
	Direito de restrição de processamento;	Direito ao anonimato, podendo bloquear ou excluir dados desnecessários ou excessivos ou dados que não estão sendo processados segundo o compliance da LGPD;
	Direito à portabilidade dos dados;	Direito à portabilidade dos dados para outro prestador de serviços ou produtos, mediante solicitação expressa;
	Direito de objeção;	Direito de revogar o consentimento;
	Obrigação de notificação relativa à retificação, eliminação ou restrição;	
	Tomada de decisão individual automatizada, incluindo criação de perfis (direito de não estar sujeito a uma decisão baseada apenas em processamento automatizado);	
BASE LEGAL PARA PROCESSAMENTO DE DADOS	ARTIGO 6	ARTIGO 7
	Consentimento do titular de dados (data subject);	Consentimento do titular de dados (data subject);
	Para cumprir as obrigações legais;	Para cumprir as obrigações legais ou regulamentares;
	Desempenhar funções de interesse público ou no exercício de autoridade oficial investida no controlador;	Executar políticas públicas previstas em leis ou regulamentos, ou com base em contratos, acordos ou instrumentos semelhantes;
	Para cumprir os interesses legítimos do controlador ou de terceiros, exceto quando tais interesses sejam anulados pelos interesses ou direitos e liberdades fundamentais do titular de dados que requeira a proteção dos dados pessoais, em particular quando o data subject é uma criança;	Para cumprir os legítimos interesses do controlador ou de terceiros, exceto quando prevalecem os direitos e liberdades fundamentais do titular de dados, que requerem proteção de dados pessoais;
	Para executar um contrato do qual o titular de dados seja parte ou para tomar medidas a pedido do data subject antes de celebrar um contrato;	Executar um contrato ou procedimentos preliminares relacionados com um contrato do qual o titular de dados seja parte, a pedido do titular de dados ;
	Para proteger os interesses vitais do titular de dados ou de outra pessoa natural;	Para proteger a vida ou a segurança física do titular de dados ou de terceiros;
		Proteger a saúde, em procedimento realizado por profissionais de saúde ou por entidades de saúde;
		Exercer direitos em procedimentos judiciais, administrativos ou arbitrais;
		Realizar estudos por entidades de investigação que garantam, sempre que possível, o anonimato dos dados pessoais;
		Para proteger a pontuação de crédito (credit score).
MULTAS	ARTIGO 83	ARTIGO 52
	As multas chegam a € 20 milhões ou 4% da receita global anual, o que for maior.	As multas chegam a 2% da receita de pessoa jurídica privada, grupo ou conglomerado no Brasil, no exercício fiscal anterior, sem impostos, até um máximo total de R$ 50 milhões.

Fonte: Elaboração das autoras com base nos textos legislativos do RGPD da UE e na LGPD brasileira.

A Tabela 1 ilustra uma comparação entre o RGPD da UE e a LGPD brasileira no que diz respeito aos direitos e à base legal de processamento de dados. É possível notar como a legislação brasileira se inspirou no que tem sido feito na UE em relação ao RGPD, ainda que existam diferenças. Por um lado, o RGPD da UE visa ser muito preciso na definição da base jurídica para o tratamento de dados e dar à pessoa natural titular dos dados (*data subject*) o máximo de informação e o direito de escolher livremente por consentir o acesso de seus dados pessoais. Por outro lado, a LGPD brasileira é mais ampla na legalidade do processamento de dados pessoais — prevê dez justificativas em contraste com as seis do RGPD. A LGDP permite o processamento de dados pessoais de saúde; procedimentos judiciais, administrativos ou de arbitragem; pontuação de crédito, ou fins de pesquisa, sem uma restrição precisa das necessidades. No entanto, embora isso deixe muito espaço para a discricionariedade do controlador e do processador para justificar o tratamento de dados, surge a necessidade de apresentar os fundamentos para o mesmo no caso de uma consulta do supervisor. Outra diferença entre as duas leis diz respeito à magnitude máxima das multas a serem aplicadas.

São ainda necessárias normas para se regulamentar as novas maneiras de viver e fazer negócios na nova era digital. Os Estados-Membros da UE chegaram a um acordo sobre uma proposta de legislação para *ePrivacy* em fevereiro de 2021, durante a Presidência portuguesa do Conselho da UE. O Regulamento para a *ePrivacy* visa substituir a Diretiva sobre Privacidade e Comunicações Eletrônicas (Diretiva 2002/58 / CE)[24] para padronizar a utilização de serviços de comunicação eletrônica na UE. Originalmente, pretendia-se que tal Diretiva entrasse em vigor junto com o RGPD, em maio de 2018. No entanto, as negociações sobre os vários projetos não haviam sido bem-sucedidas e ainda não havia consenso total.

Regular o tratamento de dados pessoais foi um passo fundamental para a adaptação dos sistemas jurídicos ao mundo digital, algo que o Brasil e a UE conquistaram até agora. Outras medidas são esperadas em ambos os lados do Atlântico na próxima década. A questão é se o ritmo deles continuará a ser comparável.

24. Para mais detalhes, cf.: Key content of the ePrivacy Regulation

CEBRI
BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

EUROPE PROGRAM

Brief focus on Europe

DIGITAL TRANSFORMATION AND DATA PROTECTION:

THE EU GENERAL DATA PROTECTION REGULATION (GPDR) AND THE BRAZILIAN GENERAL PERSONAL DATA PROTECTION LAW (LGPD)

September, 2021

Digital transition in the EU

The world is changing, and the digital sphere has gained a lot of space over the last decades, creating thus another layer of complexity in human relations and rights. The 21st century has brought along changes of such magnitude. Digital technologies are transforming our world: mobile internet access, social media, e-Commerce, internet security, cloud services and digital skills — it is the onset of the Digital Age brought about by the Digital Revolution. The diffusion of digital technologies is present in nearly every business, societies and world of work, and the Covid-19 pandemic worked as a turning point in accelerating the digital transformation on an unprecedented scale.

In the face of the changes brought about by digital technologies, the European Union (EU) has been adapting its single market to make it fit for the digital age by creating standards and a level playing field for the activities in this new sphere. The Commission's first European Digital Agenda (EDA) was created in the mid-term of José Manuel Barroso's Presidency of the EU Commission (2004-2014) and focused on providing wide access to broadband infrastructure, particularly for rural and underdeveloped regions, and increasing the volume of cross-border e-Commerce, which was exceptionally low[25].

The EDA had a more limited scope but set the background for the creation of the Digital Single Market (DSM) strategy. Adopted in May 2015, the DSM strategy is one of the European Commission's ten priorities[26]. The strategy aimed at improving access to the online world to individuals and businesses by creating a level playing field for digital networks and services to maximize the growth potential of the digital economy within the Union[27].

The DSM has been built upon numerous legislative measures, such as directives and regulations, which we will outline in this article and particularly the EU General Data Protection Regulation (GDPR). The GDPR influenced Brazil and several other countries, such as Japan, South Korea, Chile, and Argentina to adopt concepts and similar rules, reinforcing the EU's ability to spread norms and act as a regulatory world actor.

---

25. MAKOWSKA, Marta. 2020. The Challenges of Making the EU fit for the Digital Age. PISM Policy Paper n. 4 (179) The Polish Institute of International Affairs. Available at: The Challenges of Making the EU Fit for the Digital Age

26. For more details, see EUROPEAN COMMISSION: EUROSTAT: Overview - Digital economy and society - Eurostat

27. EUROPEAN COMMISSION, 2021. Shaping Europe's digital future, Available at: Shaping Europe's digital future | Shaping Europe's digital future

The existence of a digital single market puts into question the traditional way of thinking about its four freedoms. The importance of the free circulation of goods, capital, people, and services can be better understood when we unpack the detailed implications of regulations and legal harmonization among the Member States. There is a huge impact on the region, including border control, institutional innovation, and the economic life of citizens living in the new internal market — of a regional character. The guarantee of the four freedoms will depend more on the digital transition than on physical limitations to the circulation within the Member States. This is because current barriers are no longer physical, they are of knowledge, skills, and technology. The future of the EU will depend on its potential to transform its single market and make it fit for the Digital Age. According to analysts, in addition to creating thousands of jobs, it would contribute to the EU economy €415 billion per year[28]. In order for the EU to maintain its international role as a setter of standards regarding technological development and digital transformation and aligned with European values, it had to take it as a priority.

A digital economy and the new ambition to create the DSM address clearly democratic rights and freedoms of people. Due to the fragmentation of the impacts of this type of market on the European citizens' daily life, such as the new workplace, the right to privacy, the use of e-Commerce mechanisms, etc., we see a direct relationship with the individual rights protection. This is so not only for European citizens who are already part of the EU Single Market but also for individuals who could circulate or integrate activities related to the DSM remotely — which is characteristic of the fluidity of the digital age in social life.

28. BOBAN, M. 2016. "Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world". Economic and social development. 16 International Scientific Conference on Economic and Social Development. The Legal Challenges of Modern World. 1-2 September, 2016, p.191.

Why does information matter?

One important distinction needs to be clarified: the difference between data and information. Not without first remembering that Big Data regards a very large volume of data accumulated in computers, clouds or any other form of data storage through digital means.

Data is information that is not processed or treated. It is usually stored on a computer, cloud or other data storage source. Information in this context refers to the processed data, which becomes known, whether by classification, organization or documentation. Thus, personal data protection becomes as or more relevant than the protection and access to personal information[29].

In a technological condition and with great computational capacity, the expansion of data processing instruments brings a new concern with the accumulation and possibility of collecting and processing such data.

The technological transformation that now allows the handling and processing of Big Data, associated with the increase in the situation in which consumers access virtual commerce mechanisms or simply use computers and platforms that record personal data, generates risks for data owners and new ways of unethical or even illegal use of other people's data.

The relevance of data protection hits debates on both economy and democracy. The digital economy permeates two levels of rights and demands of protection: on the one hand, the economic elites with its business interests, and on the other, the individuals, which are both citizens and consumers. It regards the exercise of individual rights on data, reputation, anonymity, privacy, liberty and information protection for consumers.

29. TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (Eds). 2019. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters. Revista dos Tribunais.

Digital Economy

The Digital Revolution has altered the patterns of production and behaviour, as did the Industrial Revolution, changing the logic from the traditional industry based on the scarcity of resources to an economy based on information, computerization and knowledge. Under the accelerating pace in the field of data storage and processing, with abundant information and knowledge, the challenge is one of optimization: to use them in a relevant manner. The Digital Age brings about a change in scope, frontiers and challenges for individuals, businesses, and the economy as a whole.

The diffusion of digital technologies in the different spheres of our lives has led to the creation of a digital economy. The digital economy consists of the economic activity from billions of everyday online connections among people, businesses, processes, devices, and data[30]. The change in the economy and business, however, is in the context of a transformation of the societies, in relationships, in the build of preferences and opinions, in the search for information, communication, and more recently — that is, in the context of the Covid-19 pandemic, a change in the world of work. Understanding this transformation takes time and knowledge.

Hyperconnectivity was already perceived as the backbone of the digital economy. Although the EU has been conducting its digital policy for many years, it is better known as a regulatory superpower than a high-tech economy. In the United States (U.S.) case, the high-tech potential is notorious, and we can find research that looks for a better understanding of the new digital age impacting the North-American society and workforce.

A report published by the Brookings Institution[31] presents a detailed analysis of changes in the digital content of 90 percent of the U.S. workforce in all industries between 2001-2017. The research categorized occupations into jobs that require high, medium or low digital skills and tracked the impacts of rapid change. One of the interesting conclusions is the lack of sufficient information on the spread of digital adoption in the world of work, which would help to map the level of transformation and a more precise degree of change. The report concludes, among other things, the digitalization requires significant improvements in digital education and high skills.

30. DELOITTE. 2021. What is digital economy? Unicorns, transformation and the internet of things. 2021 Malta Technology Leadership Survey. Available at: What is digital economy?

31. For more details, see: Brookings Report Digitalization and the American workforce

In fact, digital education and training are one of the areas the EU has been targeting since 2015, while creating new race- and gender-based access challenges. Under the new Presidency and the context of the pandemic situation, the Commission published a new Digital Education Action Plan (2021-2027), which is a renewed EU policy initiative to support the sustainable and effective adaptation of the education and training systems of EU Member States to the digital age. The two priority areas of the Action Plan are fostering the development of a high-performing digital education ecosystem and enhancing digital skills and competences for the digital transformation[32].

Brazilian parliamentarians have also understood digital literacy and training is the right way forward in this 21st century. A legislative bill was proposed in September 2020 for a National Digital Education Policy[33]. The proposal comprises initiatives on education but also digital inclusion, labour market qualification, increase in employability, and digital research.

Under the EU's digital agenda priority, the Union created the Digital Economy and Society Index (DESI). It is an index aimed at monitoring Europe's overall digital performance and tracking the progress of EU countries in digital competitiveness. The index has **five dimensions** in its structure to assess the overall aspects of digitalization: **connectivity**; **human capital**; **use of the internet**; **integration of digital technology**; **digital public services**[34]. **Connectivity** concerns digital infrastructure, the access to a fast and reliable broadband connection, both fixed and mobile. It is key for the delivery of societal and economic services in a digital economy. **Human capital** regards the set of skills needed to access the digital world, and it is the backbone of the digital society: in order to engage in digital activities from scheduling an appointment, shopping or working, one needs the skills to do so.

The **use of the internet** refers to the internet use by individuals, which has been growing since 2015. As for businesses, the **integration of digital technologies** relates to businesses going digital in their way of work, communication and sale (such as the case of e-Commerce). Finally, **digital public services** refer to the quality and usage of digital resources and solutions in the provision of public services. The recent pandemic scenario has highlighted the importance of ensuring the continuation of the provision of public services in spite of the social distancing and lockdown measures. Nonetheless, according to the DESI 2020 report, there had been an improvement in the quality and usage of digital public services in 2019, prior to the pandemic and as a consequence of the DSM strategy[35].

Overall, digital adoption has increased notably since the adoption of the DSM strategy in 2015. However, discrepancies among Member States exist and evidence inequalities within the Union, as figure 1 shows. When comparing EU Top 4 to the EU average, there

32. For more details, see EUROPEAN COMMISSION, 2021, see: Digital Education Action Plan (2021-2027) | Education and Training

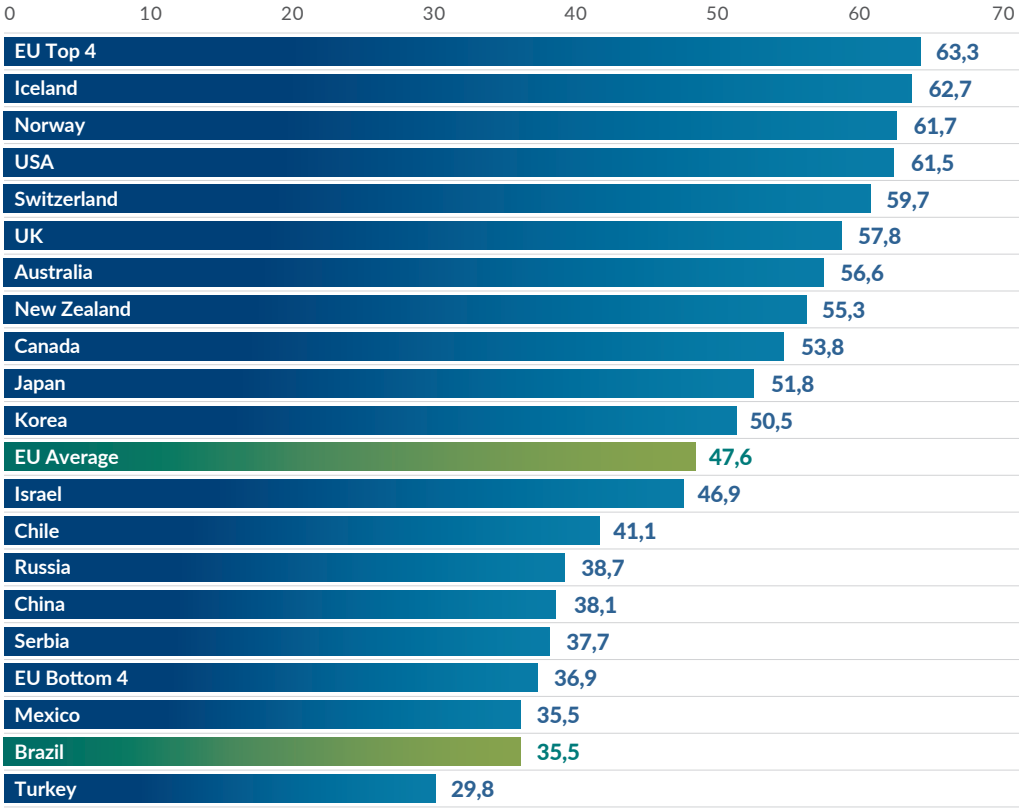
33. LEGISLATIVE PROPOSAL PL 4513/20, see: Projeto institui Política Nacional de Educação Digital - Notícias

34. EUROPEAN COMMISSION, 2020. The Digital Economy and Society Index. Available at: https://digital-strategy.ec.europa.eu/en/policies/desi

35. Idem.

is a gap of over 15 points in the score, and it is even more significant if the EU Bottom 4 are considered. Still, the EU Bottom 4 have scored better than Brazil in the 2018 I-DESI assessment.

FIGURE 1 - DIGITAL ECONOMY AND SOCIETY INDEX SCORE (2018)



Source: European Commission, 2020[36].

36. EUROPEAN COMMISSION, 2020a. Shaping Europe's digital future REPORT. I-DESI 2020. Available at: I-DESI 2020: How digital is Europe compared to other major world economies? | Shaping Europe's digital future

The boost on digital transition under Juncker's Commission

Over the past decades, technology and the internet have been transforming the world more and more rapidly. The existing online barriers directly impact EU Member States in the form of a lack of access to goods and services for its citizens, a limitation for high technology start-ups to thrive, and the impossibility to reap certain benefits from the internet for businesses and governments. The problem had been mapped under Barroso's Commission (2004-2014), with the creation of a first-ever digital agenda in the Union. It focused on wide access to broadband infrastructure and increasing the volume of cross-border e-Commerce.

In light of that, as president of the European Commission from 2014 to 2019, Jean-Claude Juncker pushed forward two transition agendas that were already coming to life internationally before his arrival: the green and the digital agendas. Juncker was casting promises to revolutionize the economy and the market before beginning his mandate, saying the economy should become green and the market digital. In a moment where countries were still recovering from the financial crisis and the European debt, the creation of a DSM was not seen as an urgent matter until international scandals related to the expansion of the digital sphere[37] came to life in the final years of the Juncker's Commission.

In addition, a judicial case at the Court of Justice of the European Union (CJEU) on the unauthorized use of users' cookies by Facebook in 2015 based on a complaint by the Belgium Data Protection Authority has reinforced the urge of the agenda. The CJEU's decision extended to other tech giants like Twitter, Google and Apple and highlighted how the existing European Data Protection Directive (Directive 95/46 EC) from 1995 was outdated and did not cover the reality brought about by the digital transformation and the growing digital economy.

Juncker launched a EU's strategy for the EU's digital transition. It was aimed as a European project according to European values and rules to catch up with the digital transformation in place. At the same time, it envisaged an open, fair, inclusive and people-centred internet in a digital transition,[38] this strategy aimed to seek digital solutions as a way to create new economic and business opportunities in line with a green transition.

37. Such as the *Cambridge Analytica* scandal.

38. Cf. ref. note 3

Called “Shaping Europe’s digital future”, the strategy is set under three pillars to support its approach: technology that works for the people, a fair and competitive digital economy, and an open, democratic, and sustainable society[39]. The strategy comprised a broad range of issues concerning the digitisation of European societies, but the key issue was the improvement in cross-border electronic commerce within the EU[40]. It did indeed repeat many goals previously set out in the previous strategy, the EDA, but which outcomes were far from satisfactory. This strategy originated the DSM. According to the Commission, a DSM would be “one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence”[41]. The strategy was built on three pillars: access, environment, and economy & society.

The mid-term review of the DSM strategy in 2017 indicated several accomplishments. However, it was known the overarching aim of the strategy, that is, a truly digital single market was yet to be achieved. And the achievement of the strategy’s main objective was key to create the proper conditions for European companies to grow. Nonetheless, the EU Regulation on Data Protection, well known as the GDPR (2016/679), adopted in 2016, was considered one of the most significant adopted legislation during the Juncker’s Commission, representing a landmark in terms of consumer privacy rights[42].

39. For more details, see: EUROPEAN COMMISSION Brussels, 19.2.2020 COM(2020) 67 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT.

40. EUROPEAN PARLIAMENT, 2019 (STUDY PE 631044, January 2019) MARCUS, J.S.; PETROPOULOS, G.; YEUNG, T., see: Contribution to growth: The European Digital Single Market Delivering economic benefits for citizens and businesses

41. Cf. ref. note 3

42. Cf. ref. note 17

The EU GDPR

Juncker's Commission had the digital and the green agendas as priorities. The creation of a DSM implied policies and initiatives in different fronts such as connectivity, shopping, culture, training, innovation, blockchain, health, public services, and trust. In fact, in order to have many of the initiatives in the DSM strategy implemented, it was key to ensure the regulation of the use of personal data, set data privacy standards and deal with the security issues originated from the digital world (cybersecurity).

Personal data is any and all information related to a person, not just name or data relating to address or identification, but also profiles of internet usage, shopping, data about financial life or property. Whether through the use of the internet, digital identification, cameras and all kinds of increasingly sophisticated technology, personal data has been collected and processed without the necessary attention by the citizens or processed without enough caution by institutions, companies, and even by the Government. The excessive exposure of absolutely sensitive information, not only personal information in general but also concerning health and economic information, has become a new focus of concern and attention regarding security and economy.

The existing Data Protection Directive from 1995 affirmed the principle of free flow of personal data among the EU Member States, prohibiting all sorts of restrictions[43]. The "good practices" and "codes of conduct" in European data protection rules dated back to the Directive, which was in line with the EU objective in the 1990s. In the EU legal framework, directives introduce parameters and principles to be regulated by Member States. At that time, for example, Germany approved a federal data protection law in 2001 only. Several other rules were being approved in the country, bringing some legal uncertainties on the topic. Nowadays, the German political leaders look much more convinced about the importance of data protection. A new sophisticated German Data Protection Act was adopted in May 2021 in line with the new EU's Regulation and consolidating the previously existing rules on the matter.

A digital transformation that would affect the way we live, work, produce, communicate and shop would appear as a new commodity since 2016[44]. Evidence of that were the international scandals on the use and transfer of personal data from Facebook to Cambridge Analytica and the concerns on data processing and privacy and its relationship with political marketing[45].

43. CELESTE, Edoardo. 2021. "Cross-Border Data Protection After Brexit. Brexit Institute Working Paper Series, n. 4. Available at: Cross-Border Data Protection After Brexit by Edoardo Celeste :: SSRN

44. The year of the Brexit referendum.

45. For more details, see: Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (Published 2018).

Data becomes power and could influence elections, economic interests, and elites. Although there were denunciation from earlier years, it was after 2016 that most of the societies and governments around the world have realized that political or private preferences and behaviours, religious or cultural influences and relations, personal life details registered in photos and videos on social media etc. were processed without the knowledge of their holders. Thus, the request for data protection involves protecting rights over the personality — considered fundamental rights.

Although the GDPR started to be discussed in the EU in 2012, it was only approved in 2016, under the clear urgency to consider personal data a new focus for the ESM. Since 2011, the EU institutions started to adopt e-Government initiatives, with strategies to develop governmental and policy instruments to the EU function in cross border e-Services and develop digital solutions for the formalities of business, Social Security Information, and all kinds of potential for e-Consultation, e-Information, and e-Decision-making. This ambition is also part of the Digital Europe Programme launched for the 2021-2027 period.

Since May 2018, the new EU Regulation has entered into force aiming to correspond to the technological scenario of the 21st century and to facilitate business by clarifying rules and individuals' fundamental rights in fragmented national systems of data protection among the EU's Member States.

The EU Data Protection package adopted in May 2016 was first designed to protect people's privacy in the EU, at the same time, it could represent better conditions to continue to develop the e-Government potential and the digital economy. The complexity of the digital transition became quickly evident, and the GDPR came into force in May 2018 to fit Europeans for the digital age. The GDPR includes a package of initiatives, such as the creation of a European Data Protection Board (EDPB) and a European Data Protection Supervisor (EDPS), which were complementary to the preparation of the digital era of the EU market. The European and local supervisors have already been applying fines for controllers and processors non-compliant with the regulation[46].

Nowadays, EU data protection law allows the unhindered flow of personal data within the European Economic Area (EEA),[47] including the EU Member States, Norway, Iceland and Liechtenstein. It also outlines the rules and the limited cases for the international transfer of personal data. This is particularly important as 90% of the Union's data is stored outside of the continent[48]. Important aspects of the GDPR were the principles of purpose limitation and data minimization, referring to the collection of data for a specific, explicit, and clear purpose and limited to what is necessary for the purposes in which the data is processed, as stated in article 5 of the Regulation.

---

46. For more details about the fines per EEA countries, see: GDPR Enforcement Tracker - list of GDPR fines

47. The EEA Agreement, which entered into force in 1994, brings together the EU countries and three countries of the European Free Trade Agreement (EFTA). The EFTA includes Norway, Iceland, Liechtenstein, and Switzerland. It was created for the purpose of extending the free trade provisions of the ESM to non-members.

48. Cf. ref. note 1

The Brazilian LGPD[49]

In the wake of the GDPR, Brazil opened a wide discussion on a Brazilian legal framework for the topic. The General Personal Data Protection Law (LGPD), Law No. 13.709, was approved on August 14, 2018, and it entered into force in 2020. However, the articles relating to its sanctions were postponed, entered into force from August 1st, 2021 . The LGPD was inspired by the EU law, especially the definition of "personal data". Private and public activities currently work with the use of data from private and legal persons, thus, bases, definitions of expressions and principles, and practices of data application were determined by national legislation.

Historically we can remark on the Brazilian advances in data protection even before the LGPD. Since 2010, the beginning of the treatment of data protection and the first laws related to the subject emerged: the Access to Information Law (Law No. 12,527/2011) and the Carolina Dieckmann Law (Law No. 12,737/2012), related to access to information and criminalization of obtaining personal data through electronic devices. The acceleration of the *Marco Civil da Internet* with public debates on the subject led to the approval of Law No. 12 965/2014, which entered into force in June of the same year.

The LGPD provides for the processing of personal data, including in digital media, by a natural person or by a legal entity governed by public or private law, with the objective of protecting the fundamental rights of freedom and privacy and the free development of natural persons' personality. In this context, one of the great innovations brought by the GDPR not foreseen in the previous Directive 95/46 EC, is the so-called "principle of accountability", which was also incorporated by the LGPD (article 6). The principle of accountability refers more directly to the possibility of a certain actor or person being called into account for their conduct. The inclusion of the principle aimed to constrain the Member States to allocate responsibilities to ensure the compliance of the controller's activities with the other established data protection principles.

TABLE 1 - SIMILARITIES BETWEEN THE EU GDPR AND THE BRAZILIAN LGPD WHEN IT COMES TO THE RIGHTS AND THE LEGAL BASIS FOR PROCESSING DATA

49. In this article we will adopt the acronym in Portuguese, LGPD.

	GDPR	LGPD
DEFINITION OF PERSONAL DATA	ARTICLE 4	ARTICLE 5
	Any information relating to an *identified* or *identifiable* natural person (called the 'data subject'). An *identifiable* natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Any data related to a natural person that, by itself or combined with other data, could identify or subject him or her to a specific treatment.
DATA SUBJECT RIGHTS'	ARTICLES 12-23 (CHAPTER 3)	ARTICLE 18
	Transparent information, communication, and modalities for the exercise of its rights;	Right to confirmation of the existence of the processing;
	Where personal data are collected from the data subject, clear information on identity and contact details of the controller, Data Protection Officer (DPO), purposes of processing, location, legitimate interest and other information regarding the data processing must exist;	Right to information about the possibility of denying consent and the consequences of such denial;
	Where personal data are not collected from the data subject, clear information on identity and contact details of the controller, Data Protection Officer (DPO), purposes of processing, location, legitimate interest and other information regarding the data processing must exist;	Right to information about public and private entities with which the controller has shared data;
	Right of access by the data subject;	Right to access the data;
	Right to rectification;	Right to correct incomplete, inaccurate or out-of-date data;
	Right to erasure / to be forgotten;	Right to delete personal data processed with the consent of the data subject;
	Right to restriction of processing;	Right to anonymize, block, or delete unnecessary or excessive data or data that is not being processed in compliance with the LGPD;
	Right to data portability;	Right to the portability of data to another service or product provider, by means of an express request;
	Right to object;	Right to revoke consent;
	Notification obligation concerning rectification, erasure or restriction;	
	Automated individual decision-making, including profiling (right not to be subject to a decision based solely on automated processing);	
LEGAL BASIS FOR PROCESSING DATA	ARTICLE 6	ARTICLE 7
	Data subject consent;	Data subject consent;
	To comply with legal obligation;	To comply with legal or regulatory obligation;
	To perform a task carried out in the public interest or in the exercise of official authority vested in the controller;	To execute public policies provided in laws or regulations, or based on contracts, agreements, or similar instruments;
	To fulfill the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;	To fulfill the legitimate interests of the controller or a third party, except when the data subject's fundamental rights and liberties, which require personal data protection, prevail;
	To execute a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	To execute a contract or preliminary procedures related to a contract of which the data subject is a party, at the request of the data subject;
	To protect the vital interests of the data subject or another natural person;	To protect the life or physical safety of the data subject or a third party;
		To protect health, in a procedure carried out by health professionals or by health entities;
		To exercise rights in judicial, administrative or arbitration procedures;
		To carry out studies by research entities that ensure, whenever possible, the anonymization of personal data;
		To protect credit (referring to a credit score).
FINES	ARTICLE 83	ARTICLE 52
	Fines go up to €20 million or 4% of annual global revenue, whichever is higher.	Fines go up to 2% of a private legal entity's, group's, or conglomerate's revenue in Brazil, for the prior fiscal year, excluding taxes, up to a total maximum of R$50 million.

trates a comparison between the EU GDPR and the Brazilian LGPD, when it comes to the rights and the legal basis for processing data. It is possible to note how the Brazilian legislation

was inspired by what has been done in the EU regarding the GDPR, although differences do exist. On the one hand, the EU GDPR aims to be very precise at defining the legal basis for processing data and giving natural persons (the data subject) the maximum amount of information and the right to be its own man concerning and consenting the access to its personal data. On the other hand, the Brazilian LGPD is broader in the lawfulness of processing personal data — it foresees ten justifications in contrast with GDPR's six. The LGDP allows processing personal data on health; judicial, administrative, or arbitration procedures; credit scores, or research purposes, without a precise restriction on needs. However, although this leaves a lot of space for the discretion of the controller and the processor to justify its data processing, it comes with the need to present the fundamentals for it in case of an inquiry by the supervisor. Another difference among the two regulations concerns the maximum magnitude of the fines to be applied.

Nonetheless, further legislation is needed to regulate the living and doing business in the new digital era. The EU Member States have agreed upon a legislation for ePrivacy in February 2021, under the Portuguese EU Council presidency. The ePrivacy Regulation is aimed to replace the Directive on Privacy and Electronic Communications (Directive 2002/58/EC)[50] to standardise the use of electronic communications services within the EU. Originally, it was intended to enter into force together with the GDPR, in May 2018. However, the negotiations on the various drafts had not been successful, and full consensus was still to be achieved.

To regulate on processing personal data was an essential step towards adapting the legal systems to the digital world, something Brazil and the EU have achieved so far. Further steps are to be expected on both sides of the Atlantic in the next decade. The question is whether their pace will continue to be comparable.

50. For more details, cf.: Key content of the ePrivacy Regulation

Conselho Curador/ *Board*

Presidente/ *Chairman*
José Pio Borges

Presidente Emérito/ *Emeriti Chairman*
Fernando Henrique Cardoso

Vice-Presidentes/ *Vice Chairmen*
Jorge Marques de Toledo Camargo José
Alfredo Graça Lima
Tomas Zinner

Vice-Presidentes Eméritos/ *Vice Chairmen Emeriti*
Daniel Klabin
José Botafogo Gonçalves
Luiz Augusto de Castro Neves
Rafael Benke

Conselheiros Eméritos/ *Trustees Emeriti*
Luiz Felipe de Seixas Corrêa
Luiz Fernando Furlan
Marcos Azambuja
Pedro Malan
Rubens Ricupero

Fundadores/ *Founders*
Carlos Mariani Bittencourt
Celso Lafer
Daniel Klabin
Gelson Fonseca Jr.
João Clemente Baena Soares
Marcus Vinicius Pratini de Moraes
Maria do Carmo (Kati) Nabuco de Almeida Braga
Roberto Teixeira da Costa
Eliezer Batista da Silva *(in memoriam)*
Luciano Martins de Almeida *(in memoriam)*
Luiz Felipe Palmeira Lampreia *(in memoriam)*
Luiz Olavo Baptista *(in memoriam)*
Sebastião do Rego Barros Netto *(in memoriam)*
Walter Moreira Salles *(in memoriam)*

Diretora-Presidente/ *CEO*
Julia Dias Leite

Conselheiros/ *Board of Trustees*
André Clark
Anna Jaguaribe
Armando Mariante
Armínio Fraga
Clarissa Lins
Claudio Frischtak
Demétrio Magnoli
Edmar Bacha
Henrique Rzezinski
Ilona Szabó
Izabella Teixeira
Joaquim Falcão
José Aldo Rebelo
José Luiz Alquéres
Luiz Ildefonso Simões Lopes
Marcelo de Paiva Abreu
Marcos Galvão
Paulo Hartung
Renato Galvão Flôres Jr.
Roberto Abdenur
Roberto Jaguaribe
Ronaldo Veirano
Sergio Amaral
Vitor Hallack
Winston Fritsch

Conselho Consultivo Internacional

International Board

Albert Fishlow
Alfredo Valladão
André Corrêa do Lago
Antonio Patriota
Felix Peña
Flávio Damico
Jackson Schneider
Leslie Bethell
Marcos Caramuru
Marcos Jank
Monica de Bolle
Sebastião Salgado

Senior Fellows

Adriano Proença
Ana Célia Castro
Ana Paula Tostes
Ana Toni
André Soares
Benoni Belli
Carlos Milani
Daniela Lerda
Denise Nogueira Gregory
Diego Bonomo
Evangelina Seiler
Fabrizio Sardelli Panzini
Fernanda Magnotta
Hussein Kalout
Larissa Wachholz
Lia Valls Pereira
Lourival Sant'anna
Mário Ripper
Matias Spektor
Miguel Correa do Lago
Monica Herz
Patrícia Campos Mello
Paulo Sergio Melo de Carvalho
Pedro da Motta Veiga
Philip Yang
Ricardo Ramos
Ricardo Sennes
Rafaela Guedes
Rogerio Studart
Ronaldo Carmona
Sandra Rios
Tatiana Rosito
Vera Thorstensen
Victor do Prado

Associados
Members

Instituições/ *Institutions*

Abiquim
Aegea
Altera
BAMIN
Banco Bocom BBM
BASF
BAT Brasil
BDMG
BMA Advogados
BNDES
BRF
Bristow
Brookfield Brasil
Captalys Investimentos
CCCC/Concremat
COMERC Energia
Consulado Geral dos Países Baixos no Rio de Janeiro
Consulado Geral da Irlanda em São Paulo
Consulado Geral do México no Rio de Janeiro
Consulado Geral da Noruega no Rio de Janeiro
CTG Brasil
Dannemann, Siemsen, Bigler & Ipanema Moreira
Dynamo
EDP
Eletrobras
Embaixada da China no Brasil
Embaixada da República da Coreia
ENEVA
ENGIE Brasil
Equinor
ExxonMobil
FCC S.A.
Grupo Lorentzen
Grupo Ultra
Huawei
IBÁ
IBRAM
Icatu Seguros
Itaú Unibanco
JETRO
Klabin
Lazard
Light
Mattos Filho Advogados
Michelin
Museu do Amanhã
Neoenergia
Oktri Empreendimentos
Paper Excellence
Petrobras
Pinheiro Neto Advogados
Prumo Logística
Repsol Sinopec
Sanofi
Santander
Shell
Siemens Energy
SPIC Brasil
State Grid
Suzano
Tecnoil
Total E&P do Brasil
Vale
Veirano Advogados
Vinci Partners

Equipe CEBRI
CEBRI Team

Diretora-Presidente / *CEO*
Julia Dias Leite

Diretora de Projetos / *Director of Projects*
Luciana Gama Muniz

Diretora de Relações Institucionais e Comunicação /
Director of Institutional Relations and Communications
Carla Duarte

Projetos
Projects

Gerente de Projetos / *Projects Manager*
Marianna Albuquerque

Coordenador de Projetos / *Projects Coordinator*
Hugo Bras Martins da Costa

Analista de Projetos / *Projects Analyst*
Gustavo Berlie

Estagiários / *Interns*
Larissa Vejarano
Lucas Cabral
Rafaela Machado Cândido
Sofia da Silva Urech

Relações Institucionais
Institutional Relations

Coordenadora de Parcerias /
Partnerships Coordinator
Cintia Hoskinson

Coordenadora de Relações Institucionais
Institutional Relations Coordinator
Fernanda Araripe

Coordenador de Projetos Especiais /
Special Projects Coordinator
Caio Vidal

Analista de Projetos Especiais /
Special Projects Analyst
Lucas Bilheiro

Estagiário / *Intern*
Heron Fiório

Comunicação e Eventos
Communications and Events

Gerente de Comunicação e Eventos /
Communications and Events Manager
Betina Moura

Coordenadora de Eventos / *Events Coordinator*
Nana Villa Verde

Coordenadora de Comunicação Institucional /
Institutional Communication Coordinator
Renata Fraga

Analistas de Comunicação /
Communication Analysts
Natasha Mastrangelo
Paula Reisdorf

Analista de Eventos / *Events Analysts*
Julia Felipe Mendonça Cordeiro
Nana Maria Barbosa

Secretária Executiva / *Executive Secretary*
Rigmor Andersen

Administrativo e Financeiro
Administrative and Financial

Coordenadora Adminstrativa-Financeira /
Administrative-Financial Coordinator
Fernanda Sancier

Analista Admistrativo / *Assistant*
Kelly C. Lima

CEBRI

CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS

Rua Marquês de São Vicente, 336
Gávea, Rio de Janeiro – RJ - Brasil
22451-044

Tel: +55 (21) 2206-4400

cebri@cebri.org.br

@cebrionline **cebri.org**