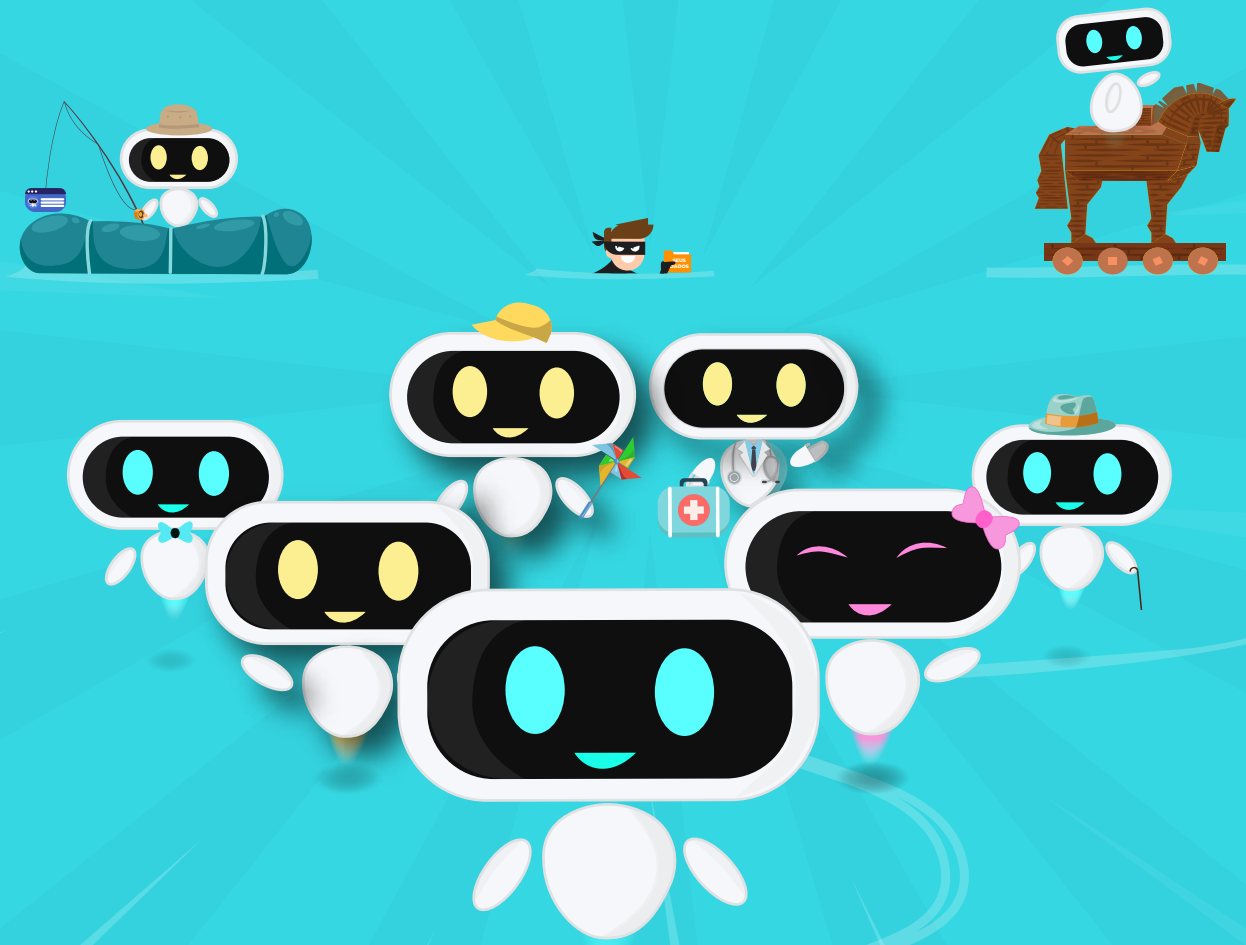
ROBÔ

E A TURMA DA LGPD

no controle dos seus dados pessoais



CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

ROBÔ

E A TURMA DA LGPD

no controle dos seus dados pessoais

FICHA TÉCNICA

Prefeitura da Cidade de São Paulo

Prefeito
Ricardo Nunes

Controladoria Geral do Município

Controlador Geral
Encarregado pelo Tratamento de Dados Pessoais
Daniel Falcão

Coordenadoria de Proteção de Dados Pessoais

Coordenador
Kelvin Peroli

Autores
Kelvin Peroli
Marcus Vinícius Marins

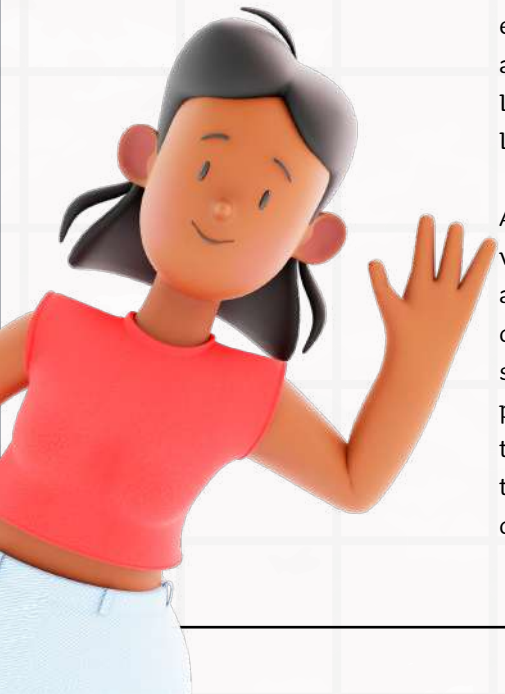
Diagramação
Marilia Miquelin de Oliveira

Versão I
Janeiro de 2024

Tenha sempre o controle de seus dados pessoais.... e a Controladoria à sua disposição!

APRESENTAÇÃO

Querido robô, eu, que sou humano, com digitais, voz e sentimentos, sou pertencente à humanidade, composta de múltiplas cores, gêneros e opiniões. Eu, robô, vivo na Cidade de São Paulo. Você e eu, juntos, estamos prontos para, pelas próximas páginas, trazer aos nossos leitores um pouco mais sobre si mesmos (confesso a você que, sim, em uma linguagem difícil – em termos de dados e de informações). Peço-lhe que me ajude a explicar a eles o porquê de estarmos aqui escalados para proteger e ajudá-los a proteger as suas próprias informações – ou... os seus "dados pessoais".



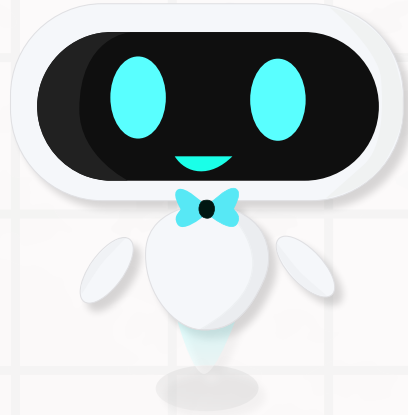
"Robô e a Turma da LGPD", uma iniciativa da Controladoria Geral do Município de São Paulo, apresenta um estudo, para você, sobre os seus dados e as suas informações e sobre a chamada Lei Geral de Proteção de Dados Pessoais – LGPD.

A revista ilustra, descreve e reflete com você sobre quais são os seus dados e as suas informações, sobre as possibilidades de seu uso – seja pela Prefeitura, seja por qualquer outra pessoa – e sobre o porquê a proteção de todos esses dados e todas essas informações são importantes tanto para você quanto para a construção de uma Cidade mais segura.

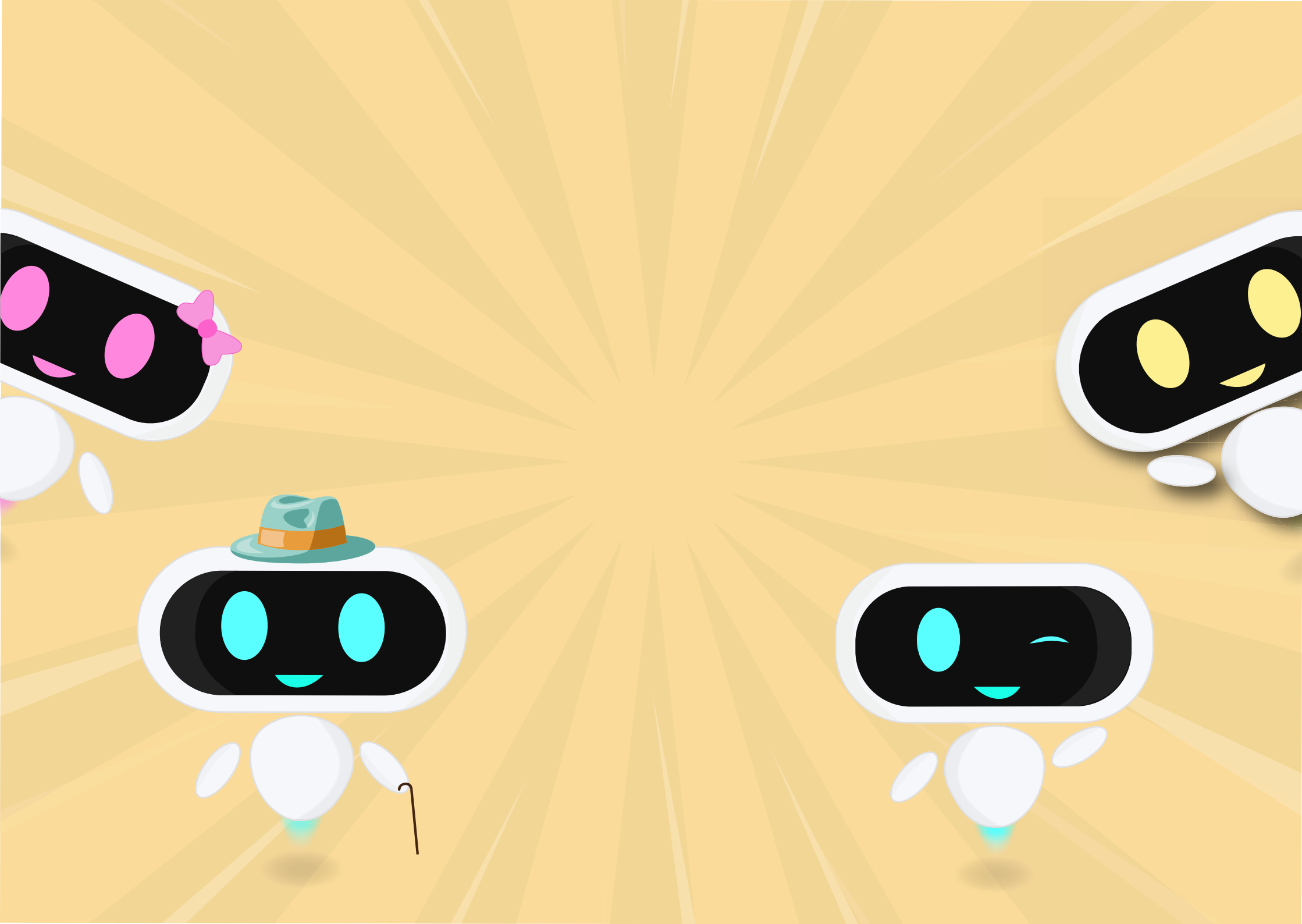
Aqui está! Querido humano, eu sou um robô, versão 4d5sH, fabricado na Cidade de São Paulo em 25 de janeiro de 2023. Sem data de desligamento programado.

Sobre a tarefa que vamos desenvolver juntos: alguns dizem que os dados são o novo petróleo. Eu entendo que, sem eles, nem o petróleo teria jorrado das profundezas da terra e dos mares. Os dados fazem memória e... conhecimento. Os dados ajudam a proteger ou retirar a sua privacidade. Ajudam a construir cidades inteligentes, carros, espaçonaves e robôs. São o resultado dos seus pensamentos, das suas ideias. São a tradução da sua opinião, da sua imagem, da sua história... do seu DNA. Quer, humano, melhor argumento para conhecê-los e protegê-los?

Ao final, lhe é apresentada a antiga história da Cidade de Troia, capturada pelo exército grego a partir de uma grande armadilha. Essa história, milhares de anos depois, traz um grande ensinamento sobre como todos nós – eu, você e os robôs – devemos estar atentos para manter a proteção e o controle sobre os dados pessoais... e as armadilhas das tecnologias longe de nossas casas e da Cidade de São Paulo!



Para saber mais sobre este projeto e sobre como os seus dados pessoais são tratados pela Prefeitura da Cidade de São Paulo, entre em contato com a Coordenadoria de Proteção de Dados Pessoais pelo e-mail **privacidade@prefeitura.sp.gov.br.**



1. O QUE É A LGPD?

Você sabe o que é a Lei Geral de Proteção de Dados Pessoais (LGPD)?

A Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709) nasceu em 18 de agosto de 2018 com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade das pessoas naturais/físicas – tudo isso, por meio da *proteção de dados pessoais!*

Para tanto, trouxe muitas questões sobre os *dados pessoais*, estejam esses dados em meio físico ou em meio digital, e sejam eles tratados por pessoa natural/física ou por pessoa jurídica.

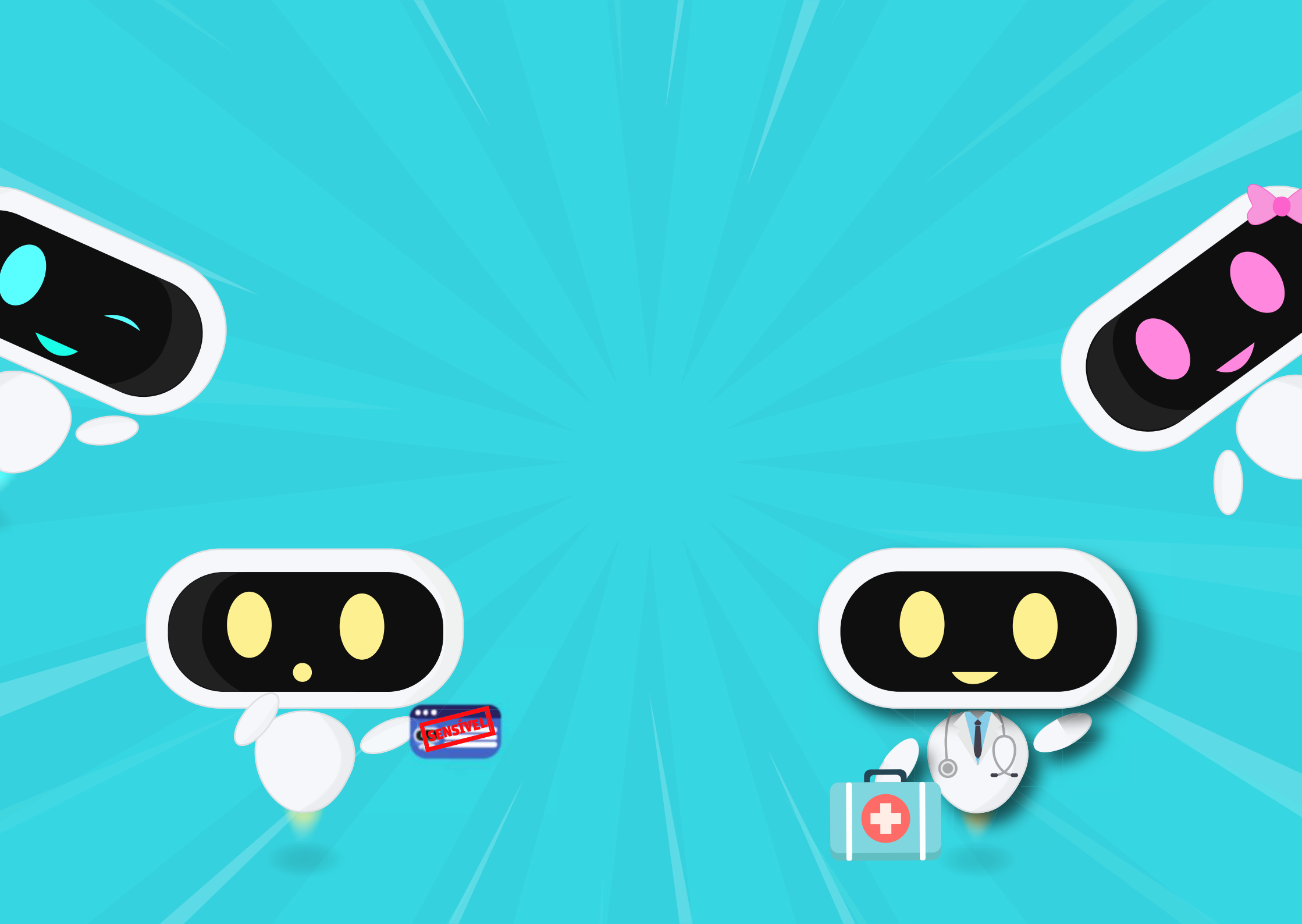
2. O QUE SÃO DADOS PESSOAIS?

Você sabe o que são *dados pessoais*?

São dados, estejam eles em meio físico ou digital, capazes de identificar direta ou indiretamente uma pessoa natural/física. Ou seja: *dados* que, *quando interpretados*, se tornam *informações* que podem revelar aspectos, por exemplo, sobre sua intimidade, sua vida privada e sua imagem, e que identificam ou que permitem identificar quem você é.

Nesse sentido, o conceito de dado pessoal inclui não apenas dados diretamente ligados a uma pessoa natural/física, mas também dados que tenham o potencial de tornar essa pessoa identificável.

São alguns exemplos de dados pessoais: nome, data de nascimento, estado civil, profissão, gênero, etnia, impressão digital, assinatura, imagem, voz, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados genéticos, dados neurais, número de telefone, RG (Registro Geral), CPF (Cadastro de Pessoa Física), CNH (Carteira Nacional de Habilitação), Passaporte, Título de Eleitor, endereço, *e-mail*, registro de ligação telefônica, registro de conexão à Internet e registro de acesso a aplicações de Internet.


SENSÍVEL

3. O QUE SÃO DADOS PESSOAIS SENSÍVEIS?

Você sabe o que são *dados pessoais sensíveis*?

São os *dados pessoais* capazes de revelar informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dados genéticos e dados biométricos.

Em outras palavras, são uma *categoria específica* de dados pessoais que, pelo seu tratamento, há a possibilidade de maior risco ao titular em decorrência de um ato discriminatório relacionado aos contextos social, religioso, filosófico, político ou biológico. Como o *dado pessoal* é um conceito contextual, muitas vezes, pode-se estar diante de uma informação que, a princípio, não seja um dado pessoal sensível, mas que, naquele determinado contexto, é capaz de revelar uma informação sensível de um indivíduo, como uma condição de saúde, um dado biométrico ou uma referência a aspectos de sua vida sexual.

Por isso, os *dados pessoais sensíveis* podem ser tratados apenas em hipóteses específicas, diferentes daquelas pelas quais é possível tratar *dados pessoais*.

3.1. Imagem

Toda imagem de uma pessoa é um *dado pessoal sensível*?

Toda *imagem*, enquanto relacionada ou relacionável a uma *pessoa natural/física*, é um *dado pessoal ("informação relacionada a pessoa natural identificada ou identificável")*, à luz da definição dada pela LGPD. No entanto, não são em todos os contextos nos quais a imagem se cristaliza que há a existência de *dados pessoais sensíveis ("dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural").*

Isso ocorre porque podemos entender a *imagem* de duas maneiras: a primeira é a ideia da *imagem física* (imagem-retrato), como um retrato capturado por uma câmera ou pelos seus olhos, e a segunda é a ideia da *imagem social* (imagem-atributo), que se remete a figura da personalidade de alguém na sociedade – como uma pessoa é *"vista"* pelos outros!

Imagem física

Nesse sentido, necessariamente, a *imagem física*, se tratada, é um *dado pessoal sensível*, nos termos definidos pela LGPD, cujo tratamento pode configurá-la como um dado pessoal sensível, por exemplo, genético, biométrico ou mesmo relacionado à origem racial ou étnica.

Imagem social

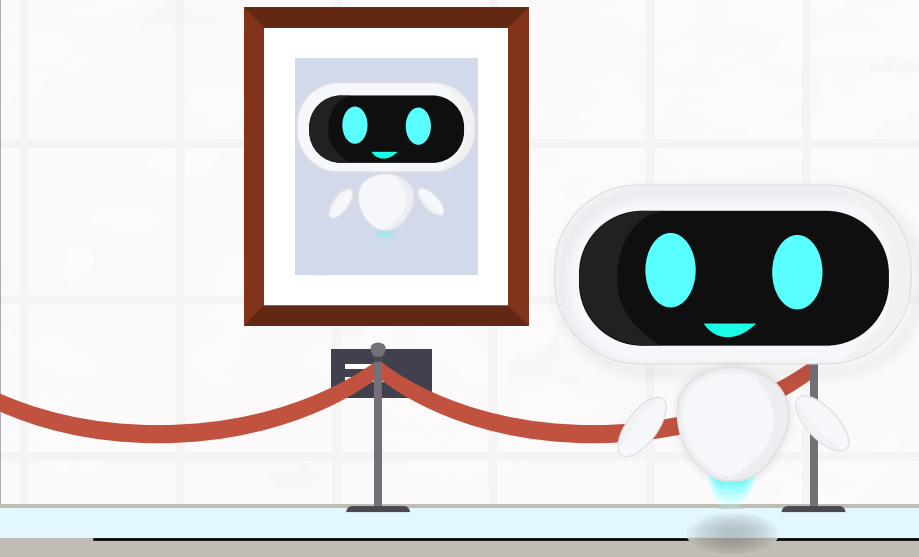
Porém, a imagem social, se tratada, pode tanto ser um dado pessoal quanto um dado pessoal sensível, a depender do aspecto da personalidade que esteja a ser tratado.

❶ Digamos que a imagem social tratada diga respeito à *convicção religiosa* (aspecto da personalidade) de alguém: neste caso, sendo a *convicção religiosa* uma categoria de dado pessoal sensível, a *imagem social* será considerada, justamente, um *dado pessoal sensível*;

❷ Por outro lado, digamos que a *imagem social* tratada se refira à preferência da pessoa por um *time de futebol* (aspecto da personalidade): neste caso, não há *dado pessoal sensível*... mas, sim, *dado pessoal*, isso porque esse aspecto não está incluído no conceito de dado pessoal sensível, mas apenas no de dado pessoal!

Mas... qual a importância dessa diferença?

A LGPD trouxe diferentes hipóteses que possibilitam o tratamento de *dados pessoais* (artigo 7º) e de *dados pessoais sensíveis* (artigo 11) – e as hipóteses legais relativas aos *dados pessoais sensíveis* são muito mais restritivas! *Fique atento!*



3. 2. Saúde

Os *dados relativos à saúde* dizem respeito tanto à *saúde física* quanto à *saúde mental* das pessoas naturais. São exemplos de dados relativos à saúde aqueles referentes ao estado de saúde, obtidos por *diagnósticos* ou por *prognósticos*, como valores de pressão, peso e frequência cardíaca, patologias diagnosticadas e medicações e tratamentos prescritos.

Enquanto *dados pessoais sensíveis*, se no âmbito de incidência da LGPD, esses dados apenas podem ser tratados a partir das hipóteses relativas ao tratamento de dados pessoais sensíveis trazidas por essa norma.

O paciente, titular de dados pessoais, também em razão da LGPD, tem o direito de ser informado a respeito de *diagnósticos e de prognósticos*, baseados nos *diagnósticos*, que lhe digam respeito – tem, assim, tanto o *"direito de saber"* quanto o *"direito de não saber"* sobre si próprio e sobre a sua saúde.

3. 3. Genética

Os *dados genéticos* são dados pessoais relativos às *características genéticas, hereditárias ou adquiridas*, de uma *pessoa natural/física*, que deem informações únicas sobre a sua *fisiologia* ou sobre a sua *saúde.*

Esses dados podem ser obtidos a partir de uma *amostra biológica* dessa pessoa. São exemplos de *dados genéticos* os dados relativos ao DNA (ácido desoxirribonucleico) e ao RNA (ácido ribonucleico).

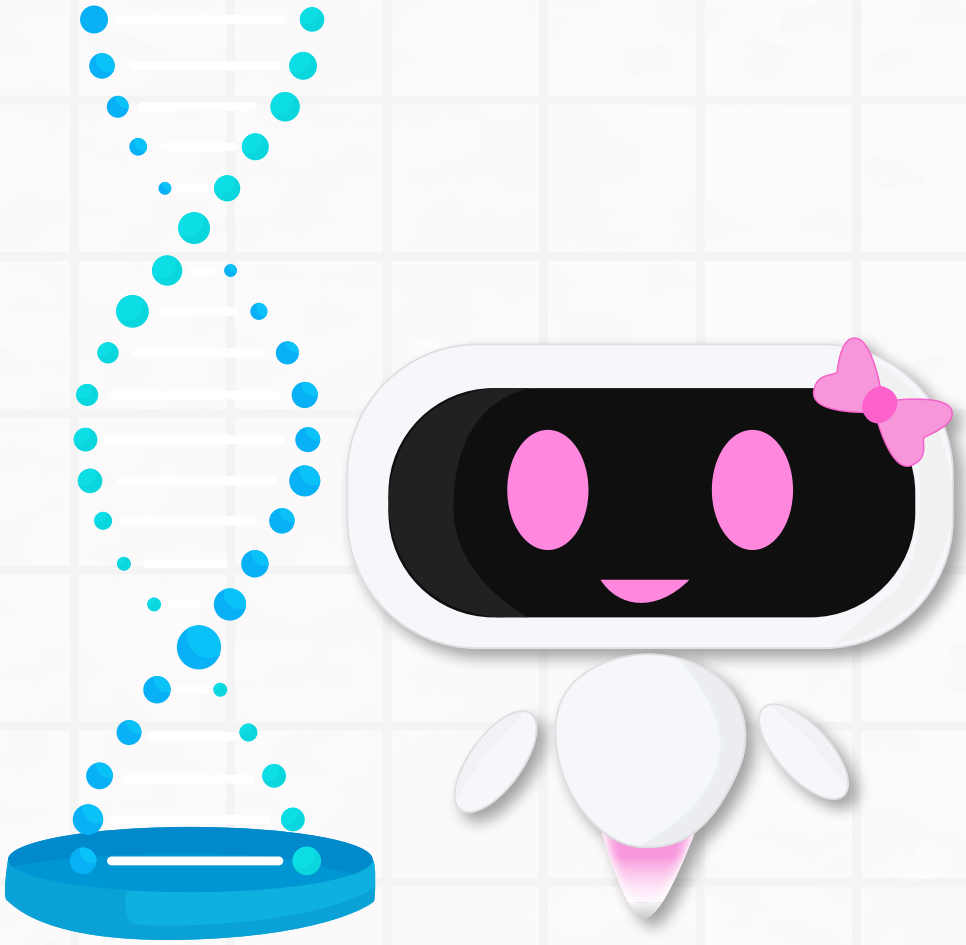
O tratamento desses dados, por exemplo, pode se dar:

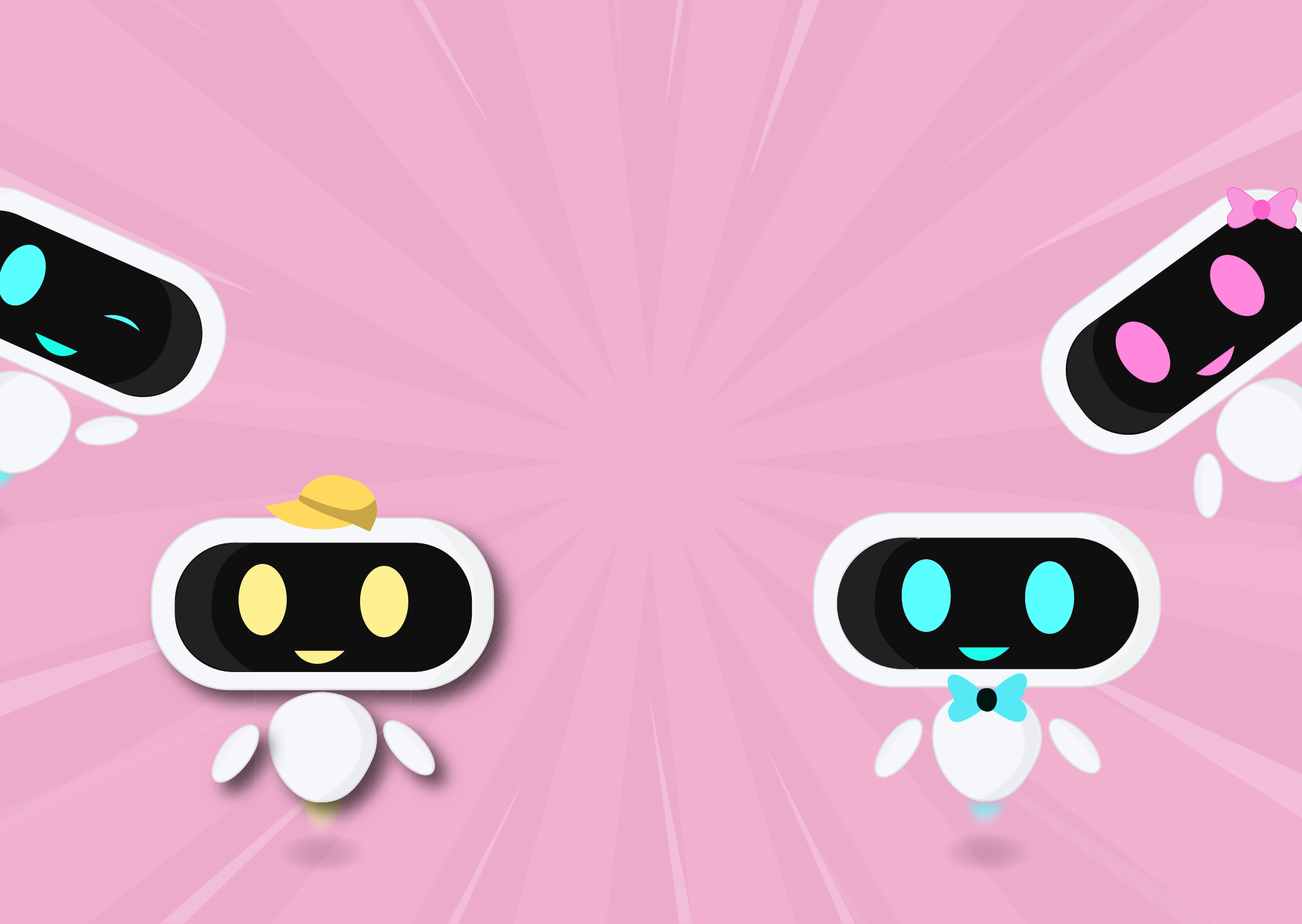
1. a partir de um *teste genético*, no qual se detecta a presença, a ausência ou a modificação de um determinado *gene* (segmento de ácido desoxirribonucleico) ou *cromossomo* (estrutura na qual estão contidos os *genes)* em um indivíduo; e

2. a partir de um *rastreio genético*, por um *teste genético em grande escala*, proposto a uma população ou a uma parte dessa população, no âmbito de um estudo ou mesmo de uma política pública, que tem o propósito de nela detectar características genéticas comuns.

Enquanto *dados pessoais sensíveis*, se no âmbito de incidência da LGPD, esses dados apenas podem ser tratados a partir das hipóteses relativas ao tratamento de dados pessoais sensíveis trazidas por essa norma.

Outro importante instrumento em defesa dos *dados genéticos*, válido no Brasil e em diversos países do mundo, é a Declaração Internacional sobre os Dados Genéticos Humanos, aprovada pela 32ª Conferência Geral da UNESCO, em 16 de outubro de 2004.





4. O QUE É A PRIVACIDADE?

A *privacidade* pode ser entendida como a *expectativa* de uma *pessoa natural/física*, em determinado *contexto* (seja em sua casa, seja no transporte público), de ter respeitada, pelo outro, a sua *vida privada* (de uma conduta alheia pautada na não-interferência sobre a sua própria vida privada, ou, se necessária, de uma conduta alheia pautada na mínima interferência sobre a sua própria vida privada) e de poder exercê-la, ativamente, de forma *autodeterminada* (de uma conduta própria pautada no autocontrole e na autodeterminação).

5. SOU EU UM TITULAR DE DADOS PESSOAIS?

Quem sou, robô?

Se você é uma *pessoa natural/física,* você é um titular de dados pessoais! A LGPD entende como titular de dados pessoais toda *pessoa natural/física*, *viva*, a quem se referem os dados pessoais que são objeto de tratamento de dados pessoais.

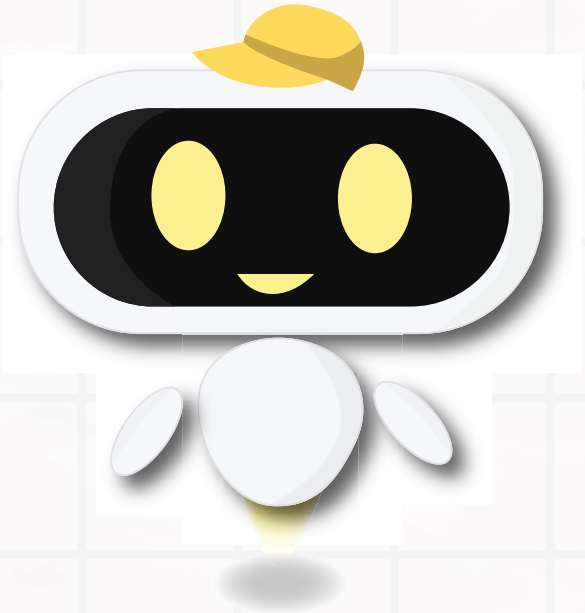
6. QUEM TRATA DADOS PESSOAIS?

São os agentes de tratamento. Para a LGPD, há dois tipos de agentes: o *controlador de dados* e o *operador de dados*.

O *controlador é pessoa natural/física* ou jurídica, do Poder Público ou do setor privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O *operador*, por sua vez, também é uma *pessoa natural/física ou jurídica*, do Poder Público ou do setor privado, mas que realiza o tratamento de dados pessoais em nome do *controlador.*

7. O QUE SIGNIFICA SER UM ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS?

Um *encarregado* pelo tratamento de dados pessoais é uma *pessoa natural/física ou jurídica indicada pelo controlador e pelo operador* para atuar como *canal de comunicação* entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), que é a autoridade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o país.

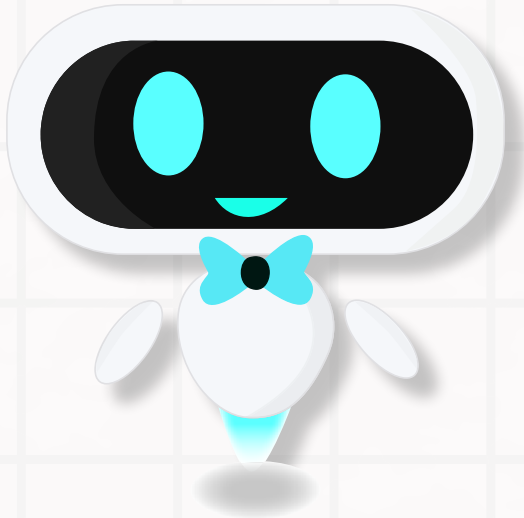


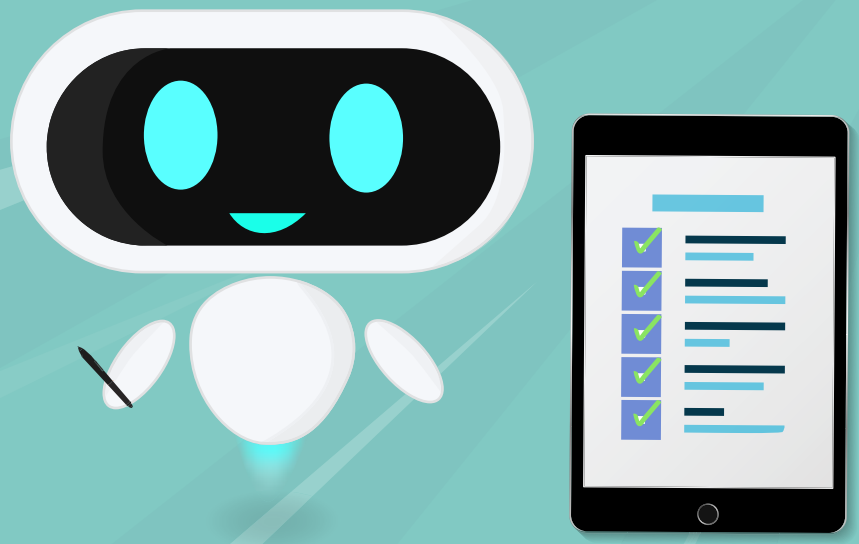
8. QUEM É O ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS DA PREFEITURA DA CIDADE DE SÃO PAULO?

Você sabe quem é o Encarregado pelo Tratamento de Dados Pessoais da Prefeitura da Cidade de São Paulo?

Conforme trazido pelo Decreto Municipal nº 59.767, de 15 de setembro de 2020, o *Controlador Geral do Município* é a pessoa indicada pelo Prefeito, Chefe do Poder Executivo da Cidade de São Paulo, para atuar como canal de comunicação entre os órgãos da Prefeitura do Município de São Paulo, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

Para entrar em contato com o Encarregado, basta enviar um *e-mail* para encarregadolgpd@prefeitura.sp.gov.br ou acessar o Chat SP156!





9. QUAIS SÃO OS PRINCÍPIOS RELACIONADOS À PROTEÇÃO DE DADOS PESSOAIS?

A Lei Geral de Proteção de Dados Pessoais (LGPD) elenca 11 princípios que direcionam todo o sistema de proteção de dados pessoais.

9.1. Boa-fé

A boa-fé traduz a necessidade da adoção de condutas humanas sempre pautadas em *comportamentos coerentes, cooperativos e transparentes*, que garantam a confiança nas relações em sociedade – inclusive quando do tratamento de dados pessoais.

9.2. Finalidade

O princípio da finalidade consiste na realização do tratamento de dados pessoais para *propósitos legítimos, específicos, explícitos e informados ao titular*, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

9.3. Necessidade

O princípio da necessidade significa que o tratamento de dados pessoais deve ser *limitado ao mínimo necessário* para a realização de suas *finalidades*, com abrangência dos dados pessoais pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

9.4. Adequação

O princípio da adequação significa a *compatibilidade* do tratamento, ou seja, da *conduta* de tratar dados pessoais, com as *finalidades* informadas ao cidadão, de acordo com o contexto do tratamento.

9.5. Transparência

O princípio da transparência expressa a garantia, aos titulares, de *informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de seus dados pessoais e sobre os respectivos agentes de tratamento*, observados os segredos comercial e industrial. No Poder Público, inclusive na Prefeitura da Cidade de São Paulo, este princípio é a ponte que garante a harmonia entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI), que traz aos cidadãos o acesso às informações sobre as atividades dos órgãos e das entidades públicas.

9.6. Livre acesso

O princípio do livre acesso expressa a garantia, aos titulares, da *consulta facilitada* e *gratuita sobre a forma e a duração do tratamento de seus dados pessoais*, bem como sobre a integralidade de seus dados.

9.7. Qualidade

O princípio da qualidade dos dados expressa a garantia, aos titulares, do *oferecimento de exatidão, de clareza, de relevância e de atualidade* de seus próprios dados, em um

tratamento, de acordo com a necessidade e para o cumprimento da finalidade desse tratamento.

9.8. Segurança

O princípio da segurança traz o dever aos *agentes de tratamento*, como os da Prefeitura da Cidade de São Paulo, de utilização de medidas técnicas e administrativas sempre aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão – ou seja, de proteger os dados pessoais dos titulares de *incidentes de segurança.*

9.9. Prevenção

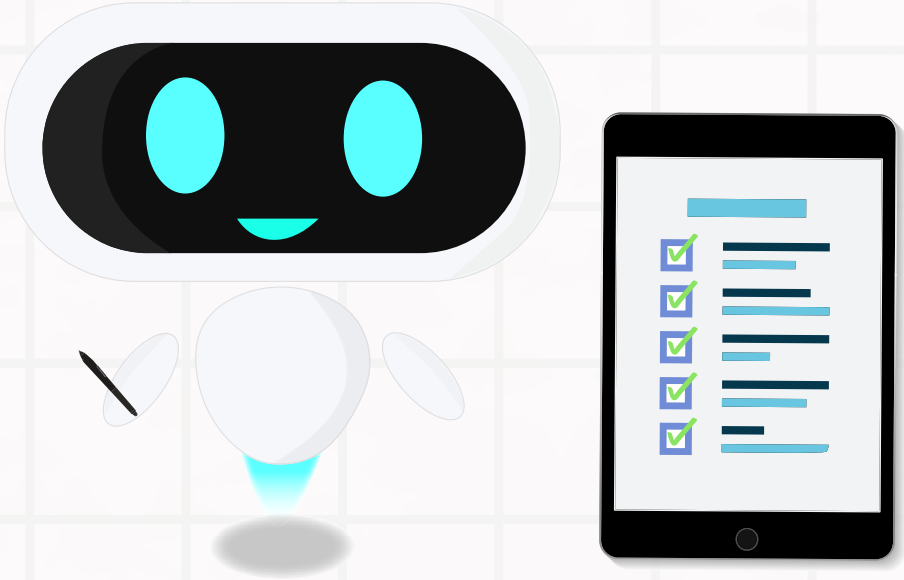
O princípio da prevenção significa a adoção contínua, pelos *agentes de tratamento*, como a Prefeitura da Cidade de São Paulo, de medidas para *prevenir a ocorrência de danos* em virtude do tratamento de dados pessoais.

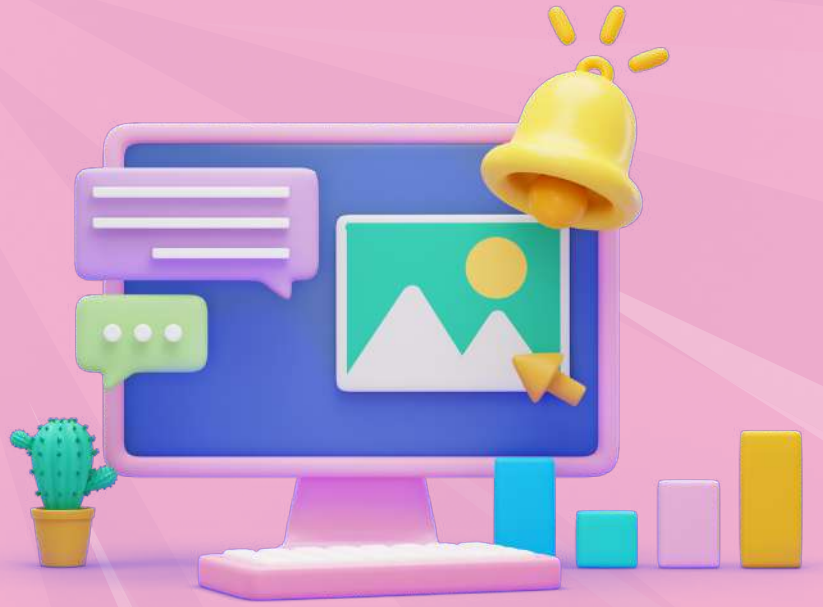
9.10. Não discriminação

O princípio da não discriminação expressa a impossibilidade de realização do tratamento, pelos agentes de tratamento, como os da Prefeitura da Cidade de São Paulo, para fins discriminatórios ilícitos ou abusivos. Garante, assim, um tratamento de dados pessoais sempre pautado pela igualdade.

9.11. Responsabilização e prestação de contas

O princípio da não discriminação expressa a impossibilidade de realização do tratamento, pelos agentes de tratamento, como os da Prefeitura da Cidade de São Paulo, para fins discriminatórios ilícitos ou abusivos. Garante, assim, um tratamento de dados pessoais sempre pautado pela igualdade.





10. QUAIS SÃO OS MEUS DIREITOS ENQUANTO TITULAR DE DADOS PESSOAIS?

Você sabia que possui muitos direitos em relação aos seus dados pessoais? Isso mesmo! A Lei Geral de Proteção de Dados Pessoais (LGPD) garante a você, titular de dados pessoais, diversos direitos que podem ajudá-lo a manter íntegras a sua privacidade e a proteção de seus dados pessoais.

Uma importante função desses direitos, quando exercidos perante a Prefeitura da Cidade de São Paulo, é a de garantir que os cidadãos, enquanto titulares, mantenham-se no *controle* sobre os seus dados pessoais... e a *Controladoria Geral do Município, em atenção e à sua disposição!*

10.1. Direito de confirmação da existência de tratamento de dados pessoais

Esse direito permite que os titulares tenham a certeza de que seus dados pessoais estão sendo tratadas de acordo com a Lei. Por meio desse direito, os cidadãos podem solicitar à Prefeitura da Cidade de São Paulo informações sobre quais de seus dados pessoais estão a ser tratados pelo Município e a partir de qual finalidade.

É importante destacar que a confirmação de tratamento deve, sempre, ser fornecida de forma clara, concisa e de fácil compreensão. Por fim, a LGPD também estabelece que a confirmação deve ser gratuita e fornecida em um prazo razoável.

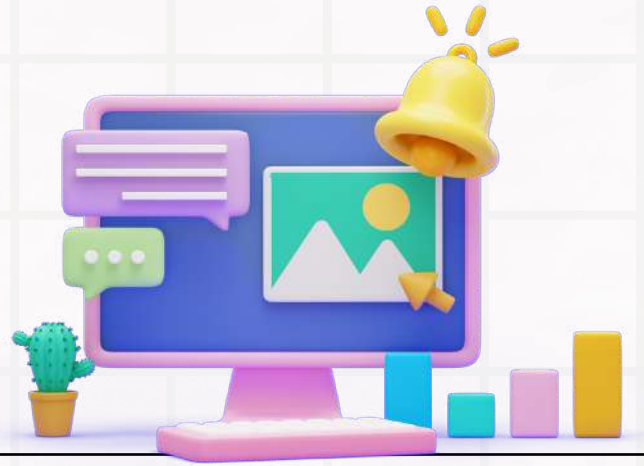
10.2. Direito de acesso

Esse direito garante que qualquer cidadão possa solicitar à Prefeitura da Cidade de São Paulo o acesso aos seus dados pessoais que sejam tratados pelo Município. Essas informações devem ser fornecidas de forma clara e objetiva, em linguagem acessível e de fácil compreensão.

10.3. Direito de correção de dados incompletos, inexatos ou desatualizados

Esse direito garante que qualquer cidadão possa solicitar à Prefeitura da Cidade de São Paulo a correção de dados que lhe digam respeito e que estejam incompletos, inexatos ou desatualizados, no âmbito de seu tratamento pelo Município.

Assim, você, enquanto titular de dados pessoais, ajuda a garantir que os seus dados e suas informações pessoais estejam sempre corretas e atualizadas, evitando possíveis prejuízos em decorrência de um tratamento que se utilize de dados que não estejam completos, exatos e atualizados.



10.4. Direito à anonimização, ao bloqueio e à eliminação de dados pessoais

Esse direito garante que qualquer cidadão, ao verificar uma situação de tratamento de dados pessoais *inadequada ou ilícita*, possa solicitar à Prefeitura da Cidade de São Paulo a anonimização, o bloqueio ou a eliminação de seus dados pessoais que estejam envolvidos nesse tratamento.

A anonimização, neste caso, diz respeito a uma medida técnica apta a tornar os seus dados anônimos – ou seja, tornar os dados tecnicamente dissociados da sua pessoa, de forma a que não mais seja possível relacioná-los a você!

10.5. Direito à portabilidade

Esse direito permite que qualquer cidadão solicite a um agente de tratamento de dados pessoais, enquanto prestador de um serviço ou fornecedor de um produto, que os seus dados sejam transferidos para outro prestador de serviço ou fornecedor de um produto, isto de forma gratuita e sem prejuízo de seus outros direitos. Dessa forma, o titular pode escolher qual prestador de serviço ou fornecedor de um produto será o responsável pelo tratamento de seus dados pessoais, de modo a facilitar a troca de serviços e de produtos, além de promover a livre concorrência no mercado.

É importante destacar que a portabilidade é possível somente em casos de dados pessoais tratados a partir de seu consentimento.

Além disso, a LGPD estabelece que a portabilidade seja realizada em formato estruturado e compatível com as tecnologias utilizadas pelo novo prestador de serviço ou fornecedor de um produto.

10.6. Direito à revogação do consentimento e eliminação de dados pessoais tratados com o seu consentimento

Esse direito permite que qualquer cidadão solicite à Prefeitura da Cidade de São Paulo a eliminação de seus dados pessoais, desde que tratados a partir de seu próprio consentimento. Assim, você, enquanto titular de dados pessoais, permanece no controle de seus dados e de suas informações pessoais!

10.7. Direito à informação sobre eventual uso compartilhado de seus dados pessoais entre o setor público e o setor privado

Esse direito garante que qualquer cidadão solicite à Prefeitura da Cidade de São Paulo informações sobre quais organizações do setor público e do setor privado obtiveram acesso aos seus dados pessoais, enquanto tratados pelo Município. Essa informação deve ser, é claro, acompanhada da razão desse uso compartilhado de dados pessoais.

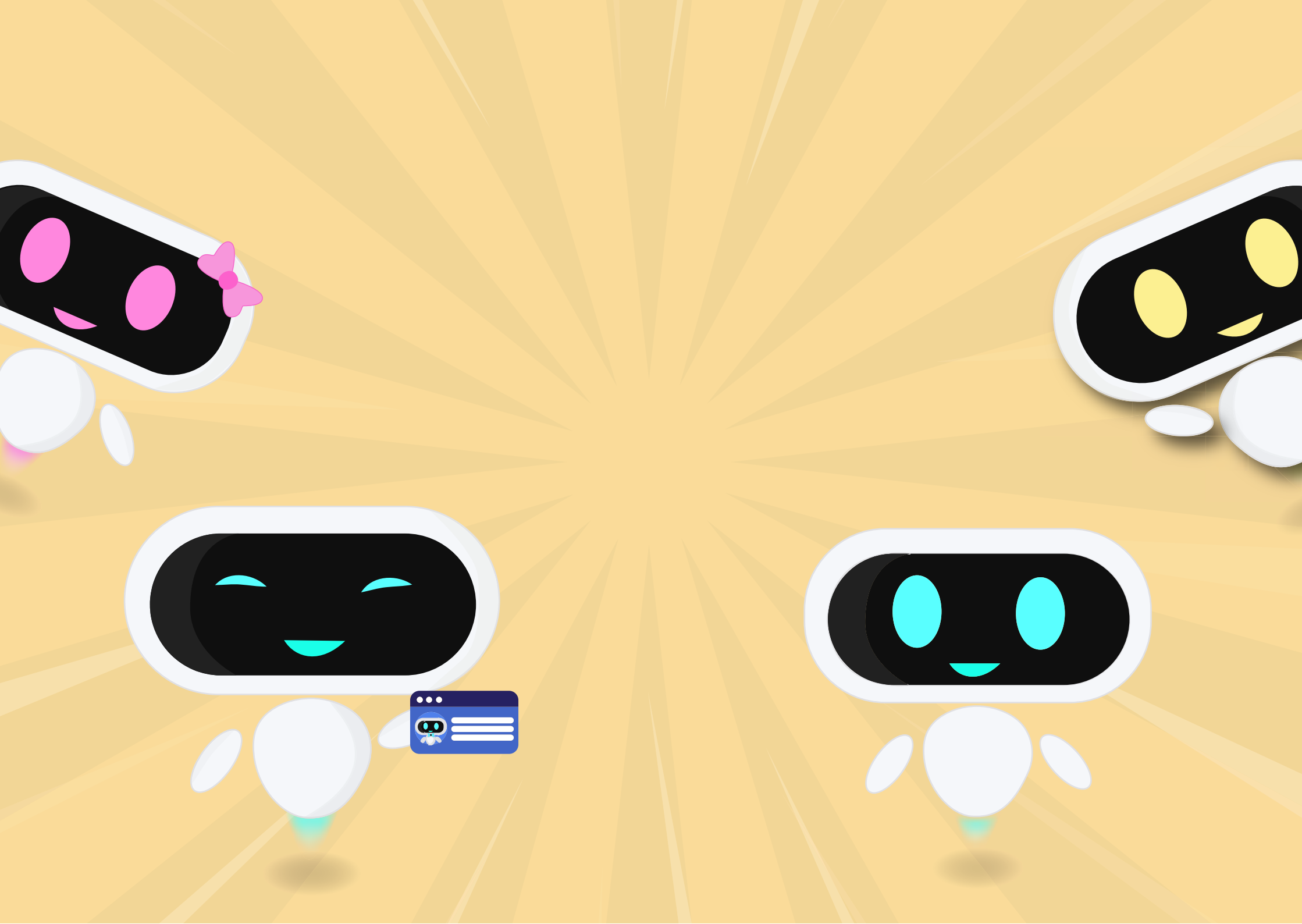
Esse direito garante que qualquer cidadão solicite à Prefeitura da Cidade de São Paulo informações sobre quais organizações do setor público e do setor privado obtiveram acesso aos seus dados pessoais, enquanto tratados pelo Município. Essa informação deve ser, é claro, acompanhada da razão desse uso compartilhado de dados pessoais.

O exercício desse direito por você, enquanto titular de dados pessoais, também se traduz em um auxílio à promoção da transparência pela Prefeitura – uma transparência sobre o tratamento de seus dados pessoais!

10.8. Direito à informação sobre a possibilidade da recusa do consentimento

Esse direito permite que você, em um contexto específico de tratamento de dados pessoais realizado a partir de seu consentimento, solicite à Prefeitura da Cidade de São Paulo informações sobre quais seriam as eventuais consequências em caso de uma negativa de seu consentimento ao tratamento de seus dados pessoais.

Assim, você, enquanto titular, mantém o controle sobre o tratamento de seus dados pessoais e pode avaliar, de forma consciente, a partir de todas as informações disponibilizadas pelo Município, as eventuais consequências em caso de sua recusa em dispor de seus dados pessoais a um tratamento a ser realizado pela Prefeitura.



11. EM QUAIS SITUAÇÕES É POSSÍVEL TRATAR DADOS PESSOAIS?

Ao falarmos sobre o tratamento de dados pessoais, muito se comenta sobre o consentimento do titular ao tratamento de seus dados. Entretanto, o consentimento não é a regra a ser sempre seguida e sim apenas uma das diversas hipóteses legais que autorizam um tratamento de dados pessoais e de dados pessoais sensíveis.

A Administração Pública, nesse sentido, dificilmente se utiliza do consentimento dos titulares a fim de realizar as suas atividades de tratamento de dados pessoais. Em muitos

dos casos, por exemplo, o tratamento é justificado diante da necessidade do cumprimento de obrigações legalmente pré-estabelecidas e à realização de políticas públicas previstas em atos normativos ou respaldadas em contratos administrativos, convênios e instrumentos congêneres.

A LGPD diferencia as hipóteses em que é possível existir o tratamento de *dados pessoais* e as hipóteses em que é possível existir o tratamento de *dados pessoais sensíveis.* Essa diferenciação é importante a fim de restringir o tratamento de *dados pessoais sensíveis*, que são atributos que, quando relacionados à *pessoa natural/física*, tornam-na sensivelmente mais identificada que na hipótese do tratamento apenas de *dados pessoais.*

11.1. Quais são as hipóteses de tratamento de dados pessoais?

Conforme a LGPD, é possível haver um tratamento de dados pessoais:

(i) mediante o fornecimento de consentimento pelo titular;

(ii) para o cumprimento de obrigação legal ou regulatória pelo controlador;

(iii) pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em atos normativos ou respaldadas em contratos, convênios ou instrumentos congêneres;

(iv) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

(v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do próprio;

(vi) para o exercício regular de direitos em processos judicial, administrativo ou arbitral, esse último nos termos da Lei de Arbitragem;

(vii) para a proteção da vida ou da incolumidade física do titular ou de terceiro;

(viii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

(ix) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e

(x) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

11.2. Quais são as hipóteses de tratamento de dados pessoais sensíveis?

Como dispõe a LGPD, é possível haver o tratamento de *dados pessoais sensíveis:*

(i) mediante o fornecimento de consentimento pelo titular;

(ii) para o cumprimento de obrigação legal ou regulatória pelo controlador;

(iii) pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em atos normativos;

(iv) para a realização de estudos por órgãos de pesquisa, garantia, sempre que possível, a anonimização dos dados pessoais sensíveis;

(v) para o exercício regular de direitos em contratos e em processos judicial, administrativo ou arbitral, esse último nos termos da Lei de Arbitragem;

(vi) para a proteção da vida ou da incolumidade física do titular ou de terceiro;

(vii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; e

(viii) para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no artigo 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais sensíveis.

11.3. Hipóteses de tratamento comuns aos dados pessoais e aos dados pessoais sensíveis

Conforme a LGPD, muitas das hipóteses são comuns ao tratamento de *dados pessoais* e de *dados pessoais sensíveis*. Nesse sentido, porém, destaca-se que:

(i) a hipótese de tratamento relativa ao consentimento do titular, apesar de ser comum a ambas as categorias de dados, quando da hipótese relativa aos *dados pessoais sensíveis*, requer a sua coleta de forma específica e destacada, para finalidades específicas; e

(ii) a hipótese relativa ao tratamento e uso compartilhado de dados pela Administração Pública, apesar de ser comum a ambas as categorias de dados, é mais restritiva quando da hipótese relativa aos *dados pessoais sensíveis*, porque pode ser utilizada à execução de políticas públicas previstas apenas em atos normativos (leis ou regulamentos), frente à sua utilização à execução de políticas públicas previstas em atos normativos (leis ou regulamentos) ou também respaldadas em contratos, convênios ou instrumentos congêneres, quando da hipótese referente aos *dados pessoais.*

11.4. Hipóteses de tratamento exclusivamente relacionadas aos dados pessoais

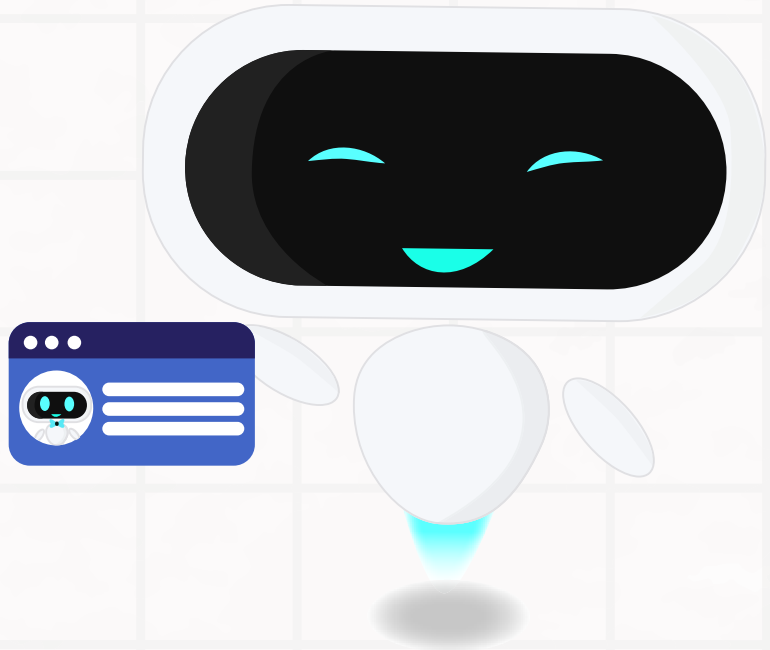
Conforme a LGPD, algumas das hipóteses são exclusivas aos *dados pessoais*, ou seja, não possuem hipótese semelhante que se aplique ao tratamento de *dados pessoais sensíveis:*

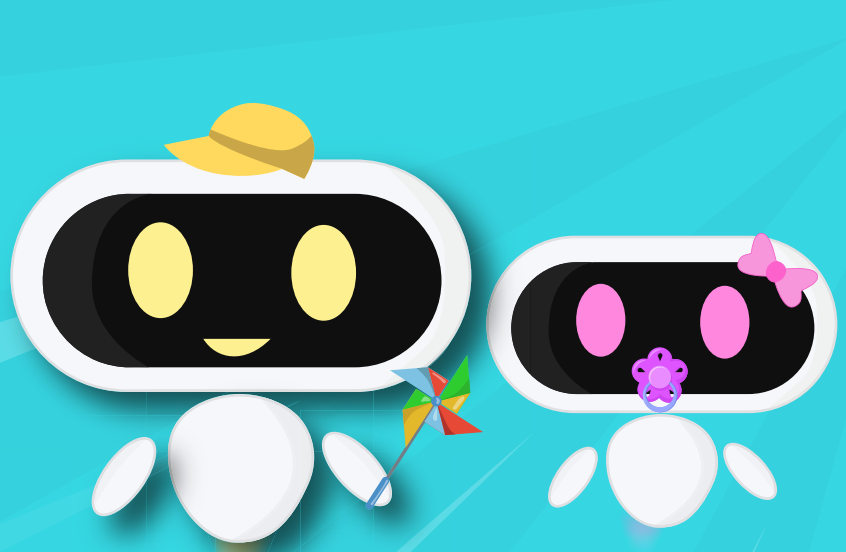
(i) a hipótese relativa ao tratamento de dados pessoais quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e

(ii) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

11.5. Hipótese de tratamento exclusivamente relacionada aos dados pessoais sensíveis

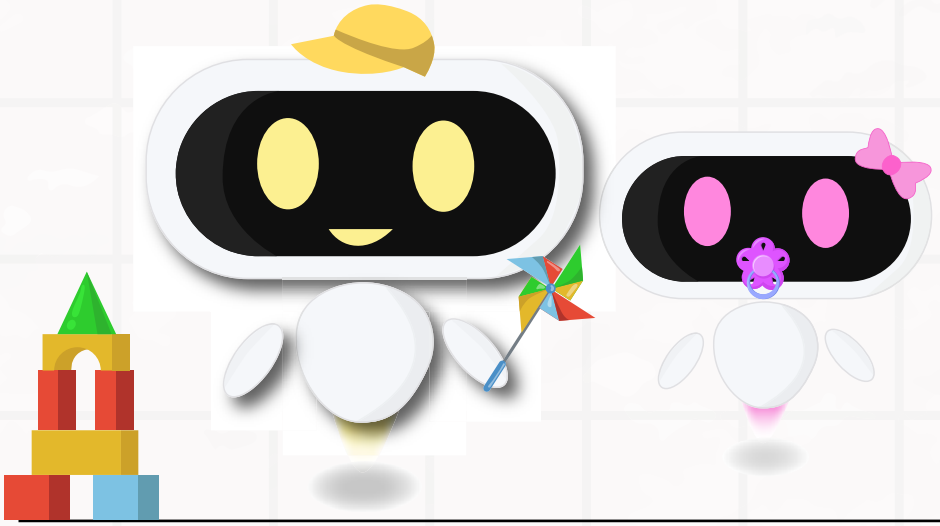
Como dispõe a LGPD, há uma hipótese exclusiva de tratamento de *dados pessoais sensíveis*, que é a hipótese de tratamento de dados pessoais sensíveis para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no artigo 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais sensíveis.





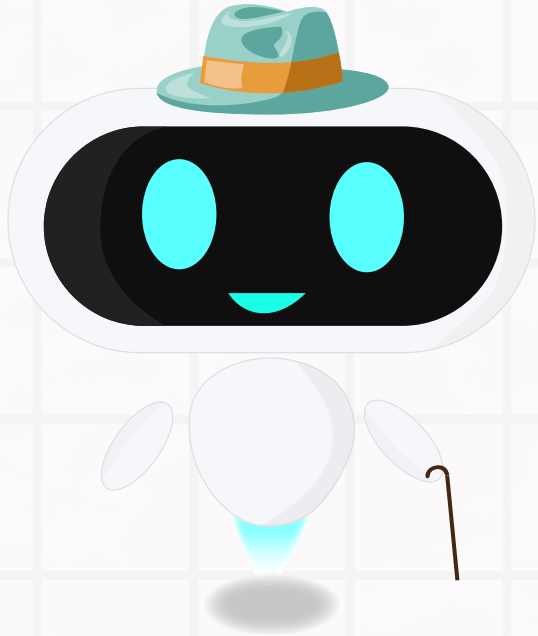
12. TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E DE ADOLESCENTES

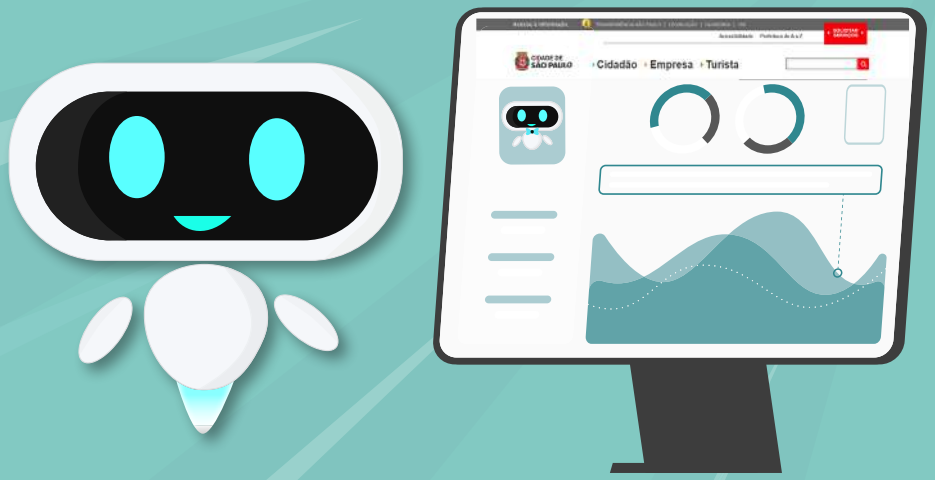
Além das hipóteses de tratamento de dados pessoais e de dados pessoais sensíveis, a LGPD também traz requisitos legais que devem ser observados quando do tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, a Lei dispõe que o *tratamento de dados pessoais de crianças e adolescentes deverá, sempre, ser realizado em seu melhor interesse*, nos termos do Estatuto da Criança e do Adolescente (ECA) e da própria LGPD.



13. TRATAMENTO DE DADOS PESSOAIS DE IDOSOS

Além das hipóteses de tratamento de dados pessoais e de dados pessoais sensíveis, a LGPD também traz requisitos legais que devem ser observados quando do tratamento de dados pessoais de idosos. Nesse sentido, a Lei dispõe que a Autoridade Nacional de Proteção de Dados (ANPD) deve garantir que o tratamento de dados de idosos *seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento*, nos termos do Estatuto do Idoso e da própria LGPD.




Cidadão
Empresa
Turista

14. TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

A LGPD traz disposições específicas ao tratamento de dados pessoais pelo Poder Público. O primeiro questionamento que pode ser feito sobre esse tema é, justamente: *"quem é o Poder Público?"*

Conforme esclareceu o Guia Orientativo sobre tratamento de dados pessoais pelo Poder Público, da ANPD, o conceito abrange os órgãos dos entes federativos (União, Estados, Distrito Federal e Município) dos três Poderes (Executivo, Legislativo e Judiciário), inclusive os Tribunais de Contas e o Ministério Público. Além disso, conforme interpretação sistemática da LGPD, o conceito também inclui:

(i) os serviços notariais e de registro; e

(ii) as entidades dos entes federativos dos três Poderes, inclusive as fundações e as empresas estatais (empresas públicas e sociedades de economia mista) que:

a. não estejam atuando em regime de concorrência; ou

b. estejam a operacionalizar políticas públicas.

Como dispõe a LGPD, o tratamento de dados pessoais pelo Poder Público deve ser realizado para o atendimento de *finalidade pública, na consecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.*

Nesse mesmo sentido, em respeito ao princípio da transparência, a LGPD estabelece a *necessidade de que o tratamento de dados pessoais pelo Poder Público seja guiado pela publicidade das informações sobre as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais*, fornecendo informações claras e

atualizadas sobre a previsão legal, a finalidade e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sites.

Necessário, também, o destaque da Lei que estabelece que os prazos e os procedimentos para o exercício dos direitos pelos titulares de dados pessoais perante o Poder Público devem observar as normas específicas a este relacionadas, especialmente as disposições constantes na Lei do Habeas Data (Lei Federal nº 9.507/1997) e na Lei de Acesso à Informação (Lei Federal nº 12.527/2011).

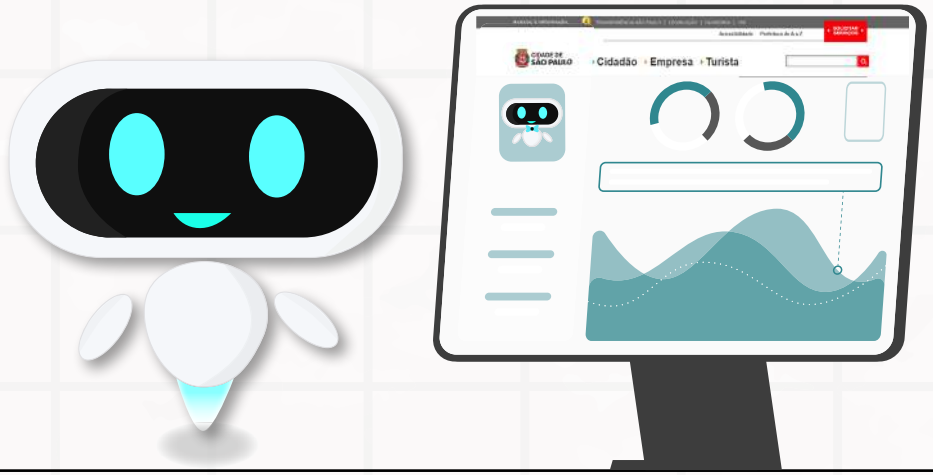
14.1. Uso compartilhado de dados pessoais pelo Poder Público

Especificamente sobre o uso compartilhado de dados pelo Poder Público, a LGPD trata da necessidade da interoperabilidade entre os sistemas a fim de que os entes públicos possam utilizar-se do uso compartilhado de dados pessoais com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Esse uso compartilhado deve atender às finalidades específicas de execução de políticas públicas ou de atribuições legais do Poder Público.

14.2. Uso compartilhado de dados pessoais entre Poder Público e entes privados

Para além do uso compartilhado de dados pessoais entre os órgãos e entidades do Poder Público, a LGPD disciplina o uso compartilhado entre estes e os entes privados, estabelecendo como regra o consentimento do titular como hipótese legal, porém também tornando-o possível a partir das hipóteses em que há a dispensa do consentimento do titular, enquanto previstas pela Lei.

Como traz a LGPD, esse uso compartilhado de dados deve ser informado à ANPD, de acordo com regulamentação ainda a ser elaborada pela Autoridade. Nesse sentido, na Cidade de São Paulo, o artigo 14 do Decreto Municipal nº 57.767/2020 dispôs que o uso compartilhado de dados pessoais entre a Administração Pública Municipal e os entes privados deverá ser informado ao Controlador Geral do Município, enquanto Encarregado pelo Tratamento de Dados Pessoais da Prefeitura do Município, a fim de que o informe à ANPD, na forma de regulamentação da Autoridade, que ainda será elaborada.



14.3. Transferência internacional de dados pessoais pelo Poder Público

A transferência internacional de dados pessoais é uma espécie de uso compartilhado de dados. Constitui-se pela transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o Brasil seja membro. A LGPD traz as hipóteses legais que permitem a realização de uma transferência internacional de dados pessoais. Nesse sentido, ela é possível:

(i) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei;

(ii) quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de:

a. cláusulas contratuais específicas para determinada transferência;

b. cláusulas-padrão contratuais;

c. normas corporativas globais; e

d. selos, certificados e códigos de conduta regularmente emitidos.

(iii) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

(iv) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

(v) quando a ANPD autorizar a transferência;

(vi) quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

(vii) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, desde que seja dada a publicidade nos termos da LGPD;

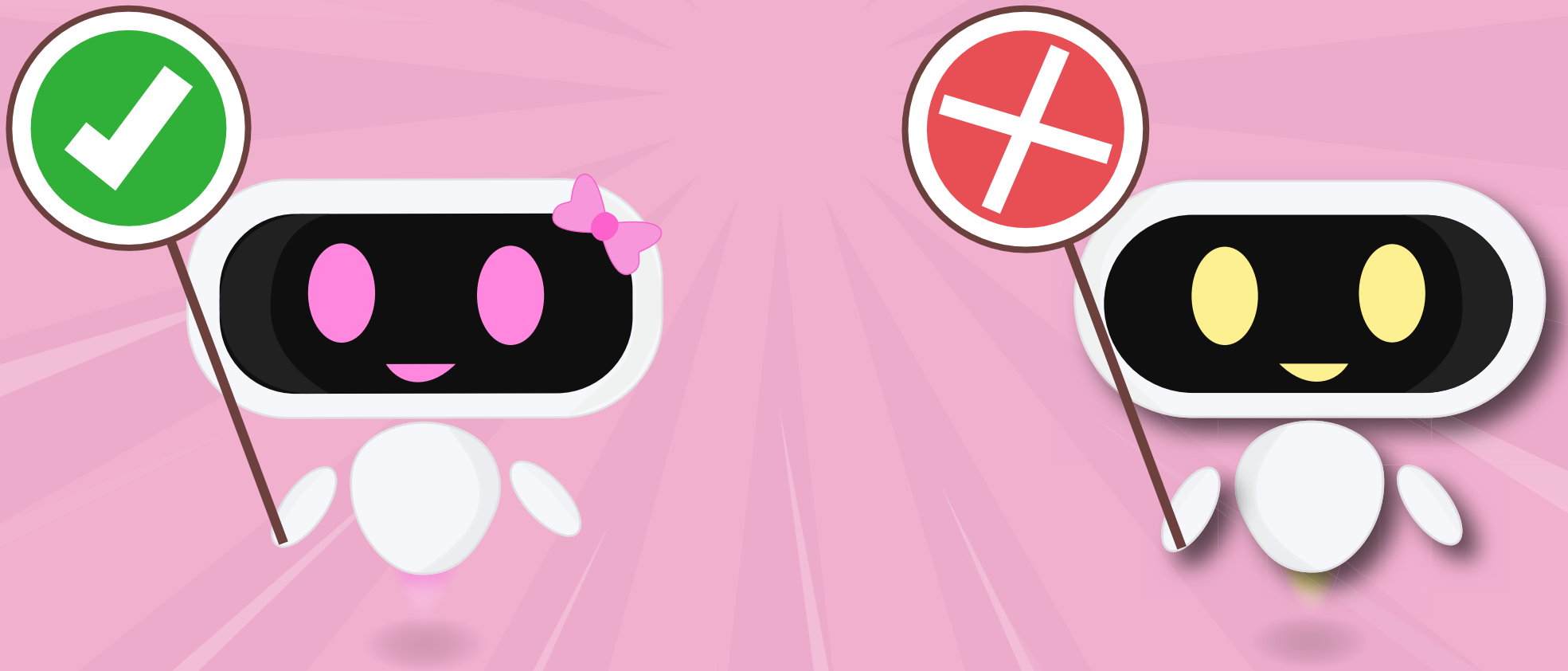
(viii) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

(ix) quando necessário para atender as hipóteses de:

a. cumprimento de obrigação legal ou regulatória pelo controlador;

b. execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; e

c. exercício regular de direitos em processo judicial, administrativo ou arbitral.



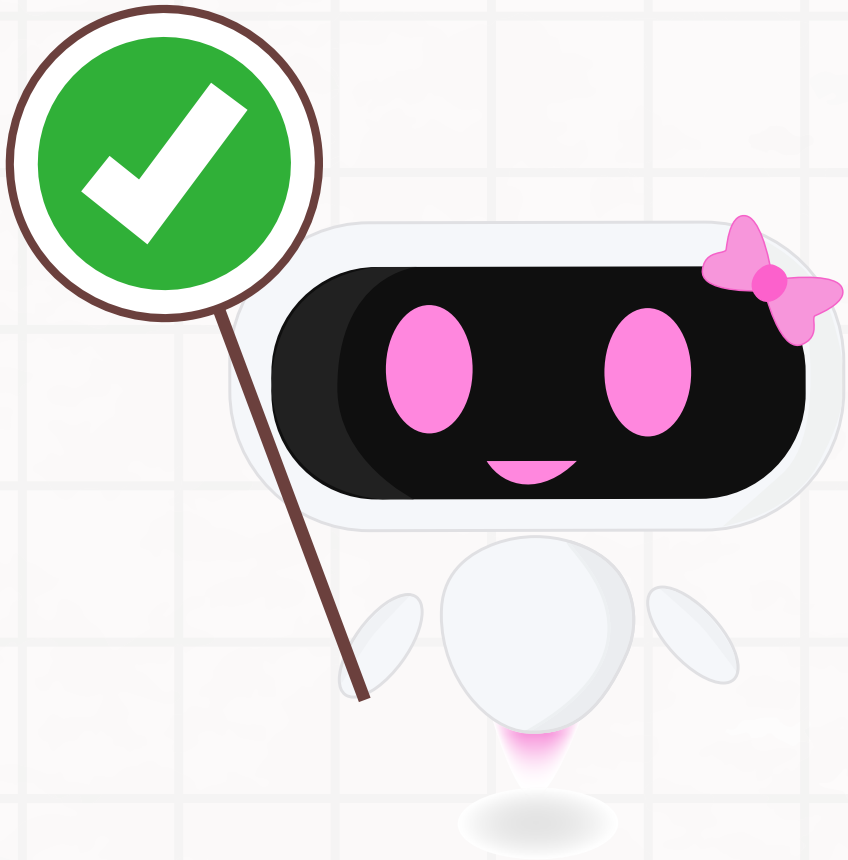
15. EM QUAIS CONTEXTOS A LGPD SE APLICA?

Os direitos à privacidade e à proteção de dados pessoais, como previstos constitucionalmente, valem, nos termos das normas que a regulam, para todos os contextos. A LGPD, porém, não é uma norma que regula o direito à proteção de dados pessoais em todos os contextos, ou seja, possui âmbito de aplicação limitado, determinado a partir de seu artigo 3º, que estabelece que as disposições da LGPD se aplicam para qualquer tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica, de direito público ou de direito privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados pessoais, desde que uma das seguintes condições seja atendida:

(i) o tratamento de dados pessoais seja realizado em território brasileiro;

(ii) os dados pessoais objeto do tratamento de dados, realizado em território estrangeiro, tenham sido coletados em território brasileiro; ou

(iii) o tratamento de dados pessoais tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados pessoais de pessoas naturais localizadas em território brasileiro.



16. EM QUAIS CONTEXTOS A LGPD NÃO SE APLICA?

A LGPD não é uma norma que regula o direito à proteção de dados pessoais em todos os contextos. Nesse sentido, como dispõe o seu artigo 4º, a Lei não se aplica quando o tratamento de dados pessoais:

(i) é realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

(ii) é realizado para fins exclusivamente:

a. jornalísticos;

b. artísticos;

c. acadêmicos, observados, excepcionalmente, os artigos 7º e 11 da LGPD, que tratam das hipóteses de tratamento de dados pessoais;

d. de segurança pública;

e. de segurança do Estado;

f. de defesa nacional; ou

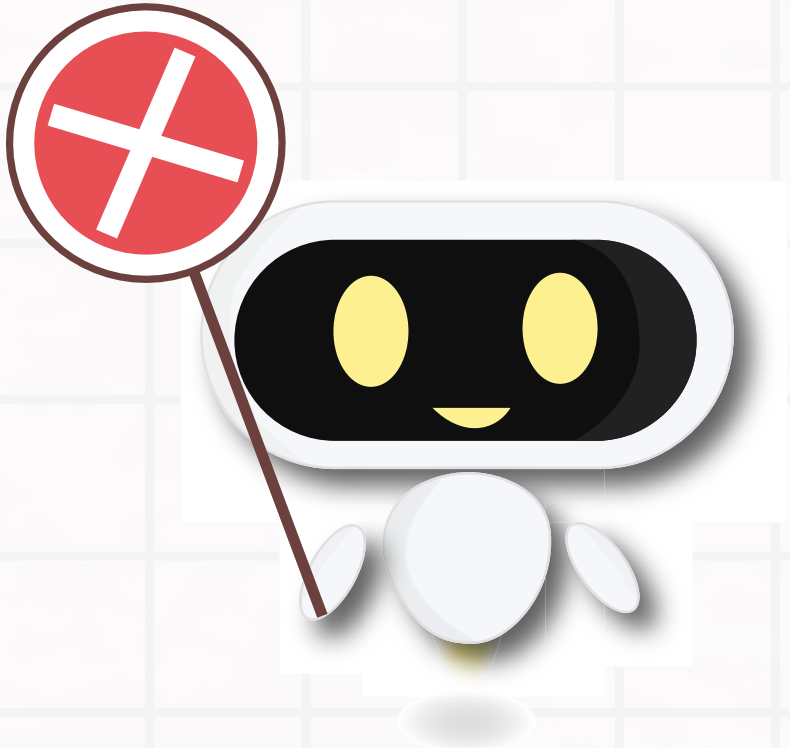
g. de atividades de investigação e repressão de infrações penais; ou

(iii) é proveniente de fora do território brasileiro e:

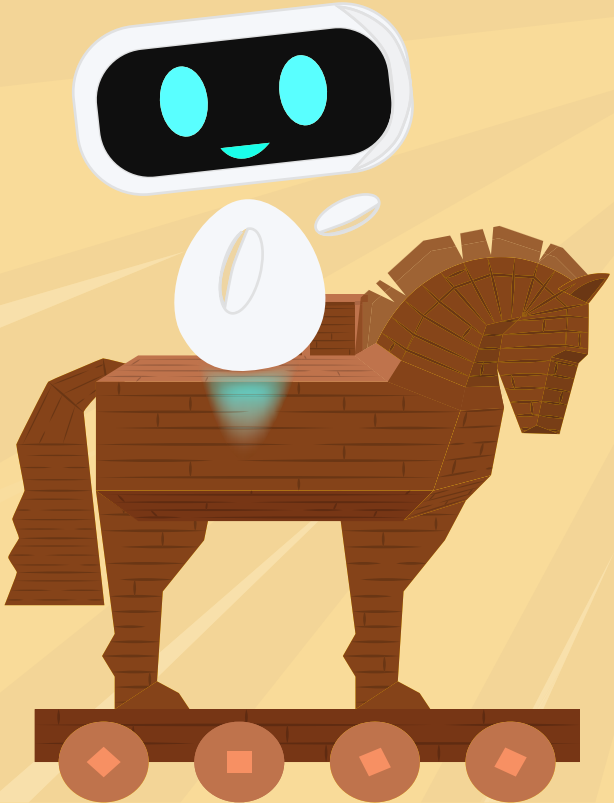
a. sobre o qual não tenha havido transferência internacional de dados pessoais a agentes de tratamento brasileiros; ou

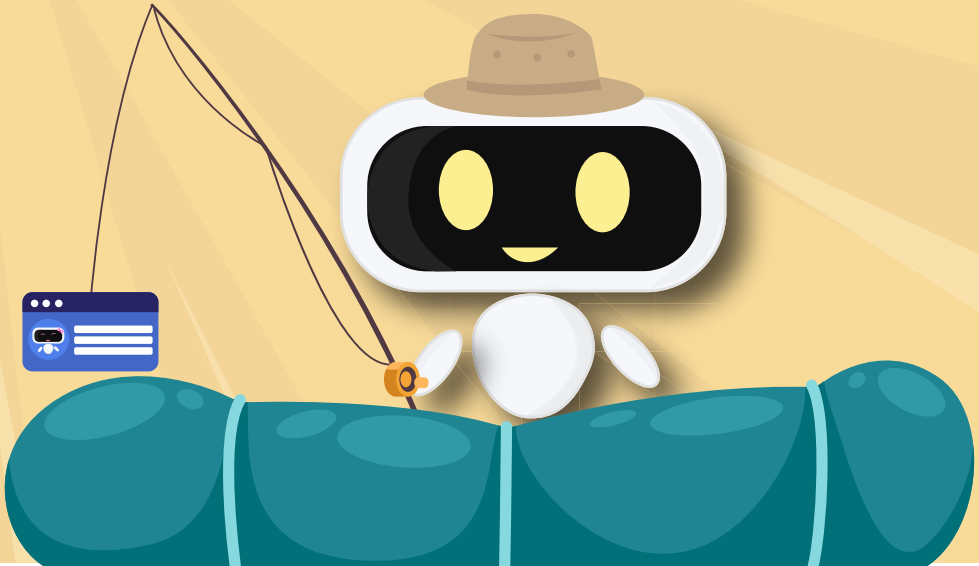
b. sobre o qual não tenha havido transferência internacional de dados pessoais com outro país que não o Brasil, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto pela LGPD.

Apesar disso, o tratamento de dados pessoais realizado para fins exclusivos de segurança pública, de segurança do Estado, de defesa nacional e de investigação e repressão de infrações penais será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.




SEUS
DADOS





17. SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um tema inseparável da proteção de dados pessoais, já que *os dados, quando interpretados, pelas pessoas naturais/físicas ou pela Inteligência Artificial (IA)*, se tornam informações. Assim, tanto a proteção de dados quanto a segurança da informação precisam caminhar juntas.

Nesse contexto, é importante conhecermos os três princípios da segurança da informação: a *confidencialidade*, a *disponibilidade* e a *integridade* dos dados e das informações.

A *confidencialidade* traz a noção de que os dados e as informações devem ser acessíveis apenas por pessoas autorizadas, o que visa a garantir que dados e informações confidenciais não caiam em mãos erradas. A quebra da confidencialidade (acesso não autorizado de terceiro), além de já ser um incidente de segurança, também pode gerar, por exemplo, um vazamento de dados pessoais.

A *disponibilidade*, por sua vez, é a ideia de que os sistemas que mantêm os dados e as informações permaneçam disponíveis quando se fizerem necessárias, isto a fim de evitar a interrupção do uso desses dados e dessas informações. Qualquer interrupção pode gerar, por exemplo, a interrupção da prestação de um serviço público.

A *integridade*, por fim, garante que os dados e as informações sejam precisos, ou seja, que não sejam alterados de forma não autorizada. Qualquer alteração indevida pode, por exemplo, comprometer a confiabilidade dos dados e das informações.

17.1. Melhores práticas para a segurança da informação na Internet

No contexto da segurança da informação, é preciso entendermos sobre as melhoras práticas para a proteção de dados pessoais na Internet. Aqui vão algumas dicas:

(i) Senhas: use senhas únicas e complexas para cada conta. Combine letras maiúsculas, minúsculas, números e caracteres especiais;

(ii) Autenticação de dois fatores: ative a necessidade de mais de uma forma de sua identificação, como senha mais código enviado por *e-mail*, sempre que possível. Isso adiciona uma camada extra de segurança à sua conta;

(iii) Atualizações periódicas: mantenha o seu sistema operacional, os aplicativos e o antivírus atualizados, para a correção de vulnerabilidades detectadas, ao longo do tempo, pelos usuários e pelos fabricantes dos *softwares*;

(iv) *E-mails*: desconfie de e-mails com links e documentos não solicitados. Não clique em nada que pareça duvidoso. Sempre cheque os remetentes dos e-mails que você tenha recebido;

(v) Redes *Wi-Fi*: evite usar redes *Wi-Fi* públicas não seguras para atividades que envolvam a sua privacidade e os seus dados pessoais, como o acesso a aplicativos de contas bancárias;

(vi) *Backup:* faça, regularmente, uma cópia de seus arquivos. Em caso de perda de seu celular ou de seu computador, você estará mais garantido com o *backup* salvo;

(vii) Redes sociais: ajuste suas configurações de privacidade e compartilhe seus dados pessoais com cuidado. Atente-se às Políticas de Privacidade – são muito importantes para conhecer as finalidades pelas quais existe, nas redes sociais, o tratamento de seus dados pessoais!

(viii) Navegação: use um navegador seguro, atualizado e evite navegar em *websites* não confiáveis.

17.2. Phishing

O *phishing* (do inglês que, literalmente, significa uma "*pescaria*" de dados) é um golpe que usa e-mails ou mensagens falsas para enganar (pescar/fisgar!) as pessoas a fornecer dados pessoais, como senhas e números de cartão de crédito. Para se proteger, é importante estar atento e nunca fornecer dados pessoais em resposta a um pedido inesperado. Aqui estão algumas dicas para não cair na *pescaria*:

(i) Desconfie de *e-mails* suspeitos: se você receber um *e-mail* não solicitado com *links* ou documentos suspeitos, não clique! Verifique, sempre, o remetente;

(ii) Verifique os *URLs* presentes no *e-mail*: antes de clicar em um link, passe o mouse sobre ele, sem clicar, para ver o real endereço eletrônico. Se parecer estranho ou suspeito, evite!

(iii) Atenção às mensagens de texto: golpistas usam mensagens de texto para roubar os seus dados pessoais. Nunca clique em *links* de SMS de remetentes desconhecidos;

(iv) Cuidado com *pop-ups* (janelas que se abrem, no navegador, ao visitar uma página): evite clicar em *pop-ups* que solicitam dados pessoais, como nome, telefone e número de cartão de crédito;

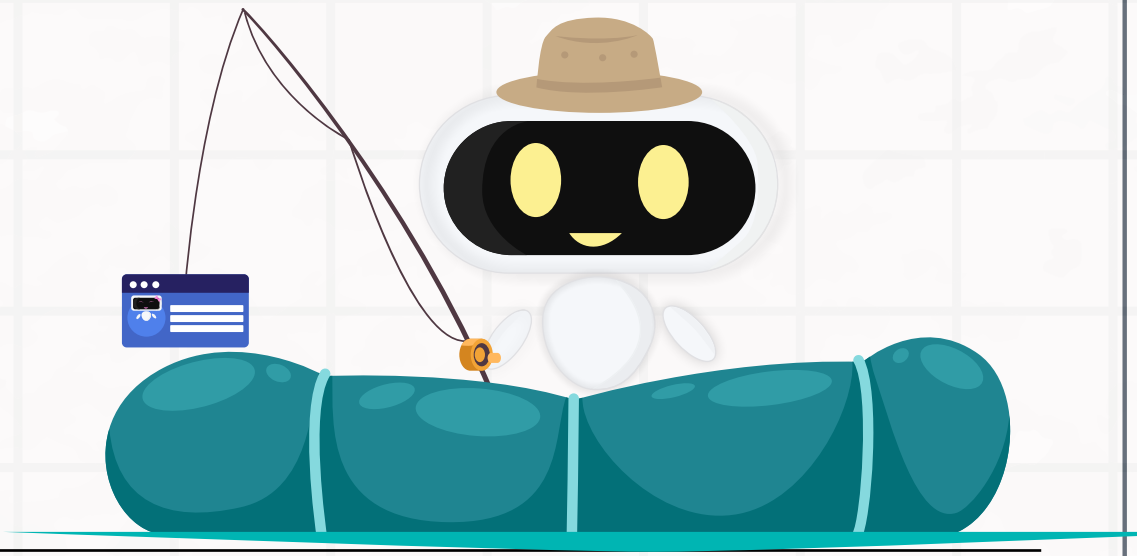
(v) Atualizações periódicas: mantenha o seu sistema operacional, os aplicativos e o antivírus atualizados! Isso ajuda na proteção contra *exploits* (códigos de softwares maliciosos usados em ataques de *phishing*)!

(vi) Não compartilhe os seus dados pessoais com qualquer um: nunca compartilhe os seus dados pessoais, como senhas e números de cartão de crédito, em *websites* desconhecidos;

(vii) Verifique a autenticidade do remetente: prestadores de serviços autênticos geralmente não solicitam dados pessoais por *e-mail*. Sempre ligue para o prestador para confirmar a sua autenticidade! e

(viii) *Denuncie!* Se receber um *e-mail* ou SMS que suspeite ser um *phishing*, denuncie para o seu prestador de serviços de Internet ou para a operadora de telefonia.

Ficar atento ao *phishing é* essencial para manter a sua privacidade e os seus dados pessoais seguros. Pratique essas dicas e proteja-se *online!*



17.3. Malware

Malware é um termo que se refere a qualquer *software* desenvolvido com a intenção manifesta de causar danos a qualquer dispositivo telemático ou informático ou até mesmo a toda uma rede.

Nesse sentido, não se confunde com erros no desenvolvimento de *softwares* – tenha sempre a ideia que o *malware* é um *software* que tem uma intenção maliciosa e que deve ser evitada!

Assim, a seguir, trazemos algumas dicas para identificar e evitar esses *softwares* maliciosos:

(i) Atualizações periódicas: mantenha o seu sistema operacional, os aplicativos e o antivírus atualizados! Isso ajuda na identificação e na remoção de um *malware*, além de ajudar na correção de vulnerabilidades detectadas, ao longo do tempo, pelos usuários e pelos fabricantes dos *softwares;*

(ii) Cuidado com *downloads*: evite baixar documentos de remetentes desconhecidos. Utilize-se apenas de *websites* e lojas de aplicativos confiáveis;

(iii) *E-mails* suspeitos: não clique em *links* ou abra documentos de *e-mails* suspeitos. Sempre cheque o remetente do *e-mail* que você recebeu. Sempre confie, em um primeiro momento, nas indicações de spam de seu *e-mail*!

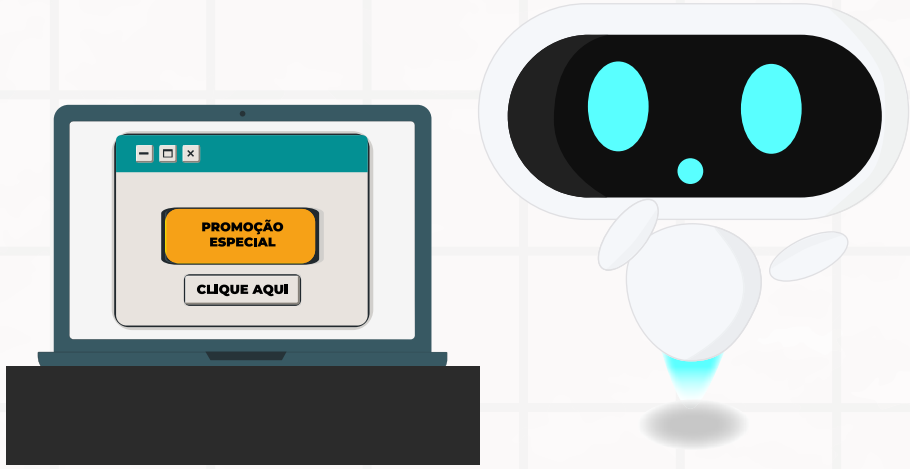
(iv) *Firewall* (sistema de segurança de rede que monitora o tráfego de dados) sempre ativo: mantenha o seu *firewall* sempre ativo e atualizado. O *firewall* age como uma *parede de fogo* (do inglês, "*firewall*") contra *malwares* em potencial, sendo a primeira linha de defesa de seu sistema de segurança contra os tipos mais comuns de *malwares*;

(v) *Backup*: faça, regularmente, uma cópia de seus arquivos. Isso ajuda a recuperar dados e informações em caso de infecção de seu sistema por *malwares*;

(vi) Redes *Wi-Fi:* evite usar redes *Wi-Fi* públicas não seguras, porque podem ser alvos de ataques com *malwares*; e

(vii) Suspeite de ofertas gratuitas! Fique atento às ofertas gratuitas *online*, porque podem esconder os malwares!

Ficar atento aos *softwares* maliciosos é essencial para manter a sua privacidade e os seus dados pessoais seguros. Pratique essas dicas e proteja-se *online*!



17.4. Ransomware

Na campanha informativa preparada pela Controladoria Geral do Município (CGM), continuaremos a falar sobre a segurança da informação – desta vez, traremos o conceito de ransomware e como você pode se proteger!

O *ransomware* é um tipo de *malware* com uma conduta maliciosa específica: após se instalar em seu sistema, o *software* malicioso criptografa alguns de seus dados ou os dados de todo o seu sistema para, então, exigir um preço pelo resgate (literalmente, do inglês, *"ransom"*)!

Aqui estão algumas dicas para não cair no *stress* desse resgate:

(i) Atualizações periódicas: mantenha o seu sistema operacional, os aplicativos e o antivírus atualizados! Isso ajuda na identificação e na remoção de um *ransomware*, além de ajudar na correção de vulnerabilidades detectadas, ao longo do tempo, pelos usuários e pelos fabricantes dos *softwares*;

(ii) *Backup*: faça, regularmente, uma cópia de seus arquivos. Isso ajuda a recuperar dados e informações em caso de infecção de seu sistema por um *ransomware*;

(iii) Cuidado com *downloads*: evite baixar documentos de remetentes desconhecidos. Utilize-se apenas de websites e lojas de aplicativos confiáveis;

(iv) *E-mails* suspeitos: não clique em *links* ou abra documentos de *e-mails* suspeitos. Sempre cheque o remetente do *e-mail* que você recebeu. Sempre confie, em um primeiro momento, nas indicações de *spam* de seu *e-mail*!

(v) Segurança em nuvem: utilize-se de serviços de armazenamento em nuvem confiáveis e protegidos para armazenar os seus dados mais importantes!

Para ajudar nessas ações e em outras relacionadas à segurança da informação, na Prefeitura de São Paulo, contamos com a Secretaria Municipal de Inovação e Tecnologia (SMIT) e a Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo (PRODAM)!

Proteja-se contra os *ransomware* e mantenha o controle de seus dados. A prevenção é a melhor defesa!

17.5. Cavalos de Troia

Conta-se que os gregos, reunidos para a destruição da cidade de Troia e para o resgate de Helena, rainha de Esparta, construíram um grande cavalo de madeira, oco, e deixaram-no às portas de Troia. Os soldados da cidade, então, acreditando que o haviam abandonado, levaram-no ao interior das muralhas troianas, em grande celebração. Ali, à noite, enquanto a cidade dormia, inesperadamente, soldados gregos saíram do interior do cavalo e abriram os portões de Troia para a entrada do exército grego – que, então, a capturaram!

A história da queda de Troia traz a metáfora de que, ao tratarmos sobre a proteção de dados pessoais e sobre a segurança da informação, devemos ter muita atenção com os *e-mails*, *links*, documentos, *softwares* e sistemas que nos utilizamos!

Assim, em segurança da informação, um cavalo de Troia é entendido como um *malware* que se oculta em *softwares* aparentemente nofensivos ou que incentiva você a baixá-lo!

Já dentro de seu dispositivo, ele pode promover a espionagem sobre você e sobre os seus dados a criminosos cibernéticos ou mesmo sequestrar os seus dados pessoais.

Aqui estão algumas dicas para deixar os cavalos de Troia longe dos portões da Prefeitura do Município de São Paulo:

(i) Atualizações periódicas: mantenha o seu sistema operacional, os aplicativos e o antivírus atualizados! Isso ajuda na identificação e na remoção de um cavalo de Troia, além de ajudar na correção de vulnerabilidades detectadas, ao longo do tempo, pelos usuários e pelos fabricantes dos *softwares*;

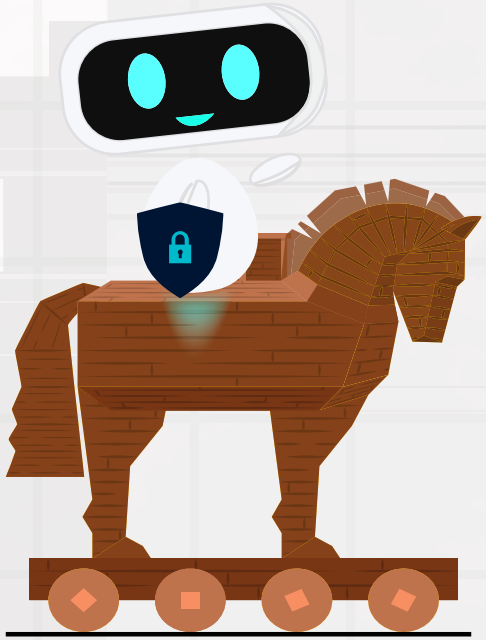
(ii) *Backup*: faça, regularmente, uma cópia de seus arquivos. Isso ajuda a recuperar dados e informações em caso de infecção de seu sistema por um *ransomware*;

(iii) Cuidado com *downloads*: evite baixar documentos de remetentes desconhecidos. Utilize-se apenas de *websites* e lojas de aplicativos confiáveis;

(iv) *E-mails* suspeitos: não clique em *links* ou abra documentos de *e-mails* suspeitos. Sempre cheque o remetente do *e-mail* que você recebeu. Sempre confie, em um primeiro momento, nas indicações de *spam* de seu *e-mail*!

(v) Segurança em nuvem: utilize-se de serviços de armazenamento em nuvem confiáveis e protegidos para armazenar os seus dados mais importantes!

Proteja-se contra os cavalos de Troia e ajude a manter a segurança da informação e a proteção de dados pessoais na Cidade de São Paulo!



Fale com o Encarregado pelo Tratamento de Dados Pessoais

encarregadolgpd@prefeitura.sp.gov.br

Fale com a Coordenadoria de Proteção de Dados Pessoais

privacidade@prefeitura.sp.gov.br

Tenha sempre o controle de seus dados pessoais.... e a Controladoria à sua disposição!

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27002:2022. *Segurança da informação, segurança cibernética e proteção à privacidade* – controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27701:2020. *Técnicas de segurança* – extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – requisitos e diretrizes. Rio de Janeiro: ABNT, 2020.

ALVES, Gustavo Alberto. *Segurança da informação:* uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna, 2006.

BELL, Daniel. The Coming of Post-Industrial Society. *The Educational Forum*, EUA, vol. 40, n. 04, 1976, pp. 574-579.

BRASIL. Lei Federal nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, *Diário Oficial da União*, 18 de novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 21 dez. 2023.

BRASIL. Lei Federal nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, *Diário Oficial da União*, 24 de abril de 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 dez. 2023.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, *Diário Oficial da União*, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 21 dez. 2023.

CASTELLS, Manuel. *A sociedade em rede* – a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. *O fim da milênio* – a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 2000.

CASTELLS, Manuel. *O poder da identidade* – a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel; HIMANEN, Pekka. *A sociedade da informação e o estado de bem-estar social*: o modelo finlandês. Oxford: Oxford University Press, 2002.

FALCÃO, Daniel; PEROLI, Kelvin. As novas abordagens da privacidade: contextos, tipos e dimensões. *Migalhas*, Migalhas de Proteção de Dados Pessoais, 30 dez. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/357252/as-novas-abordagens-da-privacidade-contextos-tipos-e-dimensoes>. Acesso em: 21 dez. 2023.

FALCÃO, Daniel; PEROLI, Kelvin. Imagem, dado pessoal sensível? *Consultor Jurídico*, Observatório Constitucional, 28 maio 2022. Disponível em: <https://www.conjur.com.br/2022-mai-28/observatorio-constitucional-imagem-dado-pessoal-sensivel>. Acesso em: 21 dez. 2023.

KOOPS, Bert-Jaap; NEWELL, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tomislav; GALIČ, Maša. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, vol. 38, n. 2, 2017, art. 4, pp. 483-575.

LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (ed.). *Privacy, Big Data, and the Public Good:* Frameworks for Engagement. New York: Cambridge University Press, 2014.

NISSENBAUM, Helen. *Privacy in Context.* Technology, Policy, and the Integrity of Social Life. Stanford, EUA: Stanford University Press, 2010.

PENTEADO, Luciano de Camargo. O direito à vida, o direito ao corpo e às partes do corpo, o direito ao nome, à imagem e outros relativos à identidade e à figura social, inclusive intimidade. *Revista de Direito Privado*, São Paulo, vol. 13, n. 49, jan./mar. 2012, pp. 73-109.

PEROLI, Kelvin; FALEIROS JÚNIOR, José Luiz de Moura. Comentários aos arts. 50 e 51 da LGPD. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (orgs.). *Comentários à Lei Geral de Proteção de Dados Pessoais.* Indaiatuba: Foco, 2022, pp. 461-479.

SÃO PAULO (Cidade). Controladoria Geral do Município. Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo. Controladoria Geral do Município, São Paulo, 28 jan. 2023. Disponível em: <https://www.prefeitura.sp.gov.br/cidade/secretarias/controladoria_geral/a_cgm/index.php?p=332358>. Acesso em: 21 dez. 2023.

SÃO PAULO (Cidade). Controladoria Geral do Município. Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022. Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. São Paulo, *Diário Oficial da Cidade de São Paulo*, 22 jul. 2022. Disponível em: <https://www.prefeitura.sp.gov.br/cidade/secretarias/controladoria_geral/a_cgm/index.php?p=332358>. Acesso em: 21 dez. 2023.

SÃO PAULO (Cidade). Decreto Municipal nº 59.767, de 15 de setembro de 2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta. São Paulo, Diário Oficial da Cidade de São Paulo, 15 de setembro de 2020. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020>. Acesso em: 21 dez. 2023.

SÃO PAULO (Cidade). Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022. Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. São Paulo, *Diário Oficial da Cidade*, 22 de julho de 2022. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-1-de-21-de-julho-de-2022>. Acesso em: 21 dez. 2023.

SÊMOLA, Marcos. *Gestão da segurança da informação:* uma visão executiva. 2ª ed. Rio de Janeiro: Elsevier, 2013.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Bruxelas, *Jornal Oficial da União Europeia*, 27 abril 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 21 dez. 2023.

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO