4ª COMPUTERS, PRIVACY AND DATA PROTECTION CONFERENCE LATAM | 17-18 JULY 2024 | FGV, RJ, BRAZIL

CPDP LATAM 2024

OUTCOME REPORT

INTRODUÇÃO

CPDP LatAm 2024: Construir a governança de dados de maneira soberana e sustentável, da América Latina ao G20

Luca Belli, Nicolo Zingales, Walter Britto Gaspar

Nos dias 17 e 18 de julho, aconteceu a quarta edição da Computers, Privacy and Data Protection Conference Latin America (CPDP LatAm), conferência que se estabeleceu como a principal – e única – plataforma para debates multissetoriais sobre governança de dados na América Latina. Considerando a presidência brasileira do G20 em 2024, o encontro foi dedicado à "Governança de dados: Da América Latina ao G20" e foi organizado como evento paralelo oficial do T20, o grupo de think tanks do G20.

O evento ofereceu uma oportunidade única de reunir perspectivas variadas dos maiores especialistas da região latino-americana e dos países do G20 a respeito da proteção de dados, tendo um objetivo duplo: debater como os desafios globais estão impactando a América Latina e o Brasil e, de outro lado, como as propostas, ideias e soluções latino-americanas podem impactar os debates globais.

Para alcançar esses ambiciosos objetivos, o evento contou com duas sessões plenárias e 27 sessões organizadas ao longo de dois dias, e foi seguido de um *side event* dedicado à "Soberania Digital no G20", no dia 19 de julho. O evento incluiu também um *keynote* de Max Schrems, fundador da organização NOYB - *European Center for Digital Rights*, conhecida mundialmente pelos casos Schrems I e II do Tribunal de Justiça da União Europeia, que levaram à renegociação das transferências de dados entre UE e EUA.

Como organizadores do evento, queremos compartilhar algumas reflexões sobre os assuntos que nos parecem se destacar como os mais relevantes para a região. No final deste artigo, o leitor poderá encontrar também as gravações das sessões realizadas.

Soberania digital

É importante ressaltar a crescente conexão entre governança de dados e soberania digital. Particularmente relevante é a emergência de um entendimento positivo da soberania digital como a capacidade de "entender o funcionamento da tecnologia digital, saber desenvolvê-la e regulá-la efetivamente, em conformidade aos seus próprios valores".

É neste sentido que a governança de dados desempenha um papel essencial para permitir que as pessoas sejam individualmente e coletivamente soberanas sobre seus dados: aos indivíduos deve ser garantida a autodeterminação informativa como base da soberania de dados.

Porém, é extremamente difícil reconciliar autodeterminação informativa com o desenvolvimento de sistemas de IA baseados em raspagem massiva de dados pessoais, cujas bases legais continuam sendo altamente questionáveis e cujo tratamento de dados acontece de maneira preocupantemente opaca. Neste contexto, parece muito difícil materializar a responsabilidade e prestação de contas que devem caracterizar todo tratamento de dados.

Assim, é mais que compreensível que, neste particular momento histórico, os reguladores de dados estejam no centro das atenções. Essas autoridades têm uma responsabilidade enorme, desempenhando uma função crucial para orientar não somente nosso desenvolvimento tecnológico, mas até social e democrático.

É normal, e até necessário, que um amplo leque de partes interessadas esteja demandando, cada dia mais, que tais reguladores sejam mais ativos, entreguem mais e assumam uma postura mais clara e assertiva. Precisamos deles e o trabalho deles desempenha um papel fundamental para que nos tornemos digitalmente soberanos.

Ser mais estratégicos com dados

A proteção de dados pessoais é um pilar essencial da governança de dados. Porém, precisamos também ser mais estratégicos na nossa relação com dados e considerá-los realmente como um dos ativos mais valiosos que temos, que desempenha um papel essencial para o desenvolvimento nacional.

O G20 é uma excelente oportunidade para destacar a necessidade de elaborar estratégias de dados integradas e coerentes, capazes de reconhecer que governança de dados não é somente proteção de dados pessoais. Para garantir que o valor dos dados seja aproveitado de maneira mais justa e sustentável, a inclusão de todos os setores se torna uma peça fundamental.

Assim, precisamos ser mais estratégicos com dados para sermos mais inclusivos e precisamos ser inclusivos para sermos mais estratégicos. Necessitamos promover acesso e uso de dados com base no respeito aos direitos individuais, na garantia da cibersegurança e na defesa da equidade. Precisamos também nos perguntar se, como indivíduos e como nações, estamos conseguindo as melhores condições possíveis no que diz respeito ao uso e à governança de nossos dados. Francamente, não parece ser o caso.

Uma abordagem latino-americana

Talvez uma das razões seja porque os países latino-americanos não estão negociando as condições de maneira coletiva, como um bloco regional, mas de maneira fragmentada e totalmente desorganizada.
Precisamos admitir que, fora o Brasil e talvez o México, nenhum ator na região tem o tamanho e capacidade para ser um ator de peso na governança global de dados. Ainda menos, no que diz respeito à IA.

Uma abordagem regional da governança de dados é essencial para o desenvolvimento tecnológico sustentável e soberano da América Latina. Nesta perspectiva, o estabelecimento de um arcabouço normativo e institucional coerente e homogêneo embasado em direitos fundamentais pode trazer não somente enormes avanços em termos de direitos, mas benefícios enormes em termos de cooperação em pesquisa, desenvolvimento e comércio e facilitação de transferências de dados regionais de maneira sustentável.

Estamos num momento histórico extremamente importante, no qual a região precisa agir de maneira mais coordenada, ser mais assertiva sobre nossos direitos e o desenvolvimento digital que queremos. Por isso, durante a CPDP LatAm foi lançada uma Proposta de Convenção Interamericana sobre Autodeterminação Informativa e Tratamento de Dados Pessoais.

A ideia é simples. A maioria dos países da região já tem uma lei de proteção de dados. Ou seja, a proteção de dados pessoais é uma escolha que já foi feita pelas nações latino-americanas. Então, podemos ser ambiciosos e propor um instrumento de integração regional sobre governança de dados. Na verdade, não somente podemos, mas realmente devemos ter tal ambição, considerando os últimos desenvolvimentos jurisprudenciais da região.

Em março 2024, a Corte Interamericana de Direitos Humanos publicou a decisão do caso CAJAR Vs. Colômbia, destacando que do conteúdo da Convenção Americana sobre Direitos Humanos deriva o direito autônomo à autodeterminação informativa, demandando a aprovação de normativas necessárias para implementar mecanismos ou procedimentos que garantam o direito à autodeterminação informativa. A harmonização regional já não é somente um ideal romântico: deve ser um objetivo comum de políticas públicas.

Reformar o ordenamento jurídico para uma melhor governança de dados

No intuito de promover uma governança de dados e IA transparente, inclusiva e representativa da nossa realidade, é recomendável elaborar e atualizar a legislação em três aspectos. Primeiro, para estimular a criação de espaços comuns de dados (conhecidos como "*data spaces*") ao nível nacional ou regional, onde os reguladores possam garantir o cumprimento de direitos e liberdades.

Trata-se tanto de infraestrutura quanto de normas e mecanismos de governança que permitam acompanhamento regulatório e facilitem a colaboração interinstitucional de vários tipos de reguladores cujas atribuições sejam relevantes para esses espaços de dados. Os "Espaços comuns europeus de dados" oferecem um exemplo interessante para pensar como construir nossa abordagem.

Segundo, para ampliar a participação social expandindo o acesso a dados pelas instituições de pesquisa. Os Projetos de Lei 2630/2020 e 2338/2023 contêm disposições específicas que oferecem essa oportunidade, mas precisam ser complementados com uma regulamentação que defina quem é pesquisador, qual tipo de pesquisa é legítima e como verificar a sua conformidade à lei e aos princípios gerais do ordenamento jurídico. Isso se conecta a outra figura profissional que será necessária em um mundo sempre mais interconectado e complexo, que é a de "auditores", e à necessidade de instituições e capacitação nesse sentido.

Terceiro, para criar um marco regulatório voltado a reconhecer intermediários de dados de diversos tipos: desde agentes que auxiliam os titulares no exercício dos seus direitos e os controladores em gerenciar esses pedidos de forma padronizada (gerando eficiência e evitando falhas de segurança) a entidades de destinação coletiva de dados com diferentes graus de governança participativa, como cooperativas e *data trusts*. Porque o empoderamento de dados não é apenas uma questão de controle individual: é importante assegurar também um controle coletivo, especialmente sobre os riscos e as externalidades produzidas por determinados tratamentos.

Como exemplo, basta olhar o projeto de lei 234/2023, que transita hoje no Congresso Nacional propondo a criação do ecossistema brasileiro de monetização de dados: por um lado, o projeto traz algumas sugestões que poderiam ser positivas para o empoderamento individual, como a possibilidade de proibir o uso de dados pessoais por padrão pelas empresas que nos fornecem serviços digitais e o direito de compensação em troca de eventual autorização.

Por outro, no seu estado atual ele arrisca produzir também efeitos indesejados, como aumentar as inequidades entre quem pode e quem não pode se permitir proteger a própria privacidade, gerar uma dependência ainda maior desses serviços e exacerbar as dinâmicas do capitalismo de vigilância. Essas são questões complexas sobre as quais a sociedade como um todo precisa discutir para definir uma política de governança de dados com ampla participação social.

Conclusão

Por fim, queremos frisar que o evento incluiu homenagem ao querido Danilo Doneda, um dos fundadores da CPDP LatAm, ao qual é dedicado o Danilo Doneda Award, prêmio que destaca as melhores publicações da CPDP LatAm para honrar a memória do nosso amigo, colega e mestre.

Estimular o trabalho cooperativo e a pesquisa com objetivo de impactar positivamente as políticas públicas é algo que o Danilo – sem o qual a CPDP LatAm não existiria – nos ensinou. É por isso que continuamos o esforço que começamos juntos, com entusiasmo e com alegria, voltado a cooperar para construir a cultura de proteção de dados no Brasil e na América Latina.

A seguir o leitor encontrará as principais informações e os principais resultados de cada sessão organizada no âmbito da CPDP LatAm 2024. Boa leitura!

No final deste relatório se encontra o "**Projeto de Convenção Interamericana sobre Autodeterminação Informativa, Tratamento e Circulação de Dados Pessoais**" elaborado com base nos valiosos comentários dos participantes da CPDP LatAm 2024, que esperamos possa ser debatido no âmbito do MERCOSUL ou outras organizações regionais.

SUMÁRIO

Sumário

ADVANCING PRIVACY IN LATIN AMERICA: EXPLORING THE POTENTIAL OF PRIVACY-ENHANCING TECHNOLOGIES

Gravação: https://youtu.be/1vZZqTyioLo

Organização: Future of Privacy Forum
Moderação: Maria Badillo (Future of Privacy Forum)

Palestrantes: Camila Nagano (Ifood), Pedro Martins (Data Privacy Brasil), Pedro Sydenstricker (Nym Technologies), Thiago Moraes (Autoridade Nacional de Protecão de Dados (ANPD))

- O painel debateu o potencial das Privacy-Enhancing Technologies (PETs) em promover o avanço da privacidade e da proteção de dados na América Latina. Foram englobados temas como o estado da implementação de algumas dessas tecnologias, a formulação de política e prioridades regulatórias e os potenciais oportunidades e limitações.
- Os painelistas analisaram a atuação da Autoridade Nacional de Proteção de Dados do Brasil (ANDP) em duas frentes: na sua condução dos estudos tecnológicos em anonimização e pseudonimização como base para orientações futuras; e na sua participação na OpenLoop. No Brasil, apontou-se uma lacuna nas leis de proteção de dados no concernente à provisão das PETs, além da conexão entre a lei e as novas tecnologias recari sobre o alcance de princípios referentes à proteção de dados, como a minimização de dados, ou em cumprir com as obrigações de anonimização.
- Por fim, foram discutidos os casos nos quais as PETs podem também auxiliar no desenvolvimento de negócios ao abrir as empresas a novas oportunidades de melhora no engajamento dos usuários, à tomada de decisão estratégica e à construção de confiança, elemento essencial nas transações digitais. Reforçou-se como as PETs são relevantes em lidar com possíveis riscos de privacidade gerados pela Inteligência Artificial, tendo em vista os desafios éticos e legais desencadeados por ela. Os palestrantes enfatizaram a importância de as organizações se esforçarem em aprovar programas e direcionamento dentro da governança interna, assim como em investir em educação em treinamento de staff e em manter registro da regulamentação.

AI AND CYBERSECURITY GOVERNANCE IN THE G20

Gravação: https://youtu.be/WMs1F5xjXy4

Organização: FGV Direito Rio, Rede Brasileira de Ciberseguraça
Moderação: Natalia Couto (CTS-FGV)

Palestrantes: Breno Pauli de Medeiros (CTS-FGV), Igor Monteiro Moraes (Professor da UFF e Coordenador da CESeg da SBC), Marcelo Malagutti (Gabinete de Segurança Institucional), Nina da Hora (Diretora do Instituto da Hora, Pesquisadora Recode IC/Unicamp, Ford Fellow 2024), Nombulelo Lekota (University of Johannesburg), Olga Cavalli (Universidad de Buenos Aires)

- O painel discutiu a importância da governança de IA e cibersegurança, destacando a crescente convergência entre a segurança cibernética e a inteligência artificial (IA) e a necessidade de governança nessas áreas, especialmente para economias emergentes como o Brasil. Foi ressaltada a relevância dos países do G20, incluindo o Brasil, na liderança dessas discussões e na atualização de suas estratégias nacionais de cibersegurança.
- Os painelistas exploraram alguns dos desafios de regulação e o papel da Agência Nacional de Proteção de Dados (ANPD), como o uso de IA para fins defensivos e ofensivos e a proteção de dados. Houve um debate sobre a adequação da ANPD como autoridade para regular a IA, considerando-se que a maioria das tecnologias de IA não lida diretamente com dados pessoais e que o setor enfrenta uma carência de padronização global.
- Por fim, foi abordada a escassez de profissionais capacitados em cibersegurança e IA, com estimativas indicando uma demanda crescente por formação. A criação de currículos específicos para cibersegurança em universidades e programas de formação, como o programa Hackers do Bem, foram apontados como iniciativas importantes para suprir essa carência e contribuir para uma melhor regulação e proteção cibernética no futuro.

AI AND DATA PROTECTION REGULATION IN THE G20

Gravação: https://youtu.be/E9KJNRq4RFU

Organização: Nelson Mandela University
Moderação: Luca Belli (CTS-FGV)

Palestrantes: Aifang Ma (Peking University), Danil Kerimi (CTS-FGV), Jai Vipra (CTS-FGV), Sizwe Snail (Nelson Mandela University), Tainá Aguiar Junquilho (IDP), Thomas Lohninger (Epicenter.Works – For Digital Rights)

- O painel debateu a existência de um consenso crescente de que a regulamentação da inteligência artificial (IA) é entendida como essencial, com várias iniciativas em andamento por parte de grandes economias como o Brasil, a China, a Rússia, a União Europeia e os EUA. Além disso, enfatizou-se a necessidade de se garantir que a IA respeite os direitos humanos e seja desenvolvida de forma ética e segura.
- Os painelistas analisaram os desafios na proteção de dados, tendo em vista que a questão é uma preocupação central nas discussões sobre IA. Foi destacado também que, em países como a Índia e a China, as leis relativas a esse tema estão em desenvolvimento e têm como foco buscar um equilíbrio entre o crescimento econômico e os direitos de privacidade dos cidadãos.
- Por fim, foi ressaltado o impacto Global do G20**,** considerada uma plataforma vital para discutir a governança da IA e a proteção de dados por reunir grandes economias em prol de alinhar estratégias globais. Apontou-se que apesar de suas declarações não serem vinculativas, elas ainda assim ajudam a moldar o debate e promover boas práticas entre os países participantes.

AI FROM THE GLOBAL MAJORITY: MEETING OF THE UN IGF COALITION ON DATA AND AI GOVERNANCE

Gravação: https://www.youtube.com/watch?v=ltJZMrdFUQE&feature=youtu.be

Organização: UN IGF Coalition on Data and AI Governance
Moderação: Luca Belli (CTS – FGV)

Palestrantes: Ana Brian Nougrères (UN Special Rapporteur on the Right to Privacy, Uruguai), Armando J. Manzueta Peña (Ministry of Economy, Planning and Development), Isadora Perez Peixoto (Datasphere Initiative), Jonathan Mendoza (INAI), Maria Julia Giorgelli (Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires), Pablo Palazzi (UDESA), Tatiana Coutinho (Lima Feigelson Attorneys)

- O painel destacou quais seriam as prioridades relativas à governança da Inteligência Artificial (IA), dentre elas a importância de abordar soberania, transparência e prestação de contas no desenvolvimento e regulamentação da IA. Foi discutida a necessidade de inclusão de perspectivas do Sul Global nos debates internacionais, que muitas vezes privilegiam as visões do Norte Global. A inclusão de stakeholders diversificados, com representatividade e capacitação adequadas, também foi identificada como essencial.
- Os painelistas discutiram também as preocupações sobre o uso de IA em contextos discriminatórios, como na questão da vigilância facial por exemplo, prática que afeta desproporcionalmente minorias raciais e de gênero. O painel enfatizou a necessidade de se promover interoperabilidade técnica e legislativa em prol de garantir que os sistemas respeitem a privacidade e os direitos humanos, mesmo em contextos diversos.
- Por fim, foi debatida a sustentabilidade da IA em termos ambientais e sociais, destacando o alto consumo de energia por centros de dados e o impacto ambiental associado às tecnologias. Além disso, questionou-se qual tipo de desenvolvimento tecnológico é desejável para garantir benefícios coletivos e minimizar riscos.

AI: FROM DATA COLLECTION BY DEFAULT TO COLLECTIVE PRIVACY BY DESIGN

Gravação: https://youtu.be/ltJZMrdFUQE

Organização: Access Now
Moderação: Franco Giandana Gigena (Access Now)

Palestrantes: Ellie Mcdonald (Global Partners Digital), Juan de Brigard (HR4ID (Human Rights for ID coalition)), Lucas Martho Marcon (Instituto de Defesa de Consumidores (Idec)), Paula Guedes (PUC-RJ)

- O painel abordou a importância de se proteger a privacidade individual e coletiva em um cenário de rápida evolução tecnológica. Os especialistas ressaltaram que a legislação atual foca predominantemente no primeiro tipo e deixa lacunas para o segundo, sendo esse último crucial no uso de dados em massa pela IA.
- Os painelistas discutiram o conceito de "privacidade coletiva" e sua definição a partir de uma concepção de proteção de grupos que leve em consideração os impactos sociais mais amplos. Somado a isso, concluiu-se que ainda não existe uma regulamentação abrangente para lidar com os danos coletivos e estruturais causados pela IA.
- Por fim, destacou-se a atuação do Brasil com o seu recente projeto da PL 2338 atualmente no Senado, que segue um modelo inspirado no AI Act europeu adaptado à realidade brasileira de desigualdade estrutural. Destacou-se como este projeto adota uma abordagem baseada em direitos, visando proteger grupos vulneráveis contra riscos da IA, e propõe avaliações de impacto para sistemas de alto risco, além de uma autoridade central de supervisão.

ARQUITETANDO UMA IDENTIDADE DIGITAL CIDADÃ: GOVERNANÇA E ACCOUNTABILITY DESDE A INFRAESTRUTURA

Gravação: https://youtu.be/cXy6iCpavds

Organização: Data Privacy Brasil
Moderação: Eduarda Costa Almeida (Data Privacy Brasil)

Palestrantes: Kunal Raj Barua (Aapti), Luanna Roncaratti (Ministério da Gestão e da Inovação), Priscila Couto (Ripple)

- O painel reuniu temas como a elucidação de pontos da aplicação da identidade digital, a identificação de lacunas regulatórias para alcançar a segurança e inclusão nas aplicações, e o mapeamento das práticas governamentais multisetoriais voltadas para esse sistema. Foi ressaltada a importância de haver a implementação de uma infraestrutura pública digital (digital public infrastructure, DPI) que respeite os direitos fundamentais e atente-se tanto às oportunidades decorrentes quanto aos riscos derivados. Debateu-se quais são as fundações necessárias para construir a aplicação de uma DPI, dentre elas a governança de dados e identificação de credenciais.
- A painelista Luana Roncaratti destacou a necessidade de se desenvolver uma governança tecnólogica e pessoal de modo a lidar com o sistema de identificação fragmentado utilizado no Brasil. O panelista Kunal Raj, por sua vez, afirmou a importância de incorporar medidas governamentais dentro da DPI por meio de protocolos padronizados, diretrizes e abordagem baseada em princípios. Também foi enfatizada a necessidade de se desenvolver mecanismos de feedback dentro da infraestrutura para permitir representatividade de valores de inclusão, equidade, segurança e colaboração com grupos vulneráveis.
- A painelista Priscila abordou a relação entre identidade e estruturas descentralizadas, na qual há potencial garantia de maior autonomia para pessoas identificadas. Por fim, ela elaborou a forma como, com o uso de ferramentas de blockchain, seria possível para o ator guardar suas informações pessoais de fora segura e gerenciar o compartilhamento de tais dados com outros atores no ecossistema.

ARTIFICIAL INTELLIGENCE AND HEALTH: BETWEEN IMPROVED ACCESS AND DISCRIMINATION

Gravação: https://youtu.be/eFY1ebyiW7w

Organização: Instituto de Defesa de Consumidores (Idec)
Moderação: Franco Giandana Gigena (Access Now)

Palestrantes: Fernanda Rodrigues (IRIS), Lucas Martho Marcon (Instituto de Defesa de Consumidores (Idec)), Marina Fernandes de Siqueira (Instituto de Defesa de Consumidores (Idec)), Matheus Falcão (Centre for Law, Technology and Society – University of Ottawa)

- O painel analisou como os sistemas de IA são treinados para a área de health tech, além de elucidar a existência de problemas na qualidade e diversidade desses dados, especialmente em populações vulneráveis e sub-representadas.
- Os painelistas avaliaram qual o risco representado pela IA para a segurança de dados relacionados à saúde sexual e à saúde. Destacou-se como aplicativos de saúde muitas vezes não oferecem transparência sobre o uso e compartilhamento dos dados dos usuários.
- Por fim, foi debatida a questão de como as tendências regulatórias na região estão abordando as ameaças à privacidade causadas pelo uso massivo de dados. Apontou-se o projeto de lei 2338 no Brasil a partir de seu objetivo de criar uma estrutura regulatória para IA, incluindo o uso em saúde, e de classificar os sistemas de IA por nível de risco, exigindo medidas de transparência e governança.

CAPITALISMO DE DADOS: NEURODIREITOS COMO NOVO PARADIGMA EM DIREITOS HUMANOS NA LIMITAÇÃO DA COMERCIALIZAÇÃO DA ESSÊNCIA HUMANA

Gravação: https://youtu.be/g6JP6HORCqQ

Organização: Centro de Tecnologia e Sociedade (CTS); Fundación Kamanau
Moderação: Paulo Faltay (UFRJ)

Palestrantes: Barbara Muracciole (Universidad de la República), Caitlin Mulholland (PUC-RJ), Camila Pintarelli (Ministério da Justiça), Jared Genser (The NeuroRights Foundation)

- O painel debateu quais são os impactos das tecnologias emergentes na sociedade no concernente aos desafios éticos e regulamentares e em como, na sociedade contemporânea - tecnológica, datificada e informacional - os dados representam ativos de valor agregado. Foi ressaltada a preocupação sobre como as neurotecnologias, invasivas e não invasivas, despontam ao permitir o estabelecimento de uma conexão bidirecional entre o sistema nervoso central de um indivíduo e um sistema eletrônico. Salientou-se como a última fronteira da privacidade é ultrapassada a partir da possibilidade de acessar as informações fornecidas pelo cérebro e explorá-las, gravá-las, excluí-las e até modificá-las.
- Os painelistas analisaram a aplicação desses novos instrumentos em contextos plurais como os da saúde, educação, recursos humanos, entreterimento, e outros, e enfatizaram a urgência de se promover um debate multisetorial e global.
- Por fim, foram levantadas as seguintes questões a serem focadas dentro da temática: qual seria a definição dos limites da interferência na atividade cerebral humana; se os neurodados devem ser classificados como dados pessoais sensíveis; se a base legal do consentimento livre, informado e prévio é um instrumento adequado para a legitimação desses tratamentos de neurodados; e qual seria o melhor modelo regulatório e de governança nesse contexto.

DATA PORTABILITY AND INTEROPERABILITY: BUSTING MYTHS AND BUILDING BRIDGES FOR INDIVIDUAL EMPOWERMENT

Gravação: https://youtu.be/Ti6O5owzVr8

Organização: MyData Brasil Hub
Moderação: Nicolo Zingales (CTS-FGV)

Palestrantes: Caroline Maciel (ABRANET), Delara Derakhshani (Data Transfer Initiative), Ian Brown (CTS-FGV), Jai Vipra (CTS-FGV), Paulo Brancher (Mattos Filho)

- Dentre as questões levantadas pelo painel, destacou-se a possibilidade de tornar a portabilidade dos dados uma realidade tangível e viável para as empresas e os utilizadores; como garantir a qualidade dos dados partilhados e a segurança dos modelos de governação e quais/como modelos tecnológicos e técnicos devem ser aplicados da mesma forma para viabilizar o sistema; e como expandir os modelos de interoperabilidade de dados em modelos de negócio caracterizados por monopólios e como superar os custos da concorrência.
- Os painelistas discorreram sobre a importância de, ao se desenvolver um modelo que seja interessante para as empresas, governos e proprietários, haver conscientização e transparência sobre como os modelos funcionam e quais são as questões técnicas e também os direitos que os indivíduos têm.
- Incorporando práticas implementadas no modelo inglês, foi proposta a prática de construção de um modelo amplo que leve em conta tanto os interesses de políticas públicas governamentais e empresariais, com o objetivo de criar um ecossistema tecnológico, do ponto de vista de APIs e segurança, que permita o compartilhamento de informações entre os diversos atores existentes.
- Por fim, foi apontado como os modelos de interoperabilidade podem ser uma alternativa para empoderar os usuários diante de serviços promovidos por conglomerados empresariais que operam sob a lógica do monopólio, permitindo maior concorrência.

DATA SHARING RESTRICTIONS FROM A GLOBAL SOUTH PERSPECTIVE: BALANCING DATA PROTECTION, COMPETITION, AND INNOVATION IN LATIN AMERICA?

Gravação: https://youtu.be/E7OJev8Rak0

Organização: Legal Ground Institute; VMCA Advogados
Moderação: Isabella Aragão (VMCA advogados)

Palestrantes: Andrés Calderon (Universidad Catolica Pontificia de Chile), Juliano Maranhão (Universidade de São Paulo (USP)), Meghna Bal (Esya Center)

- O painel abordou a forma como a interseção entre proteção de dados e leis de concorrência impacta a economia digital no Sul Global. Foi apontado o desafio de se conciliar a atenção prioritária à privacidade individual do primeiro fator com a busca promover mercados justos e competitivos do segundo, respectivamente.
- Os painelistas debateram também como o compartilhamento de dados é uma questão crítica, pois restrições rígidas podem prejudicar o dinamismo econômico e a inovação, especialmente em economias onde pequenas e médias empresas dependem de publicidade direcionada e de dados para adquirir clientes e competir no mercado digital.
- Por fim, foi abordado como países do Sul Global, como Brasil, Peru e Colômbia, têm considerado a criação de regulamentações adaptadas à sua realidade econômica e social. Sugeriu-se os modelos regulatórios alternativos, a exemplo de normas de propriedade de dados e exigências de interoperabilidade, como soluções que podem atender às necessidades locais, evitar práticas abusivas e ao mesmo tempo fomentar a inovação em mercados emergentes.

DATOS EN MOVIMIENTO: DESAFÍOS DE PRIVACIDAD PARA AMÉRICA LATINA EN UN ECOSISTEMA DE IA

Gravação: https://youtu.be/J9NVtNLWeV0

Organização: IPANDETEC, R3D, Sulá Batsú e Hiperderecho.
Moderação: Silvia María Calderón López (IPANDETEC)

Palestrantes: Francia Pietrasanta (R3D), Matias Mascitti (Universidad de Buenos Aires), Rubiela Alexandra Gaspar Clavo (Hiperderecho)

- O painel analisou as deficiências legislativas na proteção de dados, destacando como alguns países na América Latina possuem leis insuficientes, enquanto outros ainda carecem de regulamentação. Além disso, a falta de harmonização entre leis de proteção de dados e as regulamentações emergentes de inteligência artificial é mencionada como uma preocupação, já que muitas legislações são importadas sem adaptação para o contexto local.
- Os painelistas enfatizaram como a vigilância estatal e a coleta de dados biométricos são utilizadas em nome da segurança pública, especialmente em locais como aeroportos e fronteiras. Elaboraram como essas práticas são vistas como uma ameaça à privacidade e aos direitos humanos, especialmente em regiões onde os governos mantêm uma visão tecnossolucionista, acreditando que a tecnologia resolverá problemas de segurança.
- Por fim, o debate apresentou sugestões de medidas para mitigar esses riscos, como a criação de centros regionais de controle algorítmico e a adaptação de normas que contemplem a realidade sociocultural da América Latina. Também propôs uma colaboração entre países e setores para regulamentações mais coerentes, incluindo a participação ativa de autoridades e da sociedade civil, a fim de melhorar a transparência e a proteção de dados na região.

DIGITAL PUBLIC INFRASTRUCTURES & TOWARD FINANCIAL INCLUSION

Gravação: https://youtu.be/GIuSyui7n-A

Organização: Instituto de Defesa de Consumidores (Idec) & Consumers International
Moderação: Hannah Draper (Consumers International)

Palestrantes: Armando J. Manzueta Peña (Ministry of Economy, Planning and Development), Fiorentina García Miramón (Tec-Check (Organización de Consumidores en Línea)), Maria Luciano (Instituto de Defesa de Consumidores (Idec)), S Saroja (Citizen consumer and civic Action Group (CAG))

- O painel explorou o impacto das infraestruturas públicas digitais (DPIs) na inclusão financeira em diversos países, destacando como as DPIs, a exemplo do Pix no Brasil e o UPI na Índia, facilitam transações rápidas e acessíveis e promovem maior inclusão financeira, especialmente em áreas com baixo acesso a bancos. Também se analisou como a implementação dessas tecnologias enfrenta desafios relacionados à privacidade, segurança e falta de entendimento por parte dos usuários, o que leva a casos frequentes de fraudes e uso indevido.
- Os painelistas abordaram a importância da proteção e privacidade dos dados nas transações digitais, alertando para os riscos de vazamento de dados e da falta de segurança cibernética. Discutiu-se a necessidade de uma infraestrutura de segurança mais robusta e de políticas de privacidade por design para evitar abusos, somada à relevância da conscientização dos consumidores sobre o uso de seus dados.
- Por fim, o painel apontou a necessidade de inclusão dos consumidores no proceso de governança dessas DPIs, a partir de mecanismos de apoio a esse grupo.

DIREITOS DOS TITULARES EM AÇÃO: MARKETPLACES E PLATAFORMAS

Gravação: https://youtu.be/mAvbG7XXy0c?si=XTqS9rO5mYqyHBwV

Organização: Núcleo eCommerce
Moderação: Beatriz Costa (CTS-FGV)

Palestrantes: Diego Machado (Universidade Federal de Viçosa), Erica Bakonyi (CTS-FGV), Felipe Tavares (FGV Direito Rio), Giovanna Milanese (VLK Advogados), Luciano Gandolla (Mercado Livre), Rodrigo Dias de Pinho Gomes (Pinho Gomes), Júlia Mendonça (FGV Direito Rio)

- O painel tratou dos desafios e da eficácia da proteção de dados nos marketplaces e plataformas digitais, analisando o cumprimento das obrigações da Lei Geral de Proteção de Dados (LGPD) no Brasil. A pesquisa abrangeu 100 plataformas, examinando suas políticas de privacidade, com foco no fornecimento de informações sobre o controlador dos dados e o encarregado de proteção (DPO), além da transparência em relação ao compartilhamento de dados com terceiros. Observou-se que muitas empresas, principalmente as de médio e grande porte, não cumprem integralmente com as exigências legislativas.

- Os painelistas demonstraram como a análise prática da aplicação dos direitos dos titulares, como pedidos de acesso e exclusão de dados, revelou falhas significativas no atendimento ao consumidor. Em alguns casos, as empresas exigiram verificações de identidade inadequadas ou não responderam dentro do prazo estipulado, dificultando o exercício dos direitos. Também foram identificados problemas quanto ao compartilhamento de dados, com algumas empresas não especificando as finalidades e bases legais.

- Por fim, o painel destacou a importância de maior transparência e adequação das políticas de privacidade. A pesquisa sugeriu que melhorias significativas são necessárias para que os direitos dos titulares sejam efetivamente protegidos, promovendo uma maior confiança no ambiente digital e nas operações dessas plataformas.

DIREITOS HUMANOS EM SERVIÇOS PÚBLICOS DIGITAIS: DEBATENDO O PAPEL DE CIDADES E PREFEITURAS

Gravação: https://youtu.be/38gWJIfIsfM

Organização: InternetLab
Moderação: Daniel Gaspar (Prefeitura de Niterói)

Palestrantes: Bárbara Prado Simão (InternetLab), Livia Schaeffer Nonose (ONU-Habitat), Luísa Passeto (USP)

- O painel abordou a importância dos direitos humanos no desenvolvimento de serviços públicos digitais em governos locais, destacando a iniciativa da Prefeitura de Niterói, em parceria com o Internet Lab e a ONU Habitat, para criar um guia que orienta as administrações municipais sobre como humanizar esses serviços.

- Os painelistas apresentaram a proposta de um guia que tem um enfoque prático, com recomendações que incluem a necessidade de manter canais presenciais para quem enfrenta dificuldades digitais e a capacitação de gestores públicos. Para enfrentar desigualdades no acesso digital, o projeto propõe iniciativas como ajudantes digitais e pesquisas com usuários vulneráveis, permitindo que os serviços sejam redesenhados conforme as necessidades locais. A transparência é enfatizada, com indicadores que permitem à população avaliar a prestação de serviços e exercer controle social.

- Por fim, o debate destacou o papel da ONU Habitat em promover cidades inteligentes centradas nas pessoas, que usam a tecnologia como um meio para melhorar a qualidade de vida, respeitando direitos humanos digitais. A iniciativa fomenta discussões globais sobre governança digital, evidenciando a importância da inclusão digital e da criação de mecanismos de colaboração entre governos e cidadãos, de modo a garantir que a tecnologia contribua positivamente para o desenvolvimento sustentável nas cidades.

ESTÁNDARES INTERAMERICANOS DE DDHH E IA: UNA ARTICULACIÓN ENTRE DERECHOS HUMANOS, RETOS REGIONALES Y DIRECTRICES GLOBALES

Gravação: https://youtu.be/jTcFyk-Em-o

Organização: Electronic Frontier Foundation y Derechos Digitales
Moderação: Mercedes Elaskar (Allende & Brea)

Palestrantes: Fábio Soares Eon (UNESCO), Jamila Venturini (Derechos Digitales), Renata Mielli (Ministério da Ciência, Tecnologia e Inovação (MCTI)), Veridiana Alimonti (Electronic Frontier Foundation)

- O painel abordou a importância de se criar padrões interamericanos de direitos humanos na implementação de inteligência artificial (IA) em países da América Latina. Avaliou-se como a implementação de sistemas automatizados frequentemente carece de regulamentações e avaliações de impacto adequadas, o que pode prejudicar o acesso a direitos básicos e reforçar desigualdades. Além disso, demonstrou-se preocupação com o uso de dados pessoais, que muitas vezes é realizado sem o devido consentimento ou transparência.

- Os painelistas debateram sobre as posturas das organizações como a UNESCO e a Electronic Frontier Foundation (EFF) em enfatizar a necessidade de regulamentação ética e social da IA. Citou-se o exemplo da UNESCO, que criou uma recomendação global para a ética em IA, incentivando países a adotarem práticas regulatórias que garantam a proteção dos direitos humanos, com especial atenção à transparência, supervisão humana e diversidade de dados.

- Por fim, os participantes defenderam que a cooperação internacional é essencial para apoiar esses países no desenvolvimento de uma governança de IA ética e inclusiva. Isso inclui promover o direito à autodeterminação informativa, à privacidade e à igualdade, visando a evitar que tecnologias ampliem desigualdades e protejam efetivamente os direitos dos cidadãos.

GLOBAL INDEX ON RESPONSIBLE AI: AN OVERVIEW OF GOVERNANCE, CAPABILITIES, AND FUNDAMENTAL RIGHTS

Gravação: https://youtu.be/v_VsF6_NGgI

Organização: CyberBRICS, FGV Direito Rio
Moderação: José Luiz Nunes (CTS-FGV)

Palestrantes: Armando J. Manzueta Peña (Ministry of Economy, Planning and Development), Larissa Galdino de Magalhães Santos (CyberBRICS), Mercedes de los Santos (Open Data Charter), Samara Castro (Governo Federal do Brasil)

- O painel discutiu a importância de haver consideração da origem e representatividade dos dados de aplicações de IA dentro da pauta de governança de dados, com preocupações sobre a garantia de que os sistemas de IA sejam treinados de modo a refletir os contextos locais e as realidades de cada país. Adicionalmente, destacou-se a necessidade de que modelos governamentais robustos tratem do compartilhamento de dados e transferências de dados entre o setor público-privado, além atuarem na proteção de dados ao liderar e supervisionar a governança da IA.
- O segundo ponto do painel apontou para como é essencial o envolvimento do público de modo a priorizar os direitos humanos ao longo do processo de lifecycle da IA, desde a formulação da agenda até a supervisão regulamentária.
- Por fim, debateu-se como as conversas em torno das capacidades da IA em relação a compras públicas permanecem subdesenvolvidas. Apesar de haver referências a essa prática em países como o Chile, tais visões ainda não contribuem substancialmente para o debate mais amplo, no qual as capacidades ainda são consideradas secundárias.

INNOVATION OR HUMAN RIGHTS: DATA GOVERNANCE AND SANDBOXES FOR AI IN LAC

Gravação: https://youtu.be/7pd3TpTcrjk

Organização: Derechos Digitales, Datasphere Initiative
Moderação: Jamila Venturini (Derechos Digitales)

Palestrantes: Jonathan Mendoza (INAI), Laura Galindo (Meta), Lucía Camacho (Derechos Digitales), Philipe Moura (Vinci Ventures), Breno Pauli de Medeiros (CTS-FGV)

- O painel discutiu o uso de sandboxes regulatórios como ferramentas para experimentação e desenvolvimento de normas em inteligência artificial (IA) nos países da América Latina. Foi enfatizado como os sandboxes proporcionam um espaço controlado onde reguladores e inovadores podem testar tecnologias disruptivas e explorar direções normativas. Além disso, esse modelo de experimentação é defendido por permitir que os países formulem regulações mais ajustadas ao seu contexto socioeconômico, o que é crucial para a América Latina, onde a replicação de leis de outras regiões pode não se adequar à realidade local.
- Os painelistas também apontaram um desafio significativo, que é o de equilibrar a inovação tecnológica com a proteção dos direitos humanos. Foi destacado como os sandboxes não apenas incentivam a inovação, mas também precisam considerar os direitos e a segurança dos usuários, especialmente em contextos de IA.
- Por fim, o debate ressaltou a importância da colaboração multissetorial e internacional para lidar com os desafios e complexidades de regulamentação de IA. Para a América Latina, o texto sugere que uma abordagem que inclua o envolvimento de diversas partes interessadas e uma estrutura institucional mais flexível, pode ser a chave para desenvolver regulamentações de IA que protejam os direitos humanos e fomentem a inovação de maneira sustentável.

LGPD E FUTURA REGULAÇÃO DE IA NO BRASIL: INTERSECÇÕES ENTRE A AUTORIDADE DE PROTEÇÃO DE DADOS PESSOAIS E A AUTORIDADE DE GOVERNANÇA DA IA

Gravação: https://youtu.be/-2uZlkBCf0I

Organização: LIA - Laboratório de Governança e Regulação do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)
Moderação: Laura Schertel Mendes (IDP/UnB)

Palestrantes: Ana Brian Nougrères (UN Special Rapporteur on the Right to Privacy, Uruguai), Pablo Palazzi (UDESA), Tainá Aguiar Junquilho (IDP), Waldemar Gonçalves (Autoridade Nacional de Protecão de Dados (ANPD))

- O painel debateu a Lei Geral de Proteção de Dados (LGPD) e o papel crucial de uma futura regulação de Inteligência Artificial (IA) no Brasil. Foi explorada a forma como a proposta legislativa principal, o Projeto de Lei 2338, visa criar um sistema de supervisão híbrido no qual a Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central na coordenação das regulações sobre IA, atuando em parceria com outras agências reguladoras setoriais.
- Os painelistas destacaram que o modelo da PL 2338 visa garantir uma abordagem equilibrada, onde os princípios de transparência, responsabilidade e segurança são aplicados de forma uniforme, independente do setor. Além disso, o sistema também dá espaço para as agências que já lidam com IA, como a Anatel, para que usem seu conhecimento especializado em áreas específicas, sob a orientação coordenadora da ANPD.
- Por fim, foi ressaltado como a ANPD tomou medidas contra o uso de dados pessoais pela Meta para treinamento de IA, demonstrando seu compromisso com a proteção dos direitos dos titulares. Também foi elencado como que, com mais de quatro anos de discussões, o PL 2338 tem sido aprimorado com base em audiências públicas e consultas com especialistas, refletindo um amadurecimento na regulamentação de IA no Brasil.

PANORAMA DE LA NORMATIVA SOBRE REGULACIÓN ALGORÍTMICA EN AMÉRICA LATINA: AUDITORÍA DE ALGORITMOS E IMPACTO SOCIAL EN LA REGIÓN

Gravação: https://youtu.be/RKf4Z3C4C7M

Organização: Daniel law, CETYS UDESA Argentina
Moderação: Pablo Palazzi (UDESA)

Palestrantes: Nuria Lopez (Daniel Law), Mercedes Elaskar (Allende & Brea), Gemma Galdon Clavell (Conselheira Senior da Comissão Europeia), Humberto De Jesús Ortiz Rodríguez (Whirpool)

- O painel explorou o panorama regulatório sobre algoritmos e inteligência artificial na América Latina, destacando a ausência de leis específicas em diversos países. Analisou-se como, em geral, as legislações de proteção de dados tratam da questão de forma indireta, assegurando o direito de não ser sujeito a decisões automatizadas sem transparência. Destacou-se como alguns países apresentam avanços ao exigir que empresas informem os cidadãos sobre o uso de algoritmos para decisões que afetem diretamente suas vidas.
- Os painelistas enfatizaram como, no Brasil, a lei de proteção de dados permite revisão de decisões automatizadas, mas há resistência das empresas em divulgar informações técnicas sobre os algoritmos, o que cria desafios para a auditoria dos sistemas.
- Por fim, o painel ressaltou a necessidade de maior transparência algorítmica, especialmente para prevenir discriminação e garantir o cumprimento das normas de forma justa e responsável. Foram sugeridas auditorias com três níveis: governança, avaliação técnica do modelo e auditoria de impacto, sendo esta última essencial para avaliar o efeito real dos algoritmos na sociedade.

PLATFORMS ACCOUNTABILITY: TRANSPARENCY, PRIVACY AND LABOR

Gravação: https://youtu.be/j6SummX-Xkw?si=NgQhb4myqUL-w-ea

Organização: CTS-FGV, Derechos Digitales
Moderação: Jessica Pidoux (PersonalData.IO)

Palestrantes: Grenfieth Sierra (Delegatura de Protección de Datos de Colombia), Guilherme Mucelin (CTS-FGV), Jamila Venturini (Derechos Digitales), Lucía Camacho (Derechos Digitales), Rodrigo Carelli (Ministério Público do Trabalho)

- O painel centrou-se na interação entre as classificações laborais e a transparência algorítmica. Os participantes do painel examinaram a luta contínua enfrentada pelas autoridades brasileiras para determinar se os trabalhadores baseados em aplicativos devem ser classificados como empregados ou contratados autônomos, e o que deve ser proposto para garantir que esses trabalhadores recebam proteções adequadas, reconhecendo a natureza flexível dos papéis da economia de gig.
- Os painelistas avaliaram o estado atual das medidas de proteção trabalhista e práticas de transparência entre várias plataformas na América Latina, com foco especial nos setores de entrega de alimentos e mercearias. A conversa ressaltou os desafios específicos da região e a necessidade de abordagens regulatórias personalizadas para salvaguardar os direitos dos trabalhadores.
- Por fim, foram apresentadas as propostas formuladas pelos participantes, que defenderam o desenvolvimento e a aplicação de estruturas abrangentes de transparência algorítmica. Estes quadros devem obrigar as plataformas a divulgar os processos de tomada de decisão e as práticas de tratamento de dados, aumentando assim a responsabilização e permitindo que os trabalhadores e os reguladores examinem eficazmente as operações das plataformas. O conceito de soberania digital foi enfatizado como crucial para capacitar indivíduos e comunidades contra o domínio de grandes empresas de tecnologia.

PROTOTIPAGEM DE POLÍTICAS APLICADAS A TECNOLOGIAS DE APRIMORAMENTO DE PRIVACIDADE: ESTUDO DE CASO DO PROJETO OPEN LOOP NO BRASIL E NO URUGUAI.

Gravação: https://youtu.be/-ZCxZtgtKVY

Organização: Universidade Estadual da Paraíba e Instituto Liberdade Digital
Moderação: Maria Edelvacy Marinho (Instituto Liberdade Civil)

Palestrantes: Claudia Del Pozo (C Minds), Laura Galindo (Meta), Raissa Moura (Nubank), Samanta Oliveira (Mercado Livre)

- O painel discutiu como as Políticas de Prototipagem de Tecnologias de Aprimoramento de Privacidade (PETs), que incluem métodos como criptografia avançada e anonimização, visam melhorar a privacidade dos dados enquanto possibilitam a extração de informações de forma segura.
- Os painelistas mencionaram como o projeto Open Loop, promovido pela Meta, busca desenvolver protótipos e coletar dados para embasar políticas voltadas para PETs. O objetivo é oferecer diretrizes que auxiliem organizações e reguladores a entender melhor como implementar essas tecnologias em conformidade com leis de proteção de dados, como a LGPD no Brasil.
- O debate também abordou a importância de uma colaboração entre os setores público e privado para definir padrões e orientações, promovendo um ambiente de inovação responsável e segura na América Latina.

QUESTIONANDO A LEGALIDADE DO USO DE SPYWARES NA AMÉRICA LATINA: PERSPECTIVAS DA SOCIEDADE CIVIL

Gravação: https://youtu.be/-xtnoLaIres

Organização: InternetLab e Data Privacy Brasil
Moderação: Bárbara Prado Simão (InternetLab)

Palestrantes: Giovanna Milanese (VLK Advogados), Luis Fernando Garcia (R3D), Pedro Saliba (Data Privacy Brasil), Pilar Saénz (Fondación Karisma)

- O painel analisou a problemática do uso de spywares na América Latina, com foco em como governos empregam essas ferramentas para vigilância sem transparência, muitas vezes direcionada a jornalistas, ativistas e defensores de direitos humanos. Tecnologias como o spyware Pegasus possibilitam a coleta de dados pessoais, localização e conversas, intensificando preocupações sobre violações de privacidade e liberdades fundamentais. Enfatizou-se como organizações de direitos civis questionam a legitimidade desses métodos, sugerindo que tais práticas colocam em risco princípios democráticos.
- Os painelistas mencionaram que, na prática, a aplicação dessas tecnologias ocorre sem supervisão adequada, e, em muitos casos, há indícios de corrupção, com autoridades beneficiando-se da vigilância para fins políticos. A sociedade civil defende que uma regulamentação é necessária para definir limites de uso e garantir proporcionalidade e transparência.
- Por fim, também foram exploradas formas de combater os abusos a partir de um documento que recomenda a implementação de mecanismos de supervisão e regulamentação rigorosos que exijam autorização judicial e relatórios de transparência sobre o uso de spywares. Sugere também que sejam adotados princípios de necessidade e proporcionalidade. A análise aponta para o risco do "tecnoautoritarismo", onde o uso excessivo de vigilância digital ameaça a democracia e reforça a importância de proteger os direitos dos cidadãos.

REGULAMENTAÇÃO DE IA NO BRASIL: IMPACTOS, OBRIGAÇÕES E DESAFIOS PARA A INOVAÇÃO

Gravação: https://youtu.be/reMd5wLJ5ME

Organização: Prado Vidigal Advogados
Moderação: Luis Fernando Prado (Prado Vidigal Advogados)

Palestrantes: Deborah Siqueira de Oliveira (Quinto Andar), Fabro Steibel (Instituto de Tecnologia e Sociedade), Lucas Borges (Autoridade Nacional de Protecão de Dados (ANPD))

- O painel abordou como o Brasil busca equilibrar a regulamentação de inteligência artificial (IA) com a necessidade de fomentar a inovação. Foram discutidos os projetos de lei em andamento como o PL 2338. Foi levantada a preocupação de que uma regulação excessivamente prescritiva pode prejudicar pequenas empresas e startups, além de criar desafios para setores acadêmicos. A flexibilidade e a neutralidade tecnológica foram sugeridas como caminhos para uma legislação mais adaptável.
- Os painelistas apontaram para o fato de as empresas brasileiras estarem em estágios iniciais de implementação de governança em IA, e portanto ainda compreendendo conceitos básicos e avaliando frameworks globais. No entanto, foi destacado que muitas organizações ainda não realizam avaliações de riscos adequadas, indicando a necessidade de maior conscientização e treinamento interno.
- Por fim, a sustentabilidade foi destacada como um aspecto central, tanto no uso de recursos ambientais quanto na preservação cultural e social. Foi mencionado o papel do Brasil como um potencial líder em IA aberta, com soluções que equilibrem inovação e responsabilidade social.

SAÚDE DIGITAL, INTELIGÊNCIA ARTIFICIAL E COMPUTAÇÃO EM NUVEM: PERSPECTIVAS MULTISSETORIAIS

Gravação: https://youtu.be/WxZC9q4yQ4Q

Organização: Legal Grounds Institute, FGV Direito Rio
Moderação: Samuel Oliveira (Legal Grounds Institute)

Palestrantes: Adriana Marques (Secretaria de Informação e Saúde Digital, Ministério da Saúde), Diogo Manganelli (FGV Rio), Ricardo Campos (Goethe Universität Frankfurt/Main)

- O painel abordou o impacto das tecnologias digitais na saúde, destacando a importância da inteligência artificial (IA) e da computação em nuvem para aprimorar o acesso e a qualidade dos serviços no Sistema Único de Saúde (SUS). Foram apresentados exemplos de iniciativas, como telemedicina, prontuários eletrônicos e a Rede Nacional de Dados em Saúde (RNDS), que organiza bilhões de dados para suportar políticas públicas e pesquisa. Além disso, enfatizou-se o papel da IA na predição de emergências sanitárias, diagnóstico médico e apoio à decisão clínica, sempre considerando a decisão final do profissional de saúde.
- Foi destacada a criação da Secretaria de Informação e Saúde Digital em 2023, que coordena ações como governança de dados, interoperabilidade e proteção de dados pessoais. Iniciativas específicas incluem o prontuário falado, monitoramento de medicamentos e uso de IA para diagnóstico de doenças como câncer e tuberculose, reforçando a transformação digital no SUS.
- Por fim, o painel discutiu a relevância da soberania digital e da regulação no uso de IA e nuvens computacionais. Enfatizou-se a necessidade de harmonização entre saúde pública e privada, a interoperabilidade de sistemas e a proteção dos direitos dos titulares. O Brasil também busca uma posição estratégica internacional, alinhada ao G20 e ao Plano Brasileiro de IA, para garantir a aplicação ética e eficiente dessas tecnologias no contexto local e global.

THE IMPACT OF EU AI REGULATION ON LATIN AMERICAN AI GOVERNANCE: EMERGING AI AUTHORITIES?

Gravação: https://youtu.be/oHDIj2AjVoI

Organização: CPDP - Privacy Salon
Moderação: Ine van Zeeland (Vrije Universiteit Brussel)

Palestrantes: Alberto Cerda (Universidad de Chile), Barbara Lazarotto (Vrije Universiteit Brussel), Filipe Medon (CTS-FGV), Lucas Borges (Autoridade Nacional de Protecão de Dados (ANPD)), Pedro Martins (Data Privacy Brasil)

- O painel analisou a Lei de Inteligência Artificial da União Europeia (AI Act) e sua potencial influência nos quadros de governação da IA na América Latina. Explorou a abordagem regulatória horizontal da UE, centrada no ser humano e baseada no risco, enfatizando como esses princípios estão a moldar o discurso regulamentar e o desenvolvimento de políticas em todo o Atlântico.
- Um foco central da discussão foi os mecanismos de aplicação dessas novas regulações de IA. O painel analisou se são necessárias autoridades de supervisão especializadas para abordar questões específicas da IA - como a opacidade de certos modelos de IA e as complexidades das cadeias de fornecimento de dados e algoritmos - ou se os organismos reguladores existentes poderiam alargar o seu âmbito para gerir eficazmente estes desafios.
- Por fim, foram sublinhado as complexidades da regulamentação da IA e os desafios na determinação os mecanismos de supervisão mais adequados. Ressaltou-se que deve ser encontrado um equilíbrio cuidadoso entre a promoção da inovação e a proteção dos direitos fundamentais, além de a ver possibilidade de as considerações matizadas necessitadas pelos países latino-americanos gerarem obstáculos ao desenvolverem os seus próprios quadros de governação da IA.

TRANSPARENCIA ALGORITMICA, USO Y PROTECCIÓN DE DATOS POR LOS GOBIERNOS

Gravação: https://youtu.be/pb6HwYRQmQI

Organização: Article 19
Moderação: Priscila Ruiz (Artigo 19 Brasil)

Palestrantes: Romina Garrido (Universidad Adolfo Ibáñez), Lia Hernández (Legal IT), Jonathan Mendoza (INAI), Silvia María Calderón López (IPANDETEC)

- O painel refletiu questões, dentre elas a definição de transparência algorítmica e qual a sua importância no sector público; as medidas que foram adaptadas no setor público para a compra e/ou aquisição de tecnologias para uso interno e externo; e, por fim, a dúvida sobre a necesidade de haver regulamentação e transparência algorítmica e o reforço sobre as normas de transparência e proteção de dados pessoais na América Latina.
- Os painelistas defenderam a importância conceitual da transparência algorítmica no setor público como fundamental para a compreensão e aplicação do uso e desenvolvimento de tecnologías, além de ressaltar que o uso e o desenvolvimento de tecnologias são ferramentas de apoio e não soluções para problemas mais complexos dentro dos sistemas institucionais de governo e até mesmo dentro de um país.
- Por último, destacou-se que os princípios de transparência, privacidade e responsabilidade são direitos humanos que devem ser garantidos e respeitados pelos Estados e incorporados nos seus regulamentos internos.

WORLDCOIN: IDENTIDAD DIGITAL, DATOS BIOMÉTRICOS Y SEGURIDAD

Gravação: https://youtu.be/Ma5Mb5C9INI

Organização: Fundación Kamanau
Moderação: Eduarda Costa Almeida (Data Privacy Brasil)

Palestrantes: Horrara Moreira (AqualtuneLab), Maria Julia Giorgelli (Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires), Moisés Sánchez (Fundación Kumanau), Ruth Puente (Experta internacional independiente)

- O painel debateu a atuação da empresa WorldCoin e sua proposição de um modelo que desafia o pensamento sobre a proteção de dados. Partindo da premissa da necessidade de um sistema para identificar as interações humanas no mundo virtual, há o desenvolvimento de um modelo que procura credenciar essa "humanidade" com base em dados biométricos da íris. Alguns dos problemas presentes nesse processo foram analisados.
- Foi apontado como exemplo de problema o fato de a captação de dados biométricos exigir um nível elevado de consentimento informado, e como isso não é realizado pela empresa, que os capta utilizando sistemas que não são diferentes dos de qualquer aplicação. Somado a isso, outro exemplo dado foi o processo no qual, ao gerar um sistema de valorização da sua base de dados de íris através da criação de uma criptomoeda (que é dada aos utilizadores que registram sua íris na plataforma) há como resultante para os efeitos de captura de dados o vício no consentimento. Isto é, ocorre a entrega de dados biométricos com a promessa de monetização desses dados.
- Por fim, o painel debateu o impacto gerado na ordem pública econômica, na medida em que não é razoável que as duas atividades (a identificação e a moeda digital) funcionem de forma integrada. A consequência desse processo foi descrita como a indução a um comportamento monopolista e/ou a um abuso de posição no mercado.

UNA PROPUESTA DE CONVENCIÓN INTERAMERICANA SOBRE TRATAMIENTO DE DATOS PERSONALES, AUTODETERMINACIÓN INFORMATIVA Y CIRCULACIÓN DE ESA INFORMACIÓN

Luca Belli[1], Ana Brian Nougrères[2], Jonathan Mendoza Iserte[3], Pablo A. Palazzi[4] y Nelson Remolina Angarita[5]

DISCUSSION PAPER PRESENTADO EN LA **COMPUTERS PRIVACY AND DATA PROTECTION CONFERENCE LATIN AMERICA (CPDP LATAM) 2024** PARA RECIBIMIENTO DE COMENTARIOS.

POR FAVOR, POR FAVOR ENVÍE SUS COMENTARIOS SOBRE ESTE DOCUMENTO A CTS@FGV.BR ANTES DEL 10/08/2024.

RESUMEN:

PALABRAS CLAVE:

[1] Professor at Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro, director del Center for Technology and Society (CTS-FGV) and the CyberBRICS project, Director of the Latin-American edition of the Computers Privacy and Data Protection conference (CPDP LatAm).

[2] Doctora en Derecho y Ciencias Sociales por la Facultad de Derecho de la Universidad de la República Oriental del Uruguay, Relatora Especial de las Naciones Unidas en materia de Privacidad por el Consejo de Derechos Humanos de las Naciones Unidas desde el 1 de agosto de 2021.

[3] Secretario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

[4] Profesor de Derecho Universidad de San Andrés (Argentina), Director del CETyS - Centro de Tecnologia y Sociedad de Universidad de San Andrés, Director del Diplomado Internacional de protección de datos personales de la Universidad de San Andrés.

[5] Profesor de Derecho Universidad de los Andres, Director del GECTI (Univ. de los Andes), ex director de datos personales de la Superintendencia de Comercio de Colombia.

Uma Proposta de Convenção Interamericana sobre Tratamento de Dados Pessoais, Autodeterminação Informativa e Circulação dessas Informações

Luca Belli, Ana Brian Nougrères, Jonathan Mendoza Iserte, Pablo A. Palazzi y Nelson Remolina Angarita

POSITION PAPER APRESENTADO NA **COMPUTERS PRIVACY AND DATA PROTECTION CONFERENCE LATIN AMERICA (CPDP LATAM) 2024** PARA RECEBER COMENTÁRIOS.

POR FAVOR, ENVIE SEUS COMENTÁRIOS SOBRE ESTE DOCUMENTO PARA CTS@FGV.BR ATÉ 10/08/2024.

RESUMEN:

PALABRAS CLAVE:

SUMARIO

SUMÁRIO

UNA PROPUESTA DE CONVENCIÓN INTERAMERICANA SOBRE TRATAMIENTO DE DATOS PERSONALES, AUTODETERMINACIÓN INFORMATIVA Y CIRCULACIÓN DE ESA INFORMACIÓN

La idea de desarrollar esta propuesta surgió a partir del documento de discusión "Hacia un Modelo Latinoamericano de Adecuación para la Transferencia International de Datos Personales", presentado en la conferencia *Computers Privacy and Data Protection Conference Latin America* 2023 (CPDP LatAm) en Río de Janeiro, Brasil, con el fin de recibir comentarios de los asistentes al evento.

La versión actualizada con comentarios recibidos fue publicada en la obra Palazzi (Org.) "Protección de Datos personales: doctrina y jurisprudencia, tomo 4", Buenos Aires, Argentina (2024). Este documento fue premiado por el *Future of Privacy Forum* con el reconocimiento "*Privacy Papers for Policymakers Award*" y utilizado como primero capítulo de una obra en publicación dedicada a las "Transferencia Internacional de Datos Personales en América Latina: Hacia la Armonización de Normas" de autoría de Belli, Brian, Mendoza, Palazzi e Remolina.

Esta propuesta de "Convención Interamericana sobre Tratamiento de Datos Personales, Autodeterminación Informativa y Circulación de esa Información" será incluida como anexo del volumen en publicación. Los autores

UMA PROPOSTA DE CONVENÇÃO INTERAMERICANA SOBRE TRATAMENTO DE DADOS PESSOAIS, AUTODETERMINAÇÃO INFORMATIVA E CIRCULAÇÃO DESSAS INFORMAÇÕES

A ideia de desenvolver essa proposta surgiu com base no documento de discussão "Rumo a um Modelo Latino-Americano de Adequação para a Transferência Internacional de Dados Pessoais", apresentado na conferência *Computers Privacy and Data Protection Conference Latin America* 2023 (CPDP LatAm) no Río de Janeiro, Brasil, para receber comentários dos participantes do evento.

A versão atualizada com comentários recebidos foi publicada na obra Palazzi (Org.) "Protección de Datos personales: doctrina y jurisprudencia, tomo 4", Buenos Aires, Argentina (2024). Este documento foi premiado pelo *Future of Privacy Forum* com o reconhecimento "*Privacy Papers for Policymakers Award*" e utilizado como primeiro capítulo de uma obra de publicação dedicada à "*Transferência Internacional de Dados Pessoais na América Latina: Hacia la Armonización de Normas*" de autoria de Belli, Brian, Mendoza, Palazzi e Remolina.

Esta proposta de "Convenção Interamericana sobre Tratamento de Dados Pessoais, Autodeterminação Informativa e Circulação dessa Informação" será incluída como anexo do volume de publicação. Os autores

dedican estes trabajos a la memoria del querido profesor Danilo Doneda, sin el cual estas reflexiones probablemente nunca hubieran ocurrido.

Una convención regional de protección de datos puede facilitar e, idealmente, aumentar los estándares de protección de datos en los países participantes, promoviendo la tan necesaria consistencia y coherencia en los marcos regulatorios, reduciendo enormemente la inseguridad jurídica y los costos de cumplimiento para las empresas que operan a través de fronteras, facilitando las transferencias de datos transfronterizas y promoviendo las políticas regionales, integración y crecimiento económico, contribuyendo al fortalecimiento de la soberanía de cada país miembro.

La globalización y el creciente intercambio de datos personales entre países de América Latina demandan un marco regulatorio uniforme que permita proteger la privacidad y los derechos fundamentales de los individuos. Actualmente, existen diversas estructuras legales en la región, como la Organización de los Estados Americanos (OEA), el Pacto Andino y el Mercosur, que podrían albergar dicho acuerdo. De estos, la OEA, con 34 países miembros, ofrece la mayor cobertura y antecedentes en la protección de datos personales y derechos humanos.

Sin embargo, como destacamos el nuestro estudio, es también posible pensar que las ideas propuestas aquí puedan inspirar un esfuerzo de desarrollo de un marco regional, por parte de un grupo limitado de países

dedicam estes trabalhos à memória do querido professor Danilo Doneda, sem o qual essas reflexões provavelmente nunca teriam acontecido.

Uma convenção regional de proteção de dados pode facilitar e, idealmente, aumentar os padrões de proteção de dados nos países participantes, promovendo a tão necessária consistência e coerência nos quadros regulamentares, reduzindo significativamente a incerteza jurídica e os custos de conformidade para as empresas que operam além-fronteiras, facilitando as transferências de dados e promoção de políticas regionais, integração e crescimento econômico, contribuindo al fortalecimento da soberania de cada país membro.

A globalização e o crescente intercâmbio de dados pessoais entre os países latino-americanos exigem um quadro regulatório uniforme, que permita proteger a privacidade e os direitos fundamentais dos indivíduos. Atualmente, existem diversas estruturas jurídicas na região, como a Organização dos Estados Americanos, o Pacto Andino e o Mercosul, que poderiam acolher tal acordo. Destes, a OEA, com 34 países membros, oferece a maior cobertura e histórico na proteção de dados pessoais e dos direitos humanos.

No entanto, como destaca nosso estúdio, também é possível pensar que as ideias propostas aqui possam inspirar um esforço de desenvolvimento de um marco regional, por parte de um grupo limitado de países latino-americanos com interesses afins e sistemas jurídicos

latinoamericanos con intereses afines y sistemas jurídicos compatibles, sin necesidad de depender de una organización intergubernamental preexistente. Por lo tanto, podemos pensar que un esfuerzo plurilateral liderado por un grupo reducido de países abiertos a la colaboración con todos los estados de América Latina puede considerarse como una opción potencialmente exitosa.

Beneficios de una Convención Regional

Derechos Fundamentales: Reafirmaría la protección de datos personales como un derecho fundamental en América Latina, aumentando la credibilidad y la influencia en foros internacionales.

Cooperación, Desarrollo y Sostenibilidad: Un marco regional mejoraría la cooperación en temas como la investigación, el comercio electrónico y la ciberseguridad, promoviendo la integración económica y social de la región, y estimulando el desarrollo de sistemas de inteligencia artificial y tecnologías de uso intensivo de dados e de manera sostenible, basada en el Estado de derecho.

Armonización y Interoperabilidad Legislativa: Facilitaría el desarrollo de la protección de datos, armonizando las reglas y la gobernanza de dados entre los países que las tienen y ofreciendo un modelo para los que aún no las tienen. También facilitaría las transferencias internacionales de datos y la

compatíveis, sem necessidade de depender de uma organização intergovernamental preexistente. Por isso, podemos pensar que um esforço plurilateral liderado por um grupo reduzido de países abertos à colaboração com todos os estados da América Latina pode ser considerado uma opção potencialmente exitosa.

Benefícios de uma Convenção Regional

Direitos Fundamentais: Reafirmaria a proteção dos dados pessoais como um direito fundamental na América Latina, aumentando a credibilidade e a influência nos fóruns internacionais.

Cooperação, Desenvolvimento e Sustentabilidade: Um quadro regional melhoraria a cooperação em questões como a investigação, o comércio electrónico e a cibersegurança, promovendo a integração económica e social da região, e estimulando o desenvolvimento de sistemas de inteligência artificial e tecnologias de uso intensivo de dados e de forma sustentável, com base no Estado de direito.

Regulamento Unificado: Facilitaria o desenvolvimento da proteção de dados, harmonizando as regras e a governança de dados entre os países que existem e oferecendo um modelo para aqueles que ainda não existem. Facilitaria também as transferências internacionais de dados e a cooperação

cooperación entre autoridades de protección de datos.

Organismos y Mecanismos: La convención facilitaría la cooperación entre las autoridades reguladoras existentes y podría crear una Comisión Interamericana de Protección de Datos Personales (CIPDP) dentro de la OEA, que actuaría como un foro político y emisor de orientaciones, adaptándose a la complejidad y los cambios constantes en la materia.

Propuesta de Tratado

El tratado propuesto se basa en los Principios de la OEA de 2021, las del Mercosur de 2010 y otros estándares internacionales, como el Convenio 108 modernizado y el RGPD europeo, y de soft-law como los estándares de la Red Iberoamericana de Protección de Datos. El esquema del tratado incluye:

Definiciones y Principios Generales: Establece los objetivos y principios generales del tratado, como la protección de la privacidad y la seguridad en el tratamiento de datos.

Ámbito de Aplicación: Define quiénes están sujetos a sus disposiciones y qué tipos de datos personales están protegidos, incluyendo límites y condiciones para la recopilación de datos por razones de seguridad nacional .

Derechos de los Titulares: Establece derechos fundamentales como el acceso, rectificación, cancelación y oposición de datos, así como la

entre as autoridades de proteção de dados.

Organizações e Mecanismos: A convenção facilitaria a cooperação entre as autoridades reguladoras existentes e poderia criar uma Comissão Interamericana de Proteção de Dados Pessoais (CIPDP) dentro da OEA, que atuaria como fórum político e emissor de orientações, adaptando-se à complexidade e às constantes mudanças no assunto.

Proposta de Tratado

O tratado proposto baseia-se nos Princípios da OEA de 2021, as Medidas do Mercosul de 2010, e em outras normas internacionais, como a Convenção 108 modernizada e o GDPR europeu, e de soft-law como os padrões da Rede Iberoamericana de Proteção de Dados. O esboço do tratado inclui:

Definições e Princípios Gerais: Estabelece os objetivos e princípios gerais do tratado, como a proteção da privacidade e a segurança no tratamento de dados.

Âmbito de Aplicação: Define quem está sujeito às suas disposições e que tipos de dados pessoais são protegidos, incluindo limites e condições para recolha de dados por razões de segurança nacional.

Direitos dos Titulares: Estabelece direitos fundamentais como acesso, retificação, cancelamento e oposição de dados, bem como portabilidade e

portabilidad y protección en caso de decisiones automatizadas.

Obligaciones del Sector Público y Privado: Incluye medidas de seguridad, transparencia y responsabilidad, así como la designación de un encargado de protección de datos y evaluaciones de impacto.

Transferencias Internacionales: Regula las condiciones para la transferencia de datos entre países, garantizando el respeto a las normas establecidas.

Mecanismos de Cumplimiento: Prevé la creación de agencias independientes de protección de datos y la cooperación entre estas agencias para asegurar una aplicación uniforme del tratado.

proteção em caso de decisões automatizadas.

Obrigações do Setor Público e Privado: Inclui medidas de segurança, transparência e responsabilidade, bem como a nomeação de um encarregado de proteção de dados e avaliações de impacto.

Transferências Internacionais: Regula as condições de transferência de dados entre países, garantindo o respeito aos padrões estabelecidos.

Mecanismos de Conformidade: Dispõe sobre a criação de agências independentes de proteção de dados e a cooperação entre essas agências para garantir a aplicação uniforme do tratado.

Desafíos y Consideraciones

Reconociendo la complejidad de aprobar e implementar un proyecto de tal envergadura, subrayase que los beneficios superan los costos. Armonizar las regulaciones de protección de datos y promover la cooperación transfronteriza no solo mejora la seguridad cibernética y la resiliencia, sino que también posiciona a América Latina como líder en gobernanza de datos y cooperación digital. Aunque el esfuerzo diplomático necesario es considerable, los interesados en la región son conscientes de los beneficios de un marco compartido de protección de datos.

Vale la pena que Latinoamérica dé este paso importante. El esfuerzo no será

Desafios e Considerações

Reconhecendo a complexidade de aprovar e implementar um projeto desta magnitude, enfatiza-se que os benefícios superam os custos. Harmonizar as regulamentações de proteção de dados e promover a cooperação transfronteiriça não só melhora a segurança cibernética e a resiliência, mas também posiciona a América Latina como líder na governança de dados e na cooperação digital. Embora o esforço diplomático necessário seja considerável, as partes interessadas na região estão conscientes dos benefícios de um quadro partilhado de proteção de dados.

Vale a pena que a América Latina dê este importante passo. O esforço não será

fácil, pero es hora de ser audaces y ambiciosos para crear un instrumento verdaderamente latinoamericano para la gobernanza de datos con miras a garantizar un debido tratamiento de los datos de las personas en América Latina, criando un mercado latinoamericano de dados y un desarrollo tecnológico regional braseado en el derecho fundamental a la autodeterminación informativa.

fácil, mas é hora de sermos ousados e ambiciosos para criar um instrumento verdadeiramente latino-americano de governança de dados para garantir o tratamento adequado dos dados pessoais na América Latina, criando um mercado latino-americano de dados e um desenvolvimento tecnológico regional baseado no direito fundamental à autodeterminação informativa.

PROYECTO

CONVENCIÓN INTERAMERICANA SOBRE TRATAMIENTO DE DATOS PERSONALES, AUTODETERMINACIÓN INFORMATIVA Y CIRCULACIÓN DE ESA INFORMACIÓN

LOS ESTADOS PARTES DE LA PRESENTE CONVENCIÓN,

RECONOCIENDO que el respeto irrestricto a los derechos humanos y a la privacidad ha sido consagrado en la Declaración Americana de los Derechos y Deberes del Hombre y en la Declaración Universal de los Derechos Humanos y reafirmado en otros instrumentos internacionales y regionales;

RECORDANDO los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales redactados por el Comité Jurídico de la OEA en 2021;

PROJETO

CONVENÇÃO INTERAMERICANA SOBRE TRATAMENTO DE DADOS PESSOAIS, AUTODETERMINAÇÃO INFORMATIVA E CIRCULAÇÃO DE TAIS INFORMAÇÕES

OS ESTADOS PARTES DA PRESENTE CONVENÇÃO,

RECONHECENDO o respeito irrestrito para direitos humanos e privacidade foi consagrado pela Declaração Americana de Direitos e deveres do homem e pela Declaração Universal de Direitos Humanos e reafirmados em outros instrumentos internacionais e regionais;

LEMBRANDO os Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais elaborado pelo Comitê Jurídico da OEA em 2021 e afirmando que a proteção de dados pessoais transcende todos os setores do sociedade independentemente de sua nacionalidade, residência, classe, raça ou etnia, nível de renda, cultura, escolaridade, idade ou religião;

RECORDANDO que la Corte interamericana de Derechos Humanos ha reconocido el derecho a la autodeterminación informativa como un derecho autónomo en la sentencia Serie C No. 506 de 18 de octubre de 2023;

RECORDANDO que a Corte Interamericana de Direitos Humanos reconheceu o direito à autodeterminação informacional como direito autônomo na decisão Série C nº 506, de 18 de outubro de 2023;

AFIRMANDO que la infracción de los derechos a la privacidad y a la protección de los datos personalas es una violación de los derechos humanos y las libertades fundamentales y limita total o parcialmente a los titulares de datos el reconocimiento, goce y ejercicio de tales derechos y libertades y de otros derechos humanos;

DECLARANDO que a violação dos direitos à privacidade e à proteção de dados pessoais é uma violação de direitos humanos e de liberdades fundamentais e limita total ou parcialmente aos titulares de dados o reconhecimento, gozo e exercício de tais direitos e liberdades e de outros direitos humanos;

PREOCUPADOS porque la tecnología de la información esté al servicio de cada ciudadano, el desarrollo de la sociedad de la información se dé en el marco de la cooperación internacional y que ninguna tecnología atente contra los derechos humanos, ni la tutela de los datos personales, ni constituya una ofensa a la dignidad humana;

PREOCUPADOS que a tecnologia da informação esteja ao serviço de cada cidadão, que o desenvolvimento da sociedade da informação se dê em um quadro de cooperação internacional e que nenhuma tecnologia viole direitos humanos nem a tutela de dados pessoais, e não constitua uma ofensa à dignidade humana;

PREOCUPADOS porque los cada vez más frecuentes incidentes de seguridad en los sectores público y privado amenazan en la región la seguridad de los ciudadanos y les impiden disfrutar adecuadamente los beneficios del gobierno electrónico, de los servicios digitales y del desarrollo sostenible por medio de la tecnología de la información;

PREOCUPADOS que a ameaça cada vez mais frequente de incidentes de segurança nos setores público e privado afete a segurança dos cidadãos na região e os impeça de aproveitar adequadamente os benefícios do governo eletrônico, dos serviços digitais e do desenvolvimento sustentável por meio da tecnologia da informação;

CONVENCIDOS de que elevar el nivel de protección de los datos personales es una prioridad para la región y una condición indispensable para el desarrollo individual y social y su plena e igualitaria participación en todas las esferas de la sociedad de la información,

HAN CONVENIDO en lo siguiente:

CAPÍTULO I - ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1. Objetivos

1.1. La presente Convención tiene por objeto:

a) Fijar las reglas para garantizar el debido tratamiento de los datos personales y proteger los derechos de las personas titulares de esa información.

b) Facilitar el flujo de los datos personales entre los Estados miembros con la finalidad de coadyuvar al crecimiento social y económico y el desarrollo sostenible de la región.

c) Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los estados miembros, las autoridades de control de

CONVENCIDOS de que aumentar o nível de proteção de dados pessoais é uma prioridade para o região e uma condição essencial para o desenvolvimento individual e social e também para sua plena e igual participação em todas as esferas da sociedade da informação,

ACORDARAM o seguinte:

CAPÍTULO I - ÂMBITO DE APLICAÇÃO E DEFINIÇÕES

Artigo 1.º Objetivos

1.1. Esta Convenção tem como objeto:

a) Estabelecer as regras para garantir o devido tratamento do dados pessoais e proteger direitos dos titulares dessa informação.

b) Facilitar o fluxo de dados entre os Estados-Membros com o finalidade de contribuir para o crescimento social e econômico e para o desenvolvimento sustentável da região.

c) Promover o desenvolvimento de mecanismos para cooperação internacional entre as autoridades de supervisão dos Estados membros, as

estados no pertenecientes al Convenio y autoridades y entidades internacionales en la materia.

autoridades de supervisão dos Estados não membros desta Convenção e às autoridades e entidades internacionais neste assunto.

1.2. La protección de datos personales se basa en:

a. el respeto a la privacidad reconocido en el art. 11 de la Convención Americana de Derechos Humanos;

b. el derecho a la autodeterminación informativa;

c. la libertad de expresión, información, comunicación y opinión;

d. la inviolabilidad de la intimidad, del honor y de la imagen;

e. el desarrollo e innovación económica y tecnológica;

f. la libre empresa, libre competencia y protección del consumidor;

g. los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por las personas naturales.

1.2. A proteção de dados pessoais baseia-se:

a) no respeito a privacidade reconhecido no art. 11 do Convenção Americana sobre Direitos Humanos;

b. no direito à autodeterminação informacional;

c. na liberdade de expressão, informação, comunicação e opinião;

d. na inviolabilidade da privacidade, da honra e da imagem;

e. no desenvolvimento econômico e tecnológico e inovação;

f. na livre iniciativa, livre concorrência e proteção do consumidor;

g. nos direitos humanos , no livre desenvolvimento personalidade , na dignidade e no exercício de cidadania por pessoas naturais.

Artículo 2. Definiciones

Artigo 2. Definições

2.1. Para los efectos de esta Convención debe entenderse por:

2.1. Para os efeitos desta Convenção deve-se entender:

a. **Anonimización**: la aplicación de medidas de cualquier naturaleza

a. **Anonimização**: a aplicação de medidas de qualquer natureza

dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

b. **Consentimiento**: manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

c. **Datos Personales**: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

d. **Datos personales sensibles**: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan, entre otros, revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

e. **Encargado**: prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la

destinadas a prevenir a identificação ou reidentificação de uma pessoa física sem esforços desproporcionais;

b. **Consentimento**: manifestação de vontade livre, específica, inequívoca e informada do titular dos dados, através da qual aceita e autoriza o tratamento dos dados pessoais que lhe dizem respeito;

c. **Dados Pessoais**: qualquer informação relativa a uma pessoa física identificada ou identificável, expressa em forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica ou qualquer outra forma. Uma pessoa é considerada identificável quando é possível determinar direta ou indiretamente sua identidade, desde que isso não despenda prazo ou atividades desproporcionais.

d. **Dados pessoais sensíveis**: aqueles que se referem à esfera íntima de seu titular, ou cujo utilização indevida possa dar origem ou gere sério risco de discriminação. Por exemplo , são considerados dados pessoais sensíveis as informações que possam, entre outros, revelar aspectos como origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais; filiação sindical; opiniões políticas; dados relativos à saúde, vida, preferência ou orientação sexual, dados genéticos ou dados biométricos destinados a identificar de forma única uma pessoa natural.

e. **Operador:** prestador de serviços, pessoa física ou jurídica ou autoridade pública, sem relação com a organização

organización del responsable, trata datos personales a nombre y por cuenta de éste.

f. **Exportador**: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.

g. **Responsable**: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

h. **Titular del dato personal**: persona física a quien le conciernen los datos personales.

i. **Tratamiento**: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

controladora, que trata dados pessoais em nome e por conta deste último .

f. **Exportador**: pessoa física ou jurídica de direito privado, autoridade pública, serviço, organização ou prestador de serviços localizado em território de um Estado que realiza transferências dados internacionais pessoal, de acordo com disposto em estas Normas .

g. **Controlador**: pessoa física ou jurídica privada , autoridade pública, serviço ou órgão que, isoladamente ou em conjunto com outros, determina os fins, meios, escopo e demais questões relacionadas ao tratamento de dados pessoais.

h. **Titular dos dados pessoais** : pessoa física a quem se referem os dados pessoais.

i. **Tratamento** : qualquer operação ou conjunto de operações realizado através de procedimentos físicos ou automatizados realizados com dados pessoais, relacionados com, mas não limitados a obtenção, acesso, registro, organização, estruturação, adaptação, indexação, modificação, extração, consulta, armazenamento, conservação, elaboração , transferência, divulgação, posse, e, em geral, qualquer uso ou disposição de dados pessoais.

Artículo 3. Ámbito de aplicación subjetivo

3.1. Las obligaciones y derechos establecidos en esta Convención serán aplicables a las personas físicas, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones.

3.2. Las obligaciones y derechos establecidos en este Convenio serán aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

3.3. Las obligaciones y derechos establecidos en esta Convención serán aplicables a los datos personales de personas físicas, lo cual no impide que los Estados miembros en su legislación nacional dispongan que la información de las personas jurídicas sea salvaguardada acorde con el derecho a la protección de datos personales, en cumplimiento a lo establecido en su derecho interno.

3.4. Las obligaciones y derechos establecidos en este Convenio no son aplicables en los siguientes supuestos:

Artigo 3. Âmbito de aplicação subjetivo

3.1. As obrigações e direitos estabelecido nesta Convenção serão aplicáveis a pessoas físicas,

autoridades e órgãos públicos que lidam com dados pessoais no exercício de suas atividades e funções.

3.2. As obrigações e direitos estabelecidos nesta Convenção serão aplicáveis aos tratamentos de dados pessoais que estejam suporte físico ou digital, total ou parcialmente automatizados, ou em ambos os suportes, com independência da forma ou modalidade de sua criação, tipo de suporte, tratamento, armazenamento e organização.

3.3. As obrigações e direitos estabelecidos nesta Convenção serão aplicáveis ao dados pessoais de pessoas naturais, o que não impede que os Estados-Membros disponham em sua legislação nacional que as informações de pessoas jurídicas possam ser protegidas de acordo com o direito de proteção de dados pessoais, em conformidade com estabelecido em seu direito interno.

3.4. As obrigações e direitos estabelecido nesta Convenção não serão aplicáveis nas seguintes situações:

a. Cuando los datos personales estén destinados a actividades exclusivamente internas en el marco de la vida familiar o doméstica de una persona física, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como finalidade una divulgación o utilización comercial de dichos datos.

b. La información anónima en su origen, es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado.

a. Quando o dados pessoais destinarem-se exclusivamente a atividades internas em um contexto de vida familiar ou doméstica de uma pessoa natural, ou seja, a utilização de dados pessoal em ambiente de amizade, parentesco ou grupo pessoal próximo e que não tenham como finalidade a divulgação ou utilização comercial dos referidos dados .

b. As informações originariamente anônimas, isto é , aquelas que não estão relacionadas com pessoas naturais identificadas ou identificáveis , bem como dados pessoais submetido a um trato de anonimização, de tal forma que o titular não possa ser identificado ou reidentificado.

Artículo 4. Ámbito de aplicación territorial

4.1. Los derechos reconocidos en este Convenio serán aplicables al tratamiento de datos personales efectuado:

a. Por un responsable o encargado establecido en territorio de los Estados miembros.

b. Por un responsable o encargado no establecido en territorio de los Estados miembros, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados miembros, o bien, estén relacionadas con el control de su comportamiento, en la medida en

Artigo 4.º Âmbito de aplicação territorial

4.1. Os direitos reconhecidos nesta Convenção serão aplicáveis ao tratamento de dados pessoais realizado:

a. Por um controlador ou operador estabelecido em território dos Estados-Membros.

b. Por um controlador ou operador não estabelecido em território dos Estados-Membros, quando as atividades de tratamento estejam relacionadas à oferta de bens ou serviços destinados aos residentes dos Estados-Membros, ou que estejam relacionados com o controle de seu comportamento, na

que éste tenga lugar en los Estados miembros.

c. Por un responsable o encargado que no esté establecido en un Estado miembro pero que le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud de los principios del Derecho internacional público.

d. Por un responsable o encargado no establecido en territorio de alguno de los Estados miembros y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.

4.2. Para los efectos del presente Convenio, se entenderá por establecimiento el lugar de la administración central o principal del responsable o encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, con natura estable y permanente.

4.3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán

medida em que isto ocorra nos Estados-Membros.

c. Por um controlador ou operador não estabelecido em território dos Estados-Membros, mas que esteja sujeito à aplicação de uma legislação nacional, derivada da celebração de um contrato ou em virtude de princípios de Direito internacional público.

d. Por um controlador ou operador não estabelecido em território de qualquer dos Estados-Membros, e que utilize ou recorra a meios, automatizados ou não, localizados nesse território para tratar dados pessoais, a menos que estes meios sejam usados apenas para fins de trânsito de dados.

4.2. Para os efeitos desta Convenção, estabelecimento significará o local de administração central ou principal do controlador ou operador, que deve ser determinado com base em critérios objetivos e implicar o exercício efetivo de atividades de gestão que determinem as principais decisões sobre fins e meios dos tratamentos de dados pessoais que realiza, com natureza estável e permanente.

4.3. A presença e utilização de meios técnicos e tecnologias para o tratamento de dados pessoais ou atividades de tratamento não constituirão, em si mesmas, um estabelecimento principal e não serão

considerados como criterios determinantes para la definición del establecimiento principal del responsable o encargado.

considerados como critérios determinantes para a definição do estabelecimento principal do controlador ou operador.

CAPÍTULO II - PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO II - PRINCÍPIOS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS

Artículo 5. Principio de legitimación

Artigo 5. Princípio da legitimação

5.1. Por regla general, el Responsable sólo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos:

a. El titular otorgue su consentimiento expreso para una o varias finalidades específicas.

b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.

c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una habilitación legal.

d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.

5.1. Como regra geral, o Controlador apenas poderá tratar dados pessoais quando estiver presente alguma destas hipóteses:

a. O titular concede seu consentimento expresso para um ou mais finalidades específicos.

b. O tratamento seja necessário para cumprimento de ordem judicial, resolução ou mandado fundamentado e motivado de autoridade pública competente.

c. O tratamento seja necessário para exercício de poderes das autoridades públicas ou é realizado em em virtude de autorização legal.

d. O tratamento seja necessário para o reconhecimento ou defesa de direitos do titular perante uma autoridade pública.

e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.

f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.

g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.

h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley.

i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones legales.

e. O tratamento seja necessário para execução de um contrato ou pré-contrato do qual o titular é uma parte.

f. O tratamento seja necessário para cumprimento de obrigação legal aplicável ao controlador.

g. O tratamento seja necessário para proteger interesses vitais do titular ou de outra pessoa natural.

h. O tratamento seja necessário por razões de interesse público estabelecido ou previsto em lei.

i. O tratamento seja necessário para satisfação dos interesses legítimos perseguidos pelo controlador ou por um terceiro, desde que os referidos interesses não prevaleçam sobre os interesses ou direitos e liberdades fundamentais do titular que requeira a proteção de dados pessoais, especialmente quando o titular seja criança ou adolescente. O acima exposto não será aplicável aos tratamentos de dados pessoais realizados por autoridades públicas no exercício de suas funções legais.

Artículo 6. Condiciones para el consentimiento

6.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

6.2. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos.

Artigo 6. Condições para consentimento

6.1. Quando for necessária a obtenção do consentimento do titular, o controlador demonstrará de maneira inequívoca que o titular concedeu seu consentimento, seja através de uma declaração ou de uma ação afirmativa clara.

6.2. Sempre que necessário o consentimento para o tratamento dos dados pessoais , o titular poderá revogá-lo a qualquer momento, através de mecanismos simples , ágeis , eficazes e gratuitos estabelecidos pelo controlador.

Artículo 7. Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes

7.1. En la obtención del consentimiento de niñas, niños y adolescentes, el responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto en las reglas de representación previstas en el derecho interno de los Estados miembros, o en su caso, solicitará directamente la autorización del menor de edad si el derecho interno de cada Estado miembro ha establecido una edad mínima para que lo pueda otorgar

Artigo 7. Consentimento para tratamento de dados relacionados a crianças ou adolescentes

7.1. Na obtenção do consentimento de crianças ou adolescentes, o controlador deverá obter a autorização do detentor do poder familiar ou de tutela do menor, de acordo com disposto em as regras de representação previstas no direito interno dos Estados-membros, ou, caso seja possível, solicitar diretamente a autorização ao menor se o direito interno de cada Estado- Membro estabelecer uma idade mínima para que o menor possa concedê-lo diretamente

directamente y sin representación alguna del titular de la patria potestad o tutela.

e sem representação do detentor de poder familiar ou tutela.

7.2. El responsable realizará esfuerzos razonables para verificar que el consentimiento fue otorgado por el titular de la patria potestad o tutela, o bien, por el menor directamente atendiendo a su edad de acuerdo con el derecho interno de cada Estado-Membro, teniendo en cuenta la tecnología disponible.

7.2. O controlador deverá, considerando a tecnologia disponível, empreender esforços razoáveis para verificar que o consentimento foi concedido pelo detentor do poder familiar ou da tutela, ou pelo menor diretamente nos casos em que atenda ao critério etário de acordo com direito interno de cada Estado-membro.

7.3. El tratamiento de datos personales de niños, niñas y adolescentes debe realizarse en su interés superior, de conformidad con el artículo 21 de esta Convención.

7.3. Os tratamentos de dados pessoais de crianças ou adolescentes devem ser realizados em seu melhor interesse, de acordo com o artigo 21 desta Convenção.

Artículo 8. Principio de licitud

Artigo 8. Princípio da legalidade

8.1. El responsable tratará los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado Iberoamericano que resulte aplicable, el derecho internacional y los derechos y libertades de las personas.

8.1. O controlador tratará os dados pessoais em sua posse com a estrita observância e cumprimento do direito interno do Estado-Membro aplicável, do direito internacional e direitos e liberdades das pessoas.

8.2. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que el derecho interno del Estado Iberoamericano de que se trate les confiera expresamente, además de lo

8.2. O tratamento de dados pessoais realizado por autoridades públicas estarão sujeitos à poderes ou atribuições conferidos expressamente pelo direito interno do Estado-Membro

previsto en el numeral anterior de los presentes Estándares.

em questão, além do que está previsto no artigo anterior desta Convenção.

Artículo 9. Principio de lealtad

Artigo 9. Princípio da lealdade

9.1. El responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.

9.1. O controlador tratará os dados pessoais em sua posse privilegiando a proteção dos interesses do titular e abstendo-se de tratá-los por meios enganosos ou fraudulentos.

9.2. Para los efectos de los presentes Estándares, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.

9.2. Para os efeitos desta Convenção, serão considerados desleais aqueles tratamentos de dados pessoais que dêem origem a uma discriminação injusta ou arbitrária contra os titulares.

Artículo 10. Principio de transparencia

Artigo 10. Princípio da transparência

10.1. El responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

10.1. O controlador informará ao titular sobre a existência e principais características dos tratamentos a que serão submetidos seus dados pessoais, visando possibilitar a tomada de decisões informadas a respeito.

10.2. El responsable proporcionará al titular, al menos, la información siguiente:

10.2. O controlador fornecerá ao titular, pelo menos, as seguintes informações:

a. Su identidad y datos de contacto.

a. Sua identidade e dados para contato;

b. Las finalidades del tratamiento a que serán sometidos sus datos personales.

b. As finalidades do tratamento a que serão submetidos os seus dados pessoais;

c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.

c. As comunicações de dados pessoais, nacionais ou internacionais, que pretenda realizar, incluindo os destinatários e as finalidades que motivam o realização das mesmas.

d. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos definidos por el Artículo 20 de esta Convención.

d. A existência, forma e mecanismos ou procedimentos através dos quais será possível o exercício dos direitos definidos pelo artigo 20 desta Convenção.

e. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

e. A origem do dados pessoais quando o controlador não os tenha coletado diretamente do titular.

10.3. La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

10.3. As informações fornecidas ao titular devem ser suficientes e facilmente acessíveis, bem como escritas e estruturadas em linguagem clara, simples e de fácil compreensão para os titulares a quem sejam dirigidas, especialmente quando se tratar de crianças ou adolescentes.

10.4. Todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.

10.4. Todo controlador deverá ter políticas transparentes sobre os tratamentos de dados pessoais que realize.

Artículo 11. Principio de finalidad

Artigo 11. Princípio da finalidade

11.1. Todo tratamiento de datos personales se limitará al cumplimiento

11.1. Todo o tratamento de dados os dados pessoais será limitado ao

de finalidades determinadas, explícitas y legítimas.

cumprimento de finalidades específicas, explícitas e legítimas.

11.2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

11.2. O controlador não poderá tratar o dados pessoais em sua posse para fins distintos daqueles que motivaram seu tratamento original, a menos que haja alguma das causas que permitam um novo tratamento de dados em acordo com o princípio da legitimação.

11.3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

11.3. Os tratamentos ulteriores de dados pessoais para fins de arquivo, investigação científica e histórica ou para fins estatísticos, todos eles, em prol do interesse público , não serão considerados incompatíveis com os finalidades iniciais.

Artículo 12. Principio de proporcionalidad

Artigo 12. Princípio da proporcionalidade

12.1. El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

12.1. O controlador somente tratará dados pessoais adequados, relevantes e limitados ao mínimo necessário em relação aos fins que justifiquem seu tratamento.

Artículo 13. Principio de calidad

Artigo 13. Princípio de qualidade

13.1. El responsable adoptará las medidas necesarias para mantener

13.1. O controlador adotará as medidas necessárias para manter a precisão,

exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento. La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada y comprobable. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

completude e atualização dos dados pessoais em sua posse, de tal forma que não se altere sua veracidade, conforme exigido para o cumprimento das finalidades que motivaram o tratamento. A informação sujeita ao tratamento deve ser verdadeira, completa, exata , atualizada e verificável. É proibido o tratamento de dados parciais, incompletos, fragmentados ou enganosos;

13.2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

13.2. Quando os dados pessoais deixarem de ser necessários para cumprimento das finalidades que motivaram seu tratamento, o controlador irá excluí-los ou eliminá-los de seus arquivos, registros, bancos de dados ou sistemas de informação, ou , se for o caso, irá submetê-los a um processo de anonimização.

13.3. En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

13.3. No processo de exclusão dos dados pessoais, o controlador implementará métodos e técnicas visando eliminação definitiva e segura destes.

13.4. Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. No obstante, la legislación nacional de los Estados miembros aplicable en la materia podrá establecer

13.4. Os dados pessoais apenas deverão ser mantidos durante o prazo necessário para o cumprimento dos fins que justificam seu tratamento ou daqueles relacionados a requisitos legais aplicáveis ao controlador. Não obstante, a legislação nacional dos Estados-Membros poderá estabelecer exceções quanto ao período de conservação dos

excepciones respecto al plazo de conservación de los datos personales, con pleno respeto a los derechos y garantías del titular.

dados pessoais, respeitados os direitos e garantias do titular.

Artículo 14. Principio de responsabilidad demostrada

Artigo 14. Princípio da responsabilidade comprovada

14.1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

14.1. O controlador implementará mecanismos necessários para comprovar a conformidade com os princípios e obrigações estabelecidos nesta Convenção, bem como prestará contas sobre os tratamentos de dados pessoais em sua posse ao titular e à autoridade de controle, podendo utilizar-se de padrões técnicos, melhores práticas nacionais ou internacionais, sistemas de autorregulação, sistemas de certificação ou qualquer outro mecanismo que determine ser apropriado para tais fins.

14.2. Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

14.2. O artigo anterior será aplicado quando os dados pessoais forem tratados por um operador em nome e por conta de do controlador, bem como no momento de transferências de dados pessoal .

14.3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

14.3. Entre os mecanismos que controlador pode adotar para cumprir com o princípio da responsabilidade comprovada inclui, mas não está limitado, ao seguinte:

a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.

c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

14.4. El responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

a. Alocar recursos para implementação de programas e políticas de proteção de dados pessoais;

b. Implementar sistemas de gestão de riscos associado ao tratamento de dados pessoais;

c. Desenvolver políticas e programas de proteção de dados pessoais obrigatória e exequível dentro do organização do controlador .

d. Colocar em prática um programa de treinamento e atualização de pessoal sobre obrigações relacionadas à proteção de dados pessoais.

e. Revisar periodicamente políticas e programas de segurança de dados pessoais para determinar as modificações que forem necessárias;

f. Estabelecer um sistema de supervisão e vigilância interno e/ou externo , incluindo auditorias, para verificar a conformidade com políticas de proteção de dados pessoais;

g. Estabelecer procedimentos para receber e responder às dúvidas e reclamações de titulares.

14.4. O controlador deverá revisar e avaliar permanentemente os mecanismos que adotar voluntariamente para o efeito de cumprimento do princípio da responsabilidade comprovada, com a finalidade de mensurar seu nível de

	eficácia em relação ao cumprimento legislação nacional aplicável.
Artículo 15. Principio de seguridad	**Artigo 15. Princípio da segurança**
15.1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.	**15.1.** O controlador estabelecerá e manterá, independentemente do tipo de tratamento realizado, medidas administrativas, físicas e técnicas suficientes para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais.
15.2. Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores:	**15.2.** Para a determinação das medidas referidas no inciso anterior, o controlador considerará o seguintes fatores:
a. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	a. O risco para direitos e liberdades dos titulares, em particular, devido ao potencial valor quantitativo e qualitativo que poderiam ter os dados pessoais tratados por um terceiro não autorizado;
b. El estado de la técnica.	b. O estado atual da técnica;
c. Los costos de aplicación.	c. Custos de implementação;
d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.	d. A natureza do dados pessoais tratados, especialmente quando envolver dados pessoais sensíveis;
e. El alcance, contexto y las finalidades del tratamiento.	e. O escopo, o contexto e os finalidades do tratamento;
f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.	f. As transferências internacionais de dados pessoais que serão realizadas ou que se pretendam realizar;

g. El número de titulares.	g. O número de titulares envolvidos;
h. Las posibles consecuencias que se derivarían de una vulneración para los titulares.	h. As possíveis consequências para os titulares que poderiam sugir de uma violação;
i. Las vulneraciones previas ocurridas en el tratamiento de datos personales.	i. As violações anteriores que ocorreram no tratamento de dados pessoais.
15.3. El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.	**15.3.** O controlador realizará uma série de ações que garantirão o estabelecimento , implementação , operação , monitoramento , revisão , manutenção e melhoria contínua das medidas de segurança aplicáveis ao tratamento de dados pessoais periodicamente.

Artículo 16. Notificación de vulneraciones a la seguridad de los datos personales	**Artigo 16. Notificação de violações à segurança dos dados pessoais**
16.1. Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna.	**16.1.** Quando o controlador tiver conhecimento de uma violação à segurança de dados pessoais ocorrido em qualquer fase de tratamento, entendida como qualquer dano, perda, alteração, destruição, acesso e, em geral, qualquer uso ilícito ou não autorizado de dados pessoais, ainda quando ocorrerer de uma maneira acidental, deverá notificar a autoridade de controle e os titulares afetados pelo evento, sem atraso.
16.2. Lo anterior, no resultará aplicable cuando el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la vulneración de seguridad ocurrida, o bien, que ésta no represente un riesgo para los derechos y las libertades de los titulares involucrados	**16.2.** O inciso anterior não será aplicável quando o controlador puder demonstrar, tendo em conta o princípio da responsabilidade comprovada, a improbabilidade da violação de segurança ocorrida ou que esta não representa um risco aos direitos e liberdades dos titulares envolvidos.
16.3. La notificación que realice el responsable a los titulares afectados estará redactada en un lenguaje claro y sencillo.	**16.3.** A notificação realizada pelo controlador aos titulares afetados será escrita em a linguagem clara e simples.
16.4. La notificación a que se refieren los numerales anteriores contendrá, al menos, la siguiente información:	**16.4.** A notificação a que se referem os incisos anteriores conterão, pelo menos, as seguintes informações:

a. La naturaleza del incidente.

b. Los datos personales comprometidos.

c. Las acciones correctivas realizadas de forma inmediata.

d. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses.

e. Los medios disponibles al titular para obtener mayor información al respecto.

a. A natureza do incidente;

b. Os dados pessoais comprometido;

c. As medidas corretivas realizadas imediatamente;

d. As recomendações ao titular sobre as medidas que possam adotar para proteger os seus interesses;

e. Os meios disponíveis ao titular para obter maiores informações a respeito.

16.5. El responsable documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la autoridad de control.

16.5. O controlador documentará qualquer violação de segurança aos dados pessoais ocorrida em qualquer fase de tratamento, identificando, mas não se limitando, à data em que ocorreu; o motivo da violação; os fatos relacionados e seus efeitos e também as medidas corretivas implementadas imediata e definitivamente, o que deverá estar disponível para autoridade de controle.

16.6. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá los efectos de las notificaciones de vulneraciones de seguridad que realice el responsable a la autoridad de control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con el finalidade de salvaguardar los intereses, derechos y libertades de los titulares afectados.

16.6. A legislação nacional dos Estados-Parte aplicável estabelecerá os efeitos das notificações de violações de segurança feitas pelo controlador às autoridades de controle no que se refere a procedimentos, forma e condições do sua intervenção, com a finalidade de salvaguardar interesses, direitos e liberdades dos titulares afetados.

Artículo 17. Principio de confidencialidad	**Artigo 17. Princípio da confidencialidade**
17.1. El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.	**17.1.** O controlador estabelecerá controles ou mecanismos para que quaisquer intervenientes, em qualquer fase de tratamento do dados pessoais, mantenham e respeitem a confidencialidade dos mesmos, uma obrigação que subsistirá mesmo após o término seu relacionamento com o titular.
Artículo 18. Principio de precaución	**Artigo 18. Princípio da precaução**
18.1. En caso de presentarse falta de certeza frente a los potenciales daños del tratamiento de datos personales, y con miras a evitar que se cause un daño grave e irreversible, el Responsable o Encargado del tratamiento deberán abstenerse de realizar dicho tratamiento o adoptar medidas precautorias o preventivas para proteger los derechos del titular del dato, su dignidad humana y otros derechos humanos.	18.1. Em caso de falta de certeza quanto ao potenciais danos do tratamento de dados pessoais, e com o objetivo de evitar causar um danos graves e irreversíveis, o controlador ou operador deverá se abster de realizar o tratamento ou adotar medidas de precaução ou preventivas para proteger os direitos do titular dos dados, sua dignidade humana e outros direitos humanos.
18.2. El principio de precaución también se aplica cuando el riesgo o la magnitud del daño producido o que puede sobrevenir no son conocidos con anticipación, porque no hay manera de establecer, a mediano o largo plazo, los efectos de un tratamiento de datos.	18.2. O princípio da precaução também se aplica quando o risco ou magnitude do dano produzido ou que possa ocorrer não são previstos, por não existir forma de estabelecer, a médio ou longo prazo, os efeitos de um tratamento de dados.

CAPÍTULO III - DERECHOS PROTEGIDOS

Artículo 19. Derecho a la protección de los datos personales

19.1. Toda persona tiene derecho a la protección de sus datos personales y la autodeterminación informativa de conformidad con las normas de este Convenio. Dichos derechos se concretan en la facultad de toda persona para ejercer control sobre sus datos personales, que se tratarán de modo leal, para fines explícitamente definidos sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.

19.2. A toda persona cuyos datos sean tratados son garantizados los derechos definidos por el Artículo 20 de esta Convención. Las autoridades reguladoras independientes designadas por cada Estado miembro son responsables para garantizar el pleno respeto de estos derechos.

Artículo 20. Derechos

20.1. Toda persona tendrá derecho a:

CAPÍTULO III - DOS DIREITOS PROTEGIDOS

Artigo 19. Direito de proteção do dado pessoal

19.1. Toda pessoa tem direito à proteção dos seus dados pessoais e à autodeterminação informativa em conformidade com as regras desta Convenção. Ditos direitos são concretizados com a faculdade de cada pessoa exercer controle sobre seus dados pessoais, que serão tratados de forma leal, para fins explicitamente definidos com base no consentimento da pessoa afetada ou em virtude de outra base legítima prevista pela lei.

19.2. A todas as pessoas cujos dados sejam tratados serão garantidos os direitos definidos pelo artigo 20 desta Convenção. As autoridades reguladoras independentes designadas por cada Estado-Membro serão responsáveis por garantir total respeito a estes direitos.

Artigo 20. Direitos

20.1. Toda pessoa terá direito a:

a. no estar sujeto a una decisión que lo afecte significativamente, basándose únicamente en un tratamiento automatizado de datos sin considerar sus opiniones. Esta norma no será aplicable si la decisión ha sido autorizada por una ley a la cual el responsable del tratamiento está sujeto siempre y cuando esta ley establezca medidas apropiadas para garantizar los derechos, las libertades e intereses legítimos del titular de datos;

b. obtener, cuando así lo solicitare, en intervalos razonables y sin demora o gastos excesivos, confirmación del tratamiento de los datos personales relacionados con su persona, la comunicación en forma inteligible de los datos tratados, toda la información disponible sobre su origen, el período de conservación así como cualquier otra información que el responsable del tratamiento deba proporcionar con el fin de asegurar la transparencia del tratamiento incluyendo las medidas de seguridad adoptadas sobre sus datos personales;

c. obtener, cuando así lo solicitare, conocimiento del razonamiento subyacente al tratamiento de datos cuando los resultados de dicho tratamiento se le aplicaren;

d. oponerse en cualquier momento, por fundamentos relacionados con su situación, al tratamiento de datos personales que lo involucren, salvo si el responsable del tratamiento demostrara fundamentos legítimos para el tratamiento superiores

a. não estar sujeita a uma decisão que a afete significativamente, baseada apenas em a um tratamento automatizado de dados sem considerar suas opiniões. Esta regra não será aplicável se a decisão foi autorizada por lei a qualo controlador está sujeito e quando esta lei estabelecer medidas adequadas para garantir direitos, liberdades e interesses legítimos do titular dos dados;

b. obter , quando assim o solicitar, em intervalos razoáveis e sem demora ou despesas excessivas, a confirmação do tratamento do dados pessoais relacionados à sua pessoa, a comunicação de forma inteligível dos dados tratados, todas as informações disponíveis sobre sua origem, o período de conservação, bem como qualquer outra informação que o controlador deva fornecer a fim de garantir o transparência do tratamento, incluindo as medidas de segurança adotadas sobre seus dados pessoais;

c. obter , quando assim o solicitar, conhecimento da fundamentação subjacente ao tratamento dos dados quando os resultados do referido tratamento se lhe aplicarem;

d. opor-se a qualquer momento, por motivos relacionados à sua situação, ao tratamento de dados pessoal que lhe envolva, a menos que controlador demonstre motivos legítimos para o tratamento superior aos seus interesses, direitos ou liberdades fundamentos;

a sus intereses o derechos o libertades fundamentales;

e. obtener, cuando así lo solicitare, exento de costos y sin demoras excesivas, la rectificación o eliminación, según sea el caso, de dichos datos si estos estuvieron siendo o hubieren sido tratados en forma contraria a las disposiciones del presente Convenio;

e. obter , quando assim o solicitar, sem custos e sem demoras excessivas, a retificação ou eliminação, conforme o caso, dos referidos dados se estes foram ou estiveram sendo tratados de maneira contrária à disposições desta Convenção;

f. obtener una solución jurídica según lo previsto en el Artículo 26 de este Convenio cuando sus derechos de conformidad con el presente Convenio hubieren sido violados;

f. obter uma solução jurídica de acordo com o que está previsto Artigo 26 desta Convenção quando seus direitos de conformidade com esta forem violados;

g. beneficiarse, cualquiera sea su nacionalidad o residencia, de la asistencia de una autoridad de control según lo dispuesto en el Artículo 26 de este Convenio, para ejercer sus derechos de conformidad con el presente Convenio.

g. beneficiar-se, qualquer que seja sua nacionalidade ou residência, da assistência de uma autoridade supervisora de acordo com o disposto no Artigo 26 desta Convenção, para exercer seus direitos;

h. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

h. Quando houver tratamento de dados pessoais por meio eletrônico ou automatizado, o titular terá direito a obter uma cópia dos dados pessoais que tenham sido fornecidos ao controlador ou que sejam objeto de tratamento, em um formato eletrônico estruturado, comumente usado e leitura mecânica, que permita continuar seu uso e transferí-los para outro controlador, nos casos em que exigir;

i. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tiene derecho a solicitar la revisión de decisiones adoptadas únicamente sobre la base del tratamiento automatizado de datos personales que afecten a sus intereses,

i. Quando houver tratamento de dados pessoais por meio eletrônico ou automatizado, o titular terá direito de solicitar a revisão de decisões tomadas exclusivamente com base na tratamento automatizado de dados que afetam seus interesses , incluindo as decisões que

incluidas las decisiones destinadas a definir su perfil personal, profesional, de consumo y crediticio o aspectos de su personalidad. Consiguientemente, el responsable del tratamiento deberá brindar, cuando se le solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, observando secretos comerciales e industriales

visam definir o seu perfil pessoal, profissional , de consumo e de crédito ou aspectos de sua personalidade. Consequentemente , o controlador deverá fornecer, quando solicitado, informações claras e adequadas sobre o critérios e procedimentos utilizados para a decisão automatizada, observando segredos comerciais e industriais

20.2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

20.2. O titular poderá solicitar que seus dados pessoais sejam transferidos diretamente de um controlador para outro controlador, quando for tecnicamente possível. O direito de portabilidade de dados pessoais não afetará negativamente os direitos e liberdades.

20.3. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

20.3. Sem prejuízo aos outros direitos do titular, o direito à portabilidade de dados pessoais não procederá quando se tratar de informações inferidas, derivadas, criadas, geradas ou obtidas a partir da análise ou tratamento realizado pelo controlador com base nos dados dados pessoais fornecidos pelo titular, como é o caso dos dados pessoais que tenham sido submetidos a uma tratamento de personalização, recomendação, categorização ou criação de perfil.

20.4. Los Estados miembros deberán otorgar a toda persona recursos

20.4. Estados- Membros deverão conceder a todas as pessoas recursos

judiciales efectivos para la tutela de los derechos reconocidos en este Convenio, incluida la indemnización por el tratamiento no autorizado de sus datos personales o en infracción a los derechos reconocidos.

judiciais eficazes para a proteção dos direitos reconhecido nesta Convenção, incluindo a indenização por tratamento não autorizado de dados pessoais ou violação de direitos reconhecida.

20.5. La legislación nacional de los Estados miembros aplicable en la materia reconocerá el derecho que tiene el titular a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación de su derecho a la protección de datos personales.

20.5. A legislação nacional dos Estados-Membros aplicável reconhecerá o direito do titular a ser indenizado quando houver sofrido danos e prejuízos, como consequência de uma violação de seu direito de proteção aos dados pessoais.

20.6. El derecho interno de los Estados miembros señalará la autoridad competente para conocer de este tipo de acciones interpuestas por el titular afectado, así como los plazos, requerimientos y términos a través de los cuales será indemnizado éste, en caso de resultar procedente.

20.6. O direito interno dos Estados-Membros indicará a autoridade competente para conhecer este tipo de ação interposta pelo titular afetado, bem como os prazos, requisitos e condições através do quais será indenizado em caso de procedência.

Artículo 21. Tratamiento de datos personales de niñas, niños y adolescentes

Artigo 21. Tratamento de dados pessoais de crianças ou adolescentes

21.1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes, los Estados miembro del Convenio deberán privilegiar la protección del interés superior de éstos, conforme a la Convención sobre los

21.1. No tratamento de dados pessoais relativos às crianças ou adolescentes, os Estados- Membros da Convenção deverão privilegiar a proteção de seu melhor interesse, em conformidade com a Convenção sobre Direitos do Criança e

Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.	outros instrumentos internacionais que buscam seu bem-estar e proteção abrangente .
21.2. Los Estados miembros promoverán en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.	**21.2.** Estados-Membros promoverão, na formação acadêmica de crianças e adolescentes, o uso responsável, adequado e seguro de tecnologias do informação e comunicação e eventuais riscos que possam enfrentar em ambientes digitais relacionados ao tratamento indevido de seus dados pessoais, bem como o respeito pelos seus direitos e liberdades.

Artículo 22. Tratamiento de datos personales de carácter sensible

22.1. Por regla general, el responsable no podrá tratar datos personales sensibles, salvo que se presente cualquiera de los siguientes supuestos:

a. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación.

b. Se dé cumplimiento a un mandato legal.

c. Se cuente con el consentimiento expreso y por escrito del titular.

d. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

22.2. La legislación nacional de los Estados miembros aplicable en la materia podrá establecer excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles, de conformidad con su derecho interno.

Artículo 23. Excepciones y restricciones

Artigo 22. Tratamento de dados pessoais sensíveis

22.1. Como regra geral, o controlador não poderá tratar dados pessoais sensíveis, exceto quando atender a qualquer um destes requisitos:

a. Os mesmos sejam estritamente necessários para o exercício e cumprimento de poderes e obrigações expressamente previsto nas normas que regulem sua atuação;

b. Para cumprimento de ordem legal.

c. Através do consentimento expressa e por escrito do titular.

d. Caso sejam necessários por razões de segurança nacional, segurança pública, ordem pública, saúde pública ou salvaguarda dos direitos e liberdades de terceiros.

22.2. A legislação nacional dos Estados-Membros aplicável poderá estabelecer exceções, garantias e condições adicionais para garantire o devido tratamento de dados pessoais sensíveis, de acordo com seu direito interno.

Artigo 23. Exceções e restrições

23.1. No se permitirá excepción alguna a las disposiciones establecidas en este Capítulo, salvo que dicha excepción se encuentra prevista por la ley, respeta la esencia de los derechos consagrados en el Artículo 1 de este tratado y las libertades fundamentales y constituye una medida necesaria y proporcionada en una sociedad democrática para:

a. proteger la seguridad nacional, la defensa, la seguridad pública, los intereses económicos y financieros importantes del Estado, la imparcialidad e independencia del poder judicial o la prevención, investigación y procesamiento de delitos, así como la aplicación de sanciones penales, y otros objetivos esenciales de interés público general;

b. proteger al titular de datos o los derechos y las libertades fundamentales de otros, en particular, la libertad de expresión.

23.2. Las restricciones para ejercer las disposiciones especificadas en los Artículos 18 y 19 pueden ser previstas por la ley, con respecto al tratamiento de datos con el finalidade de archivo en interés público, investigaciones científicas o históricas o finalidades estadísticos cuando no exista riesgo identificable de violación de los derechos y las libertades fundamentales de los titulares de datos.

23.1. Nenhuma exceção será permitida às disposições estabelecidas neste Capítulo, salvo se dita exceção, prevista no lei, respeite a essência de direitos consagrados no artigo 1º desta Convenção e também as liberdades fundamentais, além de constituir uma medida necessária e proporcional numa sociedade democrática para:

a. proteção da segurança nacional, defesa, segurança Pública, importantes interesses econômicos e financeiros do Estado, a imparcialidade e independência do Poder Judiciário ou da prevenção, investigação e repressão de crimes, bem como a aplicação de sanções penais e outros objetivos essenciais de interesse público geral;

b. proteger o titular dos dados ou direitos e liberdades fundamentos de outros, em particular, a liberdade de expressão.

23.2. As restrições para o exercício das disposições especificadas nps artigos 18 e 19 podem ser previstos por lei, com respeito ao tratamento de dados com a finalidade de arquivo no interesse público, investigação científica ou histórica ou fins estatísticos quando não há risco identificável de violação de direitos e liberdades fundamentais dos titulares de dados.

23.3. Las actividades de tratamiento con finalidades de seguridad nacional y defensa estén sujetas a revisión y supervisión independiente y efectiva, según las leyes locales de la Parte pertinente.

23.3. As atividades de tratamento para fins de segurança e defesa nacional estão sujeitas a revisão e supervisão independente e eficaz, de acordo com as leis locais do Estado-Parte.

CAPÍTULO IV - OBLIGACIONES

CAPÍTULO IV - DAS OBRIGAÇÕES

Artículo 24. Obligaciones

Artigo 24. Obrigações

24.1. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento, tomen todas las medidas necesarias para cumplir con las obligaciones del presente Convenio y sean capaces de demostrar, sujetos a las leyes locales, que el tratamiento de datos bajo su control cumple con las disposiciones del presente Convenio

24.1. Cada Estado-Parte deverá providenciar que os controladores e, se for o caso , os operadores, tomem todas as medidas necessárias para cumprir com as obrigações desta Convenção e sejam capazes de demonstrar, sujeito às leis locais, que o tratamento de dados sob seu controle cumpre com as disposições desta Convenção.

24.2. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento, examinen el probable impacto del tratamiento de datos sobre los derechos y las libertades fundamentales de los titulares de datos, previo al comienzo de dicho tratamiento, y deberán diseñar el tratamiento de datos de manera tal que se prevenga o minimice el riesgo de interferencia con dichos derechos o libertades fundamentales.

24.2. Cada Estado-Parte deverá providenciar que os controladores e, se for o caso , os operadores, examinem o impacto provável de tratamento de dados sobre direitos e liberdades fundamentais dos titulares dos dados, antes do início do referido tratamento, e deverão projetar o tratamento de forma a prevenir ou minimizar o risco de interferência em direitos ou liberdades fundamentais.

24.3. Cada Parte deberá prever que los responsables del tratamiento y, si correspondiere, los encargados del tratamiento, implementen medidas técnicas y organizacionales que tomen en cuenta las implicancias del derecho a la protección de datos personales en todas las etapas del tratamiento de datos.

24.3. Cada Estado-Parte deverá providenciar que os controladores e, se for o caso , os operadores, implementem medidas técnicas e organizacionais que levem em conta as implicações do direito de proteção de dados pessoais em todas as etapas tratamento de dados.

24.4. Cada Parte podrá, teniendo en consideración los riesgos en relación con los intereses, derechos y libertades fundamentales de los titulares de datos, adaptar la aplicación de las disposiciones de los párrafos 1, 2 y 3 en la ley que dote de eficacia a las disposiciones del presente Convenio, según la naturaleza y el volumen de los datos, la naturaleza, el alcance y el finalidade del tratamiento y, si correspondiere, el tamaño del responsable del tratamiento o encargado del tratamiento.

24.4. Cada Estado-Parte poderá, considerando os riscos em relação aos interesses, direitos e liberdades fundamentais dos titulares dos dados, adaptar a aplicação das disposições do incisos 1, 2 e 3 na lei que torne eficaz as disposições desta Convenção, de acordo com o a natureza e o volume do dados, a natureza, escopo e finalidade do tratamento e, se for o caso, o tamanho controlador ou do operador.

CAPÍTULO V - TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Artículo 25. Reglas generales para las transferencias de datos personales

25.1. El responsable y encargado podrán realizar transferencias internacionales

CAPÍTULO V - TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

Artigo 25. Regras gerais para transferências de dados pessoais

25.1. O controlador e o operador poderão fazer transferências

de datos personales en cualquiera de los siguientes supuestos:

a. El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de éste que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado, siendo el respeto de las disposiciones de esta Convención considerado como garantía de tales condiciones mínimas y suficientes.

b. El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado miembro aplicable en la materia.

c. El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados aplicable en la materia.

internacionais de dados pessoais em qualquer uma das seguintes hipóteses:

a. O país, parte de seu território, setor, atividade ou organização internacional destinatário dos dados pessoais tiver sido reconhecido com um nível proteção de dados adequada pelo país exportador, de acordo com o legislação nacional deste que seja aplicável, ou seja o país destinatário ou vários setores do mesmo demonstrem condições mínimas e suficientes para garantir um nível de proteção de dados pessoais adequado, sendo o respeito às disposições desta Convenção considerado como garantia de tais condições mínimas e suficientes.

b. O exportador ofereça garantias suficientes de tratamento do dados pessoais no país destinatário, e isso, por sua vez, demonstre o cumprimento das condições mínimas e suficientes estabelecidas na legislação nacional de cada Estado -Membro aplicável.

c. O exportador e o destinatário assinem cláusulas contratuais ou qualquer outro instrumento jurídico que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento do s dados pessoais, as obrigações e responsabilidades assumidas pelas partes e pelo direitos dos titulares. A autoridade supervisora poderá validar cláusulas contratuais ou instrumentos legais conforme determinado em legislação nacional do Estados aplicáveis.

d. El exportador y destinatario adopten un esquema de códigos corporativos vinculantes o un mecanismo de certificación aprobado, siempre y cuando éste sea acorde con las disposiciones previstas en la legislación nacional del Estado miembro aplicable en la materia, que está obligado a observar el exportador.

d. O exportador e o destinatário adotem um esquema de Códigos Corporativos Vinculantes ou mecanismos de certificação aprovados, desde que consistentes com as disposições previstas em legislação nacional do Estado-Membro aplicável, que o exportador é obrigado a observar.

e. La autoridad de control del Estado miembro del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.

e. A autoridade supervisora do Estado - Membro do país do exportador autorize a transferência, nos termos de legislação nacional aplicável.

25.2. La legislación nacional de los Estados miembros aplicable en la materia podrá establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

25.2. A legislação nacional dos Estados-Membros aplicável será capaz estabelecer expressamente os limites para transferências internacionais de categorias de dados pessoais por razões de segurança nacional, segurança pública, proteção da saúde pública, proteção de direitos e liberdades de terceiros, bem como para assuntos de interesse público.

CAPÍTULO VI - AUTORIDADES DE CONTROL

Artículo 26. Naturaleza de las autoridades de control y supervisión

26.1. En cada Estado miembro deberá existir una o más autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad con su legislación nacional aplicable en la materia.

26.2. Las autoridades de control podrán ser órganos unipersonales o pluripersonales; actuarán con carácter imparcial e independiente en sus potestades, así como serán ajenas a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán orden ni instrucción alguna.

26.3. El miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Sus funcionarios se nombran mediante un procedimiento transparente en virtud de la legislación nacional aplicable y únicamente podrán ser removidos por causales graves establecidas en el derecho interno de cada Estado

CAPÍTULO VI - DAS AUTORIDADES DE CONTROLE

Artigo 26. Natureza das autoridades de controle e supervisão

26.1. Em cada Estado- Membro deve existir uma ou mais autoridades de controle em questão de proteção de dados pessoais com total autonomia, de acordo sua legislação nacional aplicável.

26.2. As autoridades de controle poderão ser órgãos individuais ou multipessoais; agirão de forma imparcial e independente em seus poderes, assim como serão alheios a toda influência externa, seja direta ou indireta, e não solicitarão ou admitirão ordem ou instrução alguma.

26.3. O membro ou membros de órgãos de gestão das autoridades de controle devem ter experiência e competências, em particular no que diz respeito ao domínio da protecção de dados pessoais, necessários para o cumprimento dos seus deveres e exercício dos seus poderes. Seus funcionários serão nomeados por um procedimento transparente em virtude de legislação nacional aplicável e apenas poderão ser removidos por motivos graves comprovados no direito interno

miembro, conforme a las reglas del debido proceso.

de cada Estado -Membro, de acordo com o regras do devido processo.

26.4. La legislación nacional de los Estados miembros que resulte aplicable en la materia deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, auditoría, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

26.4. A legislação nacional dos Estados-Membros aplicável deverá conceder às autoridades de supervisão poderes suficientes de investigação, supervisão, auditoria, resolução, promoção, sanção e outros que possam ser necessários para garantir seu efetivo cumprimento, bem como o exercício e respeito do direito de proteção de dados pessoais.

26.5. Las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional de los Estados miembros que resulte aplicable en la materia y su derecho interno.

26.5. As decisões das autoridades de supervisão apenas estarão sujeitas a controle jurisdicional, de acordo com os mecanismos estabelecidos na legislação nacional dos Estados-Membros aplicável em seu direito interno.

26.6. Las autoridades de control deberán contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

26.6. As autoridades de controle deverão contar com recursos humanos e materiais necessário para o cumprimento de suas funções.

Artículo 27 - Régimen de reclamaciones y de imposición de sanciones

Artigo 27. - Regime de reclamações e aplicação de sanções

27.1. Todo titular tendrá derecho a presentar su reclamación ante la autoridad de control, así como recurrir a la tutela judicial para hacer efectivos sus

27.1. Cada titular terá direito de apresentar o sua reclamação perante a autoridade de controle, bem como recorrer à proteção judicial para efetivar

derechos conforme a la legislación nacional del Estado miembro que resulte aplicable en la materia, incluyendo la solicitud de cese de la conducta violatoria del Convenio, medidas cautelares para detener el daño y la indemnización de los perjuicios de cualquier índole ocasionados por el tratamiento ilegal de datos personales.

seus direitos ao abrigo da legislação nacional do Estado-Membro aplicável, incluindo o pedido de cessação de conduta violadora da Convenção, medidas cautelares para impedir danos e compensação dosprejuízos de qualquer natureza causados pela tratamento ilegal de dados pessoais.

27.2. La legislación nacional de los Estados miembros aplicable en la materia establecerá un régimen que permita al titular presentar una reclamación ante la autoridad de control cuando considere que el tratamiento de sus datos personales infringe la normativa nacional en la materia, así como a solicitar la tutela judicial.

27.2. A legislação nacional dos Estados-Membros aplicável estabelecerá um regime que permita ao titular apresentar uma reclamação perante a autoridade de supervisão quando considerar que o tratamento de seus dados pessoais infrinja normas nacionais sobre a matéria, bem como solicitar tutelas judiciais.

27.3. La legislación nacional de los Estados miembros aplicable en la materia establecerá un régimen que permita la adopción de medidas correctivas y sancionar las conductas que contravengan lo dispuesto en las legislaciones nacionales correspondientes, indicando, al menos, el límite máximo y los criterios objetivos para fijar las correspondientes sanciones, a partir de la naturaleza, gravedad, duración de la infracción y sus consecuencias, así como las medidas implementadas por el responsable para garantizar el cumplimiento de sus obligaciones en la materia.

27.3. A legislação nacional dos Estados-Membros aplicável estabelecerá um regime que permita a adoção de medidas corretivas e sanções a comportamentos que contrariem o disposto nas legislações nacional correspondentes, indicando, pelo menos, o limite máximo e critérios objetivos para definir as sanções correspondentes, desde o natureza , gravidade , duração da infração e suas consequências, bem como as medidas implementadas pelo controlador para garantir o cumprimento de suas obrigações.

CAPÍTULO VII - MECANISMOS INTERAMERICANOS DE PROTECCIÓN

Artículo 28 - Comisión Interamericana de Proteccion de Datos personales

28.1. La Comisión Interamericana de Protección de Datos personales funcionará como un órgano autónomo de la Organización de los Estados Americanos (OEA) y estará encargada de la promoción y protección de los derechos reconocidos en este Convenio dentro del continente americano. Está integrada por las autoridades de protección de datos de los países miembros del Convenio las que actuarán ad honorem.

28.2. Sus funciones son:

a. elaborar un informe anual del estado de la protección de datos en la región;

b. preparar documentos y guías sobre la aplicación e interpretación del convenio;

c. colaborar con los Estados miembros en la implementación del tratado en sus leyes locales, sin perjuicio de las normas que resulten directamente aplicables.

CAPÍTULO VII - MECANISMOS DE PROTEÇÃO INTERAMERICANA

Artigo 28. Comissão Interamericana de Proteção de Dados pessoal

28.1. A Comissão Interamericana de Proteção de Dados pessoais funcionará como um órgão autônomo do Organização dos Estados Americanos (OEA) e será responsável pela promoção e proteção de direitos reconhecido nesta Convenção no continente americano. Será composta pelas autoridades de proteção de dados dos países membros da Convenção, que atuarão *ad honorem*.

28.2. Suas funções serão:

a. preparar um relatório anual sobre o estado da proteção de dados na região;

b. preparar documentos e guias sobre a aplicação e interpretação da Convenção;

c. colaborar com os Estados-Membros na implementação deste tratado em suas leis locais, sem prejuízo das regras que resultem diretamente aplicáveis.

Artículo 29 - Informes

29.1. Con el finalidade de proteger el derecho de las personas a la tutela de sus datos personales, en los informes nacionales a la Comisión Interamericana de Proteccion de Datos Personales, los Estados partes deberán incluir información sobre las medidas adoptadas para prevenir y hace respetar los derechos reconocidos en este Convenio, así como sobre las dificultades que observen en la aplicación de las mismas y los factores que contribuyen a la adecuada tutela de los datos personales.

Artigo 29. - Relatórios

29.1. Com o finalidade de proteger o direito das pessoas à proteção dos seus dados pessoais, nos relatórios nacionais à Comissão Interamericana de Proteção de Dados Pessoais, os Estados-Partes deverão incluir informações sobre as medidas tomadas para prevenir e efetivar direitos reconhecidos nesta Convenção, bem como sobre as dificuldades que eles observarem na aplicação dos mesmos e os fatores que contribuam para o proteção adequada de dados pessoais.

Artículo 30 - Opinión consultiva ante la Corte

30.1. Los Estados partes en esta Convención y las respectivas agencias de protección de datos personales podrán requerir a la Corte Interamericana de Derechos Humanos opinión consultiva sobre la interpretación de esta Convención.

Artigo 30. Parecer consultivo perante a Corte

30.1. Os Estados-Partes nesta Convenção e as respectivas agências de proteção de dados pessoais poderão requerer à Corte Interamericana de Direitos Humanos um parecer consultivo sobre a interpretação desta Convenção.

Artículo 31 - Recurso ante la Corte

31.1. Cualquier persona o grupo de personas, o entidad no gubernamental legalmente reconocida en uno o más Estados miembros de la Organización, puede presentar a la Comisión

Artigo 31. - Recurso para o Tribunal

31.1. Qualquer pessoa ou grupo de pessoas, ou entidade não governamental legalmente reconhecida em um ou mais Estados-Membros da Organização, poderá apresentar

Interamericana de Derechos Humanos peticiones que contengan denuncias o quejas de violación de los derechos previstos en la presente Convención por un Estado parte, y la Comisión las considerará de acuerdo con las normas y los requisitos de procedimiento para la presentación y consideración de peticiones estipulados en la Convención Americana sobre Derechos Humanos y en el Estatuto y el Reglamento de la Comisión Interamericana de Derechos Humanos.

petições à Comissão Interamericana de Direitos Humanos que contenham denúncias ou queixas de violação do direitos previstos nesta Convenção por um Estado-Parte. A Comissão as considerará de acordo com as regras e requisitos procedimentais para o apresentação e consideração de petições estipuladas em o Convenção Americana sobre Direitos Humanos e no Estatuto e o Regulamento da Comissão Interamericana de Direitos Humanos.

CAPÍTULO VIII - DISPOSICIONES GENERALES DEL CONVENIO

CAPÍTULO VIII - DISPOSIÇÕES GERAIS DA CONVENÇÃO

Artículo 32

Artigo 32.

32.1. Nada de lo dispuesto en la presente Convención podrá ser interpretado como restricción o limitación a la legislación interna de los Estados partes que prevea iguales o mayores protecciones y garantías de los derechos del titular de los datos personales.

32.1. Nada do disposto na presente Convenção poderá ser interpretado como uma restrição ou limitação à legislação interna dos Estados-Partes que preveja iguais ou maiores proteções e garantias de direitos aos titulares de dados pessoais.

Artículo 33

Artigo 33.

33.1. Nada de lo dispuesto en la presente Convención podrá ser interpretado como restricción o limitación a la Convención Americana sobre Derechos Humanos o a otras

33.1. Nada do disposto em a presente Convenção pode ser interpretado como uma restrição ou limitação ao Convenção Americana sobre Direitos Humanos ou outras convenções

convenciones internacionales sobre la materia que prevean iguales o mayores protecciones relacionadas con este tema.

internacionais sobre matéria que proporcione igual ou maior proteções relacionadas a este tópico.

Artículo 34	**Artigo 34.**
34.1. La presente Convención está abierta a la firma de todos los Estados miembros de la Organización de los Estados Americanos.	**34.1.** Esta Convenção está aberta à assinatura de todos os Estados Membros da Organização dos Estados Americanos.
Artículo 35	**Artigo 35.**
35.1. La presente Convención está sujeta a ratificación. Los instrumentos de ratificación se depositarán en la Secretaría General de la Organización de los Estados Americanos.	**35.1.** Esta Convenção está sujeita a ratificação. Os instrumentos de ratificação serão depositados na Secretaria Geral da Organização dos Estados Americanos.
Artículo 36	**Artigo 36.**
36.1. La presente Convención queda abierta a la adhesión de cualquier otro Estado. Los instrumentos de adhesión se depositarán en la Secretaría General de la Organización de los Estados Americanos.	**36.1.** Esta Convenção está aberta a adesão de qualquer um outro estado. Os instrumentos de adesão serão depositados na Secretaria Geral da Organização dos Estados Americanos.
Artículo 37	**Artigo 37.**
37.1. Los Estados no podrán formular reservas a la presente Convención al momento de aprobarla, firmarla, ratificarla o adherir a ella.	**37.1.** Os Estados não poderão formular reservas a esta Convenção no momento da sua aprovação, assinatura, ratificação ou adesão a ela.

Artículo 38

38.1. Cualquier Estado parte puede someter a la Asamblea General una propuesta de enmienda a esta Convención. Las enmiendas entrarán en vigor para los Estados ratificantes de las mismas en la fecha en que dos tercios de los Estados partes hayan depositado el respectivo instrumento de ratificación. En cuanto al resto de los Estados partes, entrarán en vigor en la fecha en que depositen sus respectivos instrumentos de ratificación.

Artigo 38.

38.1. Qualquer Estado Parte poderá submeter à Assembleia Geral uma proposta para alterar esta Convenção. As alterações entrarão em vigor para os Estados que as ratificarem na data em que dois terços dos Estados Partes tenham depositado o respectivo instrumento de ratificação. Quanto aos demais Estados Partes, entrarão em vigor na data em que depositarem os respectivos instrumentos de ratificação.

Artículo 39

39.1. Los Estados partes que tengan dos o más unidades territoriales en las que rijan distintos sistemas jurídicos relacionados con cuestiones tratadas en la presente Convención podrán declarar, en el momento de la firma, ratificación o adhesión, que la Convención se aplicará a todas sus unidades territoriales o solamente a una o más de ellas. Tales declaraciones podrán ser modificadas en cualquier momento mediante declaraciones ulteriores, que especificarán expresamente la o las unidades territoriales a las que se aplicará la presente Convención. Dichas declaraciones ulteriores se transmitirán a la Secretaría General de la Organización de los Estados Americanos

Artigo 39.

39.1. Estados Partes que possuem duas ou mais unidades territorial em aqueles que regem diferentes sistemas jurídicos relacionados a assuntos discutidos em a presente Convenção poderá declarar, em o momento da assinatura , ratificação ou adesão , que A Convenção aplicar-se-á a todas as suas unidades territoriais ou apenas a uma ou mais delas . Tais declarações pode ser modificado em a qualquer momento por meio de declarações posteriores , que especificarão expressamente a unidade ou unidades territoriais às quais esta Convenção se aplicará . provérbios As declarações subsequentes serão transmitidas ao Secretaria Geral da Organização dos Estados Americanos e

y surtirán efecto treinta días después de recibidas.

fornecerá efeito trinta dias depois de recebido .

Artículo 40

40.1. La presente Convención entrará en vigor el trigésimo día a partir de la fecha en que se haya depositado el segundo instrumento de ratificación. Para cada Estado que ratifique o adhiera a la Convención después de haber sido depositado el segundo instrumento de ratificación, entrará en vigor el trigésimo día a partir de la fecha en que tal Estado haya depositado su instrumento de ratificación o adhesión.

Artigo 40.

40.1. A presente Convenção entrará em vigor no trigésimo dia após a data em que o segundo instrumento de ratificação tiver sido depositado. Para cada Estado que ratifique ou adira à Convenção após o depósito do segundo instrumento de ratificação, esta entrará em vigor no trigésimo dia a contar da data em que esse Estado tiver depositado o seu instrumento de ratificação ou de adesão.

Artículo 41

41.1. El Secretario General informará a todos los Estados miembros de la Organización de los Estados Americanos de la entrada en vigor de la Convención.

Artigo 41.

41.1. O Secretário-Geral informará a todos os Estados Membros da Organização dos Estados Americanos a entrada em vigor desta Convenção.

Artículo 42

42.1. El Secretario General de la Organización de los Estados Americanos presentará un informe anual a los Estados miembros de la Organización sobre el estado de esta Convención, inclusive sobre las firmas, depósitos de instrumentos de ratificación, adhesión o declaraciones, así como las reservas que hubieren presentado los Estados partes

Artigo 42.

42.1. O secretário-geral da Organização dos Estados Americanos apresentará um relatório anual aos Estados-Membros da Organização sobre o status desta Convenção, incluindo assinaturas, depósitos de instrumentos de ratificação, adesão ou declarações, bem como as reservas apresentadas pelos Estados-Partes e, nestes caso, o relatório sobre as mesmas.

y, en su caso, el informe sobre las mismas.

Artículo 43	**Artigo 43.**
43.1. La presente Convención regirá indefinidamente, pero cualquiera de los Estados partes podrá denunciar esta Convención mediante el depósito de un instrumento con ese fin en la Secretaría General de la Organización de los Estados Americanos. Un año después a partir de la fecha del depósito del instrumento de denuncia, la Convención cesará en sus efectos para el Estado denunciante, quedando subsistente para los demás Estados partes.	**43.1.** Esta convenção vigorará indefinidamente, mas qualquer dos Estados-Partes poderá denunciar esta Convenção mediante o depósito de um instrumento esse fim na Secretaria Geral da Organização dos Estados Americanos. Um ano após a data do depósito do instrumento de denúncia, a Convenção cessará em seus efeitos para o Estado denunciante, permanecendo subsistente para o outros Estados-Partes.
Artículo 44	**Artigo 44.**
44.1. El instrumento original de la presente Convención, cuyos textos en español, francés, inglés y portugués son igualmente auténticos, será depositado en la Secretaría General de la Organización de los Estados Americanos, la que enviará copia certificada de su texto para su registro y publicación a la Secretaría de las Naciones Unidas, de conformidad con el artículo 102 de la Carta de las Naciones Unidas.	**44.1.** O instrumento original da presente Convenção , cujos textos em espanhol, francês, inglês e português são igualmente autênticos, será depositado na Secretaria Geral da Organização dos Estados Americanos, que enviará cópia autenticada de seu texto para registro e publicação pela Secretaria das Nações Unidas, de acordo com Artigo 102 da Carta das Nações Unidas.
EN FE DE LO CUAL, los plenipotenciarios infrascritos, debidamente autorizados por sus respectivos gobiernos, firman el presente Convenio, que se llamará	EM TESTEMUNHO DO QUE, os plenipotenciários abaixo assinados, devidamente autorizados pelos seus respectivos governos, assinam este

“Convención Interamericana para la protección de los datos personales y la libre circulación de esos datos”.

presente Acordo, que se chamará “Convenção Interamericana para a proteção do dados pessoais e para a livre circulação destes dados".