



O CIBERESPAÇO NAS *SMART CITIES* SOB A PERSPECTIVA DA PROTEÇÃO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Cyberspace in Smart Cities from the Perspective of Protecting the Personal Data of Children and Teens

Cinthia Obladen de Almendra Freitas¹

RESUMO

Relacionar os temas, crianças e adolescentes, cidades inteligentes e proteção de dados pessoais, em um único trabalho é inovador e permitiu auxiliar na busca pelo seguinte questionamento: Como pensar o ciberespaço de cidades inteligentes para crianças e adolescentes levando em consideração a proteção de dados pessoais? Por meio de método dedutivo e técnica bibliográfica e documental, o objetivo geral do artigo foi apontar elementos jurídico-tecnológicos para auxiliar na garantia de direitos de crianças e adolescentes, especificamente ao que trata da proteção de dados pessoais, considerando o ciberespaço de cidades inteligentes como base de um ecossistema de sustentação tanto tecnológica quanto jurídica. Concluiu-se que esses elementos têm por base as pessoas (crianças e adolescentes), as redes e os sistemas de informação, diante do fluxo de dados no ciberespaço, de maneira que o arcabouço jurídico brasileiro se entrelaça com aspectos tecnológicos advindos da Segurança da Informação, das normas ISO 27000 e da *Privacy by Design/Default* sob uma estratégia coletiva, preventiva e autoprotetiva para crianças e adolescentes, perfazendo um ciclo entre o Direito, as novas tecnologias e a governança em cidades inteligentes.

Palavras-chave: Cidades Inteligentes; Proteção de Dados Pessoais; Crianças e Adolescentes; Ciberespaço.

ABSTRACT

Relating the themes, children and adolescents, smart cities and personal data protection, in a single work is innovative and allowed to assist in the search for the following question: How to think about the cyberspace of smart cities for children and teens, considering the protection of personal data? Based on deductive method and bibliographic and documental technique, the general objective of the article was to point out legal-technological elements to assist in guaranteeing the rights of children and teens, specifically with regard to the protection of personal data, considering the cyberspace of smart cities as basis of an ecosystem of both technological and legal support. It was concluded that these elements are based on people (children and teens), networks and information systems, given the flow of data in cyberspace, so that the Brazilian legal framework is intertwined with technological aspects arising from

¹ Doutora em Informática pela Pontifícia Universidade Católica do Paraná. Professora Titular da Pontifícia Universidade Católica do Paraná - PUCPR (1985-atual). Professora Permanente do Programa de Pós-Graduação (Mestrado/Doutorado) em Direito (PPGD) a partir de 2005. Foi Coordenadora do Programa de Pós-Graduação em Direito (PPGD) da PUCPR (ago/2020-set/2023). Membro Consultor da Comissão de Direito Digital e Proteção de Dados da OAB/PR (Portaria 142/2019). Membro da Diretora do Instituto Nacional de Proteção de Dados - INPD (2019-atual). Coordenadora do Curso de Especialização em Direito Digital da PUCPR (2021-atual).



Information Security, ISO 27000 and Privacy by Design/Default standards under a collective, preventive and self-protective strategy for children and teens, creating a cycle between Law, new technologies and governance in smart cities.

Key words: Smart Cities; Personal Data Protection; Children and Teens; Cyberspace.

1. INTRODUÇÃO

Crianças e adolescentes são uma preocupação essencial e especial quando o tema de estudo envolve a proteção de dados pessoais no ciberespaço de cidades inteligentes. Vive-se e cada vez mais se viverá em uma sociedade de algoritmos. E, a relação das crianças e dos adolescentes com a tecnologia é crescente e ao mesmo tempo exige reflexões, seja pelos pais e/ou responsáveis ou pelo Estado. E, o Direito não pode ser deixado de lado nessas temáticas, visto que é o Direito que ao mesmo tempo questiona e também busca assegurar direitos fundamentais e estabelecer tanto limitações quanto responsabilidades, sejam essas para as empresas ou para o Estado.

A sociedade de algoritmos mostra que a atualidade está frente a um paradoxo: de um lado a extrema riqueza urbana, a ponto de equacionar-se e implantar-se cidades inteligentes, mas de outro a pobreza, a fome e os problemas ambientais. Esse paradoxo é ainda ampliado pela economia baseada em dados (*data-driven economy*) e, novamente, os algoritmos estão em cena. Eis um cenário complexo que também envolve crianças e adolescentes, pois vivem em cidades e utilizam das novas tecnologias, por consequência, estão imersos em um ecossistema algorítmico. Nunca foi tão relevante estudar e discutir sobre as novas relações entre indivíduo, dados e sociedade.

Por outro lado, cabe lembrar que a Convenção sobre os Direitos da Criança (CDC), a Constituição Federal de 1988 (CF/88) e o Estatuto da Criança e do Adolescente (ECA) postulam por meio de seus dispositivos 04 (quatro) grupos de direitos da criança e do adolescente: à vida, ao desenvolvimento, à proteção e à participação; sem deixar de lado outros dispostos ou aspectos relevantes incluso em tratados internacionais de Direitos Humanos.

Há que se mencionar ainda o Marco Civil da Internet (MCI) que estabelece o exercício de controle parental de conteúdo entendido pelos pais e responsáveis como impróprio a seus filhos menores, desde que respeitados os princípios do próprio MCI e do ECA. E, ainda, a Lei



Geral de Proteção de Dados Pessoais (LGPD) que apresenta uma seção específica sobre tratamento de dados pessoais de crianças e adolescentes, estabelecendo uma relação entre pais/responsáveis, controladores e dados pessoais por meio das operações de tratamento de dados.

Nasce assim o questionamento que norteou a pesquisa: Como pensar o ciberespaço de cidades inteligentes para crianças e adolescentes levando em consideração a proteção de dados pessoais?

Por meio de método dedutivo e técnica bibliográfica e documental, o artigo tem por objetivo geral apresentar elementos jurídico-tecnológicos a serem observados em cidades inteligentes sob a perspectiva da garantia de direitos das crianças e adolescentes. Para tanto, inicia-se descrevendo a relação das crianças e dos adolescentes com as Tecnologias de Informação e Comunicação (TICs), visto que o meio ambiente digital é o cenário principal das cidades inteligentes. Na sequência, adentra-se ao estudo da proteção de dados pessoais de crianças e adolescentes no ciberespaço de cidades inteligentes. E, finalmente, são descritos elementos jurídico-tecnológicos para auxiliar na garantia de direitos, na proteção de dados pessoais, considerando o ciberespaço de cidades inteligentes como base de um ecossistema de sustentação tanto tecnológica quanto jurídica.

O artigo é resultado de projeto de pesquisa financiado pelo Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (PROCAD/SPCF) da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

2. A RELAÇÃO DAS CRIANÇAS E DOS ADOLESCENTES COM AS TICS

Os principais resultados do Relatório TIC Kids de 2022, apresentados em 3 de maio de 2023, inicia apontado que o referido relatório teve como objetivo compreender de que forma a população de 9 a 17 anos de idade utiliza a Internet e como lida com os riscos e as oportunidades decorrentes desse uso. Para tal, foram entrevistadas 2.604 crianças e adolescentes e 2.604 pais ou responsáveis, no período de junho de 2022 a outubro de 2022, sendo as entrevistas presenciais (face-to-face). E os resultados mostram que “96% dos usuários de Internet de 9 a 17 anos acessaram a Internet todos os dias ou quase todos os dias” (CETIC.br, 2023, p. 11). Dessa forma, 24,4 milhões acessaram a Internet nos últimos três meses, 1,2 milhão acessaram



a Internet há mais de três meses e somente 950 mil nunca acessaram a Internet, de um total estimado de 26,6 milhões (CETIC.br, 2023, p. 11). Já os dispositivos utilizados de forma exclusiva para acessar a Internet: celulares, televisão, computador e videogame; respectivamente por ordem de representatividade (CETIC.br, 2023, p. 14). Os locais de acesso à internet são: casa, casa de outra pessoa, escola, outros lugares (shopping, igreja ou lanchonete), em deslocamento, centro público de acesso pago e centro público de acesso gratuito (CETIC.br, 2023, p. 15).

Em termos de atividades realizadas na Internet, tem-se que: a) multimídia: 87% ouviu música online e 82% assistiu a vídeos, programas, filmes ou séries online; b) educação: 80% pesquisou na Internet para fazer trabalhos escolares e 65% pesquisou na Internet por curiosidade ou por vontade própria; c) comunicação: 79% enviou mensagens instantâneas e 32% conversou por chamada de vídeo (CETIC.br, 2023, p. 17).

Interessante observar que 86% dos usuários de Internet de 9 a 17 anos possuem perfil em rede social, sendo essas por ordem de representatividade: WhatsApp, Instagram, TikTok, Facebook, Twitter e Snapchat (CETIC.br, 2023, p. 18). Já as redes sociais mais utilizadas são: TikTok (35%), Instagram (35%) e Facebook (7%).

No quesito sobre jogos *online*, o relatório aponta que 57% dos usuários de Internet de 9 a 17 anos fazem uso de jogos *online* não conectado com outros jogadores e 585% fazem uso conectado com outros jogadores (CETIC.br, 2023, p. 19). E, ainda, que em torno de 40% jogam todos os dias ou quase todos os dias, conectados ou não com outros jogadores (CETIC.br, 2023, p. 19).

Alguns resultados chamam à atenção: 33% dos usuários de Internet de 9 a 17 anos reportaram ter acontecido alguma coisa na Internet que não gostaram, os ofenderam ou chatearam e 30% usaram a Internet para procurar ajuda quando aconteceu algo ruim ou para conversar sobre as emoções quando se sentiram tristes (CETIC.br, 2023, p. 20). Percebe-se aqui um paradoxo, visto que a Internet pode ser tanto fonte de tristeza quanto o meio buscado para encontrar ajuda quando se sentem tristes. Deve-se ainda observar para quem esses usuários reportaram sobre situações ofensivas que ocorreram na Internet: as meninas reportam mais para amigo(a) (16%) e pais ou responsáveis (13%) e os meninos para pais ou responsáveis (7%) e amigo(a) (6%) (CETIC.br, 2023, p. 20).



Quando o tema é privacidade, o relatório indica que 43% das crianças ou adolescentes se preocupam sempre ou quase sempre, 35% nunca ou quase nunca se preocupam com a privacidade e 22% se preocupam às vezes (CETIC.br, 2023, p. 11). Importante observar que 57% das crianças e adolescentes se preocupam às vezes, quase nunca ou nunca com a privacidade. E, ainda, 56% aponta que nunca ou quase nunca deixa de usar a Internet porque seus pais ou as pessoas que cuidam da criança ou adolescente o(a) impedem de usá-la. O relatório indica também que 72% dos usuários de 11 a 17 anos de idade sabe ajustar as configurações de privacidade, como por exemplo nas redes sociais. Fato que pode ser tanto favorável se for para aumentar as restrições quanto pode ser um risco, caso os usuários “relaxem” os parâmetros de configuração (CETIC.br, 2023, p. 22).

No que tange às habilidades para o uso da Internet, os resultados apontam que os usuários de 11 a 17 anos de idade sabem: 70% denunciar um conteúdo ofensivo relacionado a criança ou a pessoas com quem convive, 62% verificar se um site é confiável, 57% verificar se uma informação encontrada na Internet está correta e 18% usar uma linguagem de programação, como Java ou Python (CETIC.br, 2023, p. 22).

O relatório categoriza as habilidades dos usuários em: operacionais, informacionais, sociais e criativas. Destaca-se como habilidade operacional que 85%, dos usuários de 11 a 17 anos de idade, sabe proteger o celular ou o tablet, como por exemplo, com um PIN, padrão de tela, impressão digital ou reconhecimento facial. Como habilidade informacional, destaca-se que 70% sabe como encontrar um site que visitou antes. Já como habilidade social, 78% sabe como reconhecer quando alguém está sofrendo bullying na Internet. E, finalmente, como habilidade criativa, 52% sabe como diferenciar conteúdo patrocinado e não patrocinado *online*, como em um vídeo ou em uma postagem em redes sociais (CETIC.br, 2023, p. 21).

Esses resultados mostram que as crianças e adolescentes fazem uso intenso da Internet e já estão desenvolvendo habilidades para utilizar como meio de multimídia, educação e comunicação. E a compreensão do meio ambiente digital vai muito além, visto que 74% dos usuários entre 11 e 17 anos concorda que empresas pagam pessoas para usar seus produtos nos vídeos e conteúdos que publicam na Internet, 61% entende que usar *hashtags* aumenta a visibilidade de uma publicação na Internet, 60% concorda que curtir ou compartilhar uma publicação pode ter um impacto negativo em outras pessoas, ou seja, as formas de monetização na Internet e reflexos negativos relacionado às pessoas (CETIC.br, 2023, p. 23). Por outro lado,



51% dos mesmos usuários compreende erroneamente que todos encontram as mesmas informações quando pesquisam coisas na Internet, desconhecendo o conceito de bolhas informacionais (PARISER, 2012).

Os resultados também trazem informações relevantes a dados pessoais e segurança dos usuários de 11 a 17 anos de idade, sendo que 79% é cuidadoso(a) com dados pessoais que diz ou posta na Internet, 77% só usa aplicativos ou sites em que confia, 76% toma cuidado com os links de vídeos em que clica, 73% é cuidadoso(a) com os convites de amizade que aceita na Internet, 63% só compartilha na Internet coisas com amigos próximos, 58% fornece o mínimo de dados pessoais possível ao se registrar online, como em jogos, em redes sociais ou para ouvir música, 55% lê os termos de privacidade dos aplicativos e sites que usa e somente 23% às vezes cobre a câmera do computador ou do celular com um papel ou adesivo para prevenir que seja visto (CETIC.br, 2023, p. 27).

Todas essas habilidades e informações parecem não ser suficientes para impedir o avanço da pornografia infantil (SAFERNET, 2023), do aliciamento de crianças e adolescentes na Internet (FREITAS et al., 2016) e a apologia ao ódio e demais formas de violência contra crianças e adolescentes, a exemplo do aplicativo Discord (UOL, 2023).

E, portanto, o Relatório TIC Kids de 2022, apresenta os resultados obtidos quando os usuários de 11 a 17 anos de idade respondem sobre as estratégias para proteger a privacidade, conforme Tabela 01 que sumariza as principais estratégias e os respectivos resultados. Agregase à referida tabela a categorização da estratégia ser positiva, quando mitiga violações ao direito à proteção de dados e privacidade, e negativa, quando expõe a privacidade dos usuários.

Tabela 01: Estratégias para proteger a privacidade (%) com categorização em positiva ou negativa

Categorização	Estratégia	11-12 anos	13-14 anos	15-17 anos
Estratégias Positivas	Bloquear mensagens de alguém com quem não queria conversar	50	60	71
	Usar senhas seguras ou complicadas, misturando letras maiúsculas e minúsculas, números e símbolos	43	57	67
	Alterar as configurações de privacidade para que	38	47	64



	menos pessoas pudessem ver seu perfil			
Estratégias Negativas	Excluir os registros de histórico de buscas do Google, do YouTube ou de sites que visitou	28	41	41
	Desativar filtros ou controles que existem para impedir de visitar determinados sites	17	17	20
	Escolher usar uma aba anônima ou privada em um navegador da Web como Chrome ou Safari	8	16	24
	Usar um servidor proxy ou VPN para ficar anônimo	4	11	9

Fonte: adaptado de (CETIC.br, 2023, p. 28)

E, portanto, o Relatório TIC Kids de 2022, apresenta os resultados obtidos quando os usuários de 11 a 17 anos de idade respondem sobre as estratégias para proteger a privacidade, conforme Tabela 01 que sumariza as principais estratégias e os respectivos resultados. Agregase à referida tabela a categorização da estratégia ser positiva, quando mitiga violações do direito à proteção de dados e privacidade, e negativa, quando expõe a privacidade dos usuários.

Finalmente, cabe relatar os resultados obtidos a partir das indagações feitas sobre a verificação realizada por responsáveis sobre o uso da Internet, 58% afirmam que consultam o histórico ou registro dos sites visitados pelos usuários de 9 a 17 anos, 58% também afirmar consultar e-mails ou mensagens, 58% afirmam que verificam amigos ou contatos adicionados às suas redes sociais e 53% verificam as redes sociais (CETIC.br, 2023, p. 29). E, sobre as orientações recebidas para o uso da Internet, 89% dos pais ou responsáveis explicam que alguns sites são bons e outros são ruins e, ainda, ensinam como se comportar na Internet com outras pessoas, 83% ensinam sobre como usar a Internet com segurança, 82% explicam o que fazer se alguma coisa na Internet o(a) incomodar ou chatear; 74% ajudam quando alguma coisa na Internet o(a) incomodou ou chateou e 64% ajudam a fazer alguma coisa na Internet que não entende.

Novamente, todas essas informações parecem não ser suficientes para impedir que em 2022, a Central de Denúncias de Crimes Cibernéticos, recebesse e processasse 111.929 denúncias anônimas de pornografia infantil envolvendo 40.572 páginas



(URLs) distintas, sendo que 18.218 foram removidas, representando 44,90% do total de páginas. Todas essas URLs estavam hospedadas em 3.160 domínios diferentes, de 142 diferentes TLDs (*Top-Level Domain* ou Domínio de Nível Superior, por exemplo, .com) e conectados à Internet por meio de 4.256 IPs distintos, atribuídos para 58 países em 6 continentes (SAFERNET, 2023).

Com base nesse panorama, que por momentos aponta para uma realidade que privilegia a proteção de dados e a cibersegurança de crianças e adolescentes e por outro lado aponta para um ambiente vulnerável e inseguro, necessita-se entender as preocupações sob o olhar da proteção de dados pessoais de crianças e adolescentes para que o ciberespaço de cidades inteligentes proporcione que elas se relacionem, estudem e cresçam saudáveis e ciberneticamente seguras.

3. O CIBERESPAÇO NAS SMART CITIES SOB A PERSPECTIVA DA PROTEÇÃO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Stoeberl *et al.* (2023) mostram que historicamente quando do surgimento das cidades modernas e, ao menos até 1989 – com o advento da Convenção sobre os Direitos da Criança (ONU, 1989) – as crianças não eram consideradas sujeitos de direitos, motivo pelo qual não eram titulares de direitos próprios, sequer tinham direito de manifestar a sua opinião e de frequentar livremente o espaço público. As crianças eram tratadas como um objeto e sua vida era regida pelas regras do ambiente privado. Eis que a atualidade demonstra que as crianças e adolescentes são considerados pessoas titulares dos mesmos direitos que os adultos. E para que os 04 (quatro) grupos de direitos da criança e do adolescente: à vida, ao desenvolvimento, à proteção e à participação; possam ser efetivados de um modo integral, o estudo refere-se especificamente às cidades inteligentes, *smart cities*.

O estudo ora realizado tem por embasamento um contexto jurídico-tecnológico-social de modo a contribuir na proteção de direitos fundamentais de liberdade e de privacidade e, por conseguinte, o livre desenvolvimento da personalidade da pessoa natural de crianças e adolescentes, conforme art. 1º da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018). Desse modo, estando as crianças e os adolescentes inseridos nas cidades inteligentes, há-se que considerar o ciberespaço nesse novo modelo de cidades, visto que do ponto de vista tecnológico,



o ciberespaço é “constituído por comunicações eletrônicas de dados em um de três estados possíveis (ou por transmitir, ou em transmissão, ou já transmitidos) que fluem entre, e estão alicerçados em três camadas distintas (a física, a lógica e a cognitiva)” (BRAVO, 2021, p. 19). E dados fluem e, considerando o panorama de uso da Internet por usuários de 9 a 17 anos de idade, como mostrado anteriormente, tem-se que essa fluidez é ainda mais ubíqua e pervasiva.

Legalmente, o ciberespaço pode ser assim compreendido: “Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação”, a partir da definição encontrada na Estratégia Nacional de Segurança do Ciberespaço 2019-2023, Resolução do Conselho de Ministros nº 92/19 (PORTUGAL, 2019). No Brasil, a Estratégia Nacional de Segurança Cibernética (E-Ciber), Decreto nº 10.222/2020 (BRASIL, 2020), não apresenta definições, mas aplica o termo espaço cibernético.

Diante de um espaço que é complexo e demanda atenção, bem como responsabilidade, seja de quem mantém a infraestrutura de rede e sistemas de informação, estabelecendo o uso das TICs, ou de quem faz uso desse espaço, há que se considerar como ponto relevante o tratamento de dados pessoais. E quando o tema é tratamento de dados pessoais, precisam ser agregadas variáveis referentes tanto às necessidades das cidades inteligentes quanto das crianças e adolescentes.

A LGPD, como é conhecida a Lei Geral de Proteção de Dados Pessoais, Lei No. 13.709 de 14 de agosto de 2018 (BRASIL, 2018), estabelece os fundamentos e princípios jurídicos que norteiam o referido texto legislativo, podendo-se mencionar o consentimento (BIONI, 2019), o legítimo interesse, os direitos dos titulares de dados, a criação da Autoridade Nacional de Proteção de Dados (ANPD), a responsabilização e o ressarcimento por danos causados a outrem por meio do tratamento de dados, as sanções administrativas e diversos outros aspectos.

Sem esquecer de outras normas já existentes no ordenamento jurídico brasileiro, a exemplo da Lei de Acesso à Informação (Lei No. 12.527/2011), Marco Civil da Internet (Lei No. 12.965/2014), Código de Defesa do Consumidor (Lei No. 8.078/1990) e da própria Constituição Federal de 1988, a LGPD vem se configurando como um marco voltado à privacidade e proteção de dados pessoais. O Brasil entrou no cenário mundial da proteção de dados pessoais, trazendo uma proteção especial aos dados pessoais de crianças e adolescentes. Se colocar um freio na coleta de dados pessoais sem finalidade específica para adultos já era



mais do que necessário, em relação às crianças e adolescentes é mandatório. Há que se fomentar a criação de uma cultura da minimização de dados e de operações de tratamento que protejam os dados, como objeto originário, mas, também como elementos de perpetuação da vida digital na infosfera – *onlife* (FLORIDI, 2014, p. 40-41).

Cabe lembrar que a unidade básica de proteção pela LGPD são os dados e sobre eles recaem todas as preocupações e modificações que precisam ser desenvolvidas e implantadas seja nos sistemas, nos sistemas de informação e na organização como um todo, incluindo as pessoas. Eis aqui o repensar do ciberespaço. E quando o ciberespaço envolve de um lado cidades inteligentes e de outro crianças e adolescentes, há que se observar atentamente a LGPD, art. 5º, inciso X (BRASIL, 2018), inicialmente, na definição de tratamento de dados:

art 5º X - “tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

As operações encontram-se listadas de modo exemplificativo e não restritivo. Essas operações não compreendem o conjunto completo de possibilidades de tratamento de dados pessoais ou sensíveis. Deve-se ter em mente que o texto legislativo não se prende às técnicas ou aos métodos computacionais ou operacionais, uma vez que a partir de determinadas operações exemplificadas no art. 5º, inciso X, pode-se realizar desde a captura do dado até a aplicação de técnicas de Mineração de Dados (*Data Mining*) ou Aprendizagem de Máquina (*Machine Learning*).

A LGPD dedica a Seção III do Capítulo II ao tratamento de dados pessoais de crianças e adolescentes, estabelecendo no artigo 14 que “O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente” (BRASIL, 2018). Nesse mesmo artigo, observa-se a relação entre a LGPD e o Marco Civil da Internet, no que tange ao controle parental, visto que “O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal”, sendo que somente poderão ser coletados dados pessoais de crianças sem o consentimento “quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem



o consentimento de que trata o § 1º deste artigo”. Ressalta-se que as informações sobre o tratamento de dados “deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança” (BRASIL, 2018).

Aos controladores caberá "manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei” (BRASIL, 2018). Além disso, os controladores “não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade”, o que pode ser de difícil controle por parte dos pais ou responsável legal. E, ainda, caberá ao controlador “realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis” (BRASIL, 2018).

A Seção III do Capítulo II da LGPD é sucinta, despertando preocupações no sentido de controles não somente jurídicos, mas tecnológicos, visto que a relação entre crianças e adolescentes com o ciberespaço em cidades inteligentes pode se iniciar a partir da coleta de dados pessoais, não somente para uso de jogos e entretenimento, entretanto considerando todas as categorias de aplicações de Internet para acesso aos transportes públicos, equipamentos urbanos (centros comunitários, bibliotecas, piscinas públicas, cinemas, playgrounds, entre outros). Há ainda que se considerar as necessidades de segurança pública, visto que crianças e adolescentes precisam circular em espaços físicos e cibernéticos seguros. As cidades inteligentes não podem ser inteligentes somente para adultos, precisam ser inteligentes para crianças e adolescentes e, portanto, o *smart* precisa se conectar ao cibernético.

4. ELEMENTOS JURÍDICO-TECNOLÓGICOS VOLTADOS À PROTEÇÃO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES EM CIDADES INTELIGENTES



Um estudo exploratório buscando relacionar os temas “crianças e adolescentes”, “cidades inteligentes” e “proteção de dados pessoais”, sem tentativa de esgotar os temas e o estudo, demonstra que o tema ainda é incipiente e demanda estudos aprofundados e discussões, seja no plano urbanístico, no plano jurídico ou no plano tecnológico. Reunir esses temas em um único trabalho é inovador e permite apontar elementos jurídico-tecnológicos para auxiliar na garantia de direitos de crianças e adolescentes, especificamente ao que trata da proteção de dados pessoais, considerando o ciberespaço de cidades inteligentes como base de um ecossistema de sustentação tanto tecnológica quanto jurídica.

Para tal, há que se sumarizar as características de uma cidade inteligente, a saber: capital humano, aspectos econômicos, governança, mobilidade, recursos naturais e qualidade de vida (HENNIG, 2017, p. 553). Aparentemente são características que existem em qualquer cidade, não necessariamente em uma cidade inteligente.

As cidades inteligentes pensadas para crianças e adolescentes precisam respeitar os Direitos das Crianças estabelecidos pela ONU (1989), de modo a ter por base o conceito de cidade amiga da criança e do adolescente e garantir que esses cidadãos e cidadãs possam: (i) influenciar as decisões sobre a sua cidade, (ii) expressar a sua opinião sobre a cidade que desejam, (iii) participar da vida familiar, comunitária e social, (iv) ser um cidadão igualitário de sua cidade com acesso a todos os serviços, independentemente de origem étnica, religião, renda, gênero ou deficiência, (v) receber serviços básicos, a exemplo de: cuidados de saúde, educação e abrigo, (vi) beber água potável e ter acesso a saneamento adequado, (vii) ser protegido da exploração, violência e abuso, (viii) andar com segurança nas ruas por conta própria, (ix) encontrar amigos e brincar, (x) ter espaços verdes para plantas e animais, (xi) viver em um ambiente não poluído, e (xii) participar de eventos culturais e sociais.

As cidades inteligentes agregam duas características importantes, a saber: (i) a formação de ciberespaço e (ii) o uso intensivo de TICs. Sobre a formação do ciberespaço há que se ponderar a partir das definições jurídica e tecnológica de ciberespaço, com base em Bravo (2021), apresentadas anteriormente, que esse “novo” espaço estabelece não somente o uso de tecnologias computacionais móveis e pervasivas, mas ubíquas, ampliado o que se entende no sistema urbanístico como equipamentos e infraestrutura voltados especificamente a formação de um ecossistema que reúne e proporciona serviços de administração, educação, saúde,



segurança pública, transporte, serviços públicos, entre outros. Tudo isto de nodo conectado e por meio de aparatos móveis, especialmente os *smartphones*.

No que se refere ao uso intensivo das TICs, há que se compreender que a informação e a comunicação estarão tão interligadas que os serviços digitais não mais serão percebidos como algo distante ou estranho, sendo a computação pervasiva o motor das cidades inteligentes. Desde o planejamento de serviços públicos inteligentes até a coleta e tratamento de dados pessoais precisarão ser revisitados e apresentados de uma maneira que considere os conceitos do *Privacy by Design* (CAVOUKIAN, 2009). Especial atenção deve ser dada à coleta e tratamento de dados de geolocalização, geovisualização e geocomunicação (HENNIG, 2017, p. 559). Há ainda que se considerar os dados relativos ao uso das TICs, conforme apresentado no item 2 desse trabalho, visto que a relação das crianças e adolescentes com as TICs se demonstra intensa porém a forma de uso e os requisitos a serem levados em consideração no desenvolvimento de aplicações deverão ter por premissa que esses usuários são distintos de adultos e não se relacionam com as TICs da mesma maneira. As crianças e adolescentes de hoje e do futuro serão cada vez mais os nativos digitais (PRENSKY, 2001).

Ghafoor-Zadeh (2023, p. 02-03) apresenta algumas preocupações relevantes sobre a interação de crianças e adolescentes com as cidades inteligentes, afirmando que é necessário dar atenção às diferentes geografias cotidianas das crianças e dos adolescentes para, então, melhorar compreender as múltiplas formas com que eles se conectam e se relacionam com espaços sócio-materiais-tecnológicos frente ao uso crescente das TICs, visto que as dimensões *online* e *offline* do espaço físico e digital se fundem cada vez mais. As cidades inteligentes são permeadas por dispositivos e aplicativos digitais e, ainda, por uma grande variedade de jogos e serviços *online* que cada vez mais incentivam que as crianças e os adolescentes se envolvam com a cidade em que vivem, de modo a possibilitar maior mobilidade e novas experiências nos espaços físico e digital urbano. As crianças e adolescentes, com seus celulares e *smartphones*, deixam de ser observadores passivos para atuarem ativamente com suas câmeras digitais, podendo até mesmo denunciar problemas (ambientais, da comunidade, da escola, entre outros) ou influenciar políticas públicas.

Clarival et al. (2023, p. 02) apontam que é necessário trabalhar a alfabetização digital (*digital literacy*) de crianças e adolescentes em cidades inteligentes, seja para apoiar as atividades em sala de aula ou para melhorar as habilidades digitais propriamente ditas. Os



autores alertam para a formação de cidadãos digitais, preparados para atuar em processos de participação visando a tomada de decisão, incluindo-se a procedimentos cooperativos, colaborativos ou por votação; todos apoiados pelas TICs (*e-voting*).

É evidente que todos esses aspectos precisam ser ponderados, considerando-se que nem todos, crianças e adolescentes de cidades inteligentes, e nem de maneira igualmente acessível e inclusiva terão as mesmas condições e qualidade de vida seja física ou digital. Há que se mencionar que o artigo 54 da Convenção das Nações Unidas sobre os Direitos da Criança (ONU, 1989) explicita direitos sustentados pelos “Ps” de direitos de proteção, provisão e participação. E, no “P” da proteção, há que se incluir a proteção de dados pessoais de crianças e adolescentes. Assim, cada vez mais, nas cidades inteligentes, os usuários serão “convidados” a produzir e compartilhar conteúdo digital, incluindo-se dados pessoais e dados pessoais sensíveis, por exemplo, biométricos, por meio de selfies. Graaf (2020, p. 3-4) alerta para os efeitos da plataformização (*platformization*), por meio do qual as plataformas ofertam serviços e facilidades em troca de volumes de dados que são coletados de maneira sutil, tornando-se o modelo organizacional *online* dominante, de modo que as *Big Techs* desenvolvem seu papel de mercado e apresentam serviços aos seus stakeholders, incluindo as cidades, por exemplo, o aplicativo de navegação social do Google Waze. Esse modelo estabelece um forte *ethos* neoliberal, por meio de uma contínua “corporatização dos serviços da cidade” sustentando todos os tipos de apropriações de (meta)dados, indo muito além do que o usuário conscientemente fornece às plataformas.

Graaf (2020, p. 4-5) vai além e adentra o que denomina de datificação (*datafication*), esclarecendo que as TICs “geram, processam e extraem valor sustentado por fluxos de dados amplamente granulares e indexados” pelos mais variados interesses. A isso se compreende como datificação, propriedade que é fortemente associada à estrutura de *Smart Cities* devido à estudos e análise de correlações a partir de bases de dados de volume inimagináveis, a exemplo de *Big Data*, permitindo a caracterização de perfil seja comportamental, de participações e predisposições para, por exemplo, efetuar uma compra *online* ou consultar um trajeto entre casa e escola. A autora, explica que tais práticas suscitam questões éticas, de privacidade, de proteção de dados pessoais, de vigilância e controle, bem como de *profiling* (BOFF; FORTES; FREITAS, 2018, p. 161-171), incluindo-se a categorização social (*social score*), a aplicação de *nudges* (FREITAS; ALMADA, 2019), entre outros problemas como a governança antecipada



por meio da qual o Estado usa dados públicos (ou que se entendem como públicos a partir das coletadas realizadas pelas plataformas) de seus cidadãos para estabelecer métodos e técnicas preditivas e obter conclusões com base nesses dados (OCDE, 2022). Todos esses aspectos permeiam o ciberespaço e quando o tema envolve crianças e adolescentes esses aspectos estão revestidos de uma maior preocupação e precisam, portanto, de uma proteção ainda mais eficiente.

Graaf (2020, p. 4) pondera sobre os riscos de transformar as pessoas em conjunto de dados, sendo tais riscos amplificados para as crianças e adolescentes, visto que também são consumidores de produtos e serviços na Internet e, portanto, produzem dados digitais. Aqui cabem ressalvas sobre a participação das crianças e adolescentes na construção da cidade inteligente que os/as beneficie e sobre a forma de governança sem que se tenha excessos de controle e vigilância. Graaf (2020, p. 4, 10) menciona a existência “*government of childhood*”, “*datafied environment*” e o que a datificação e vigilância das crianças e adolescentes “pode falar em nome deles/delas”. Entende-se dessa maneira, que há o risco de se configurar um ciberespaço não seguro e responsável. Há que se evitar não somente a exclusão digital, mas a social e espacial das crianças e adolescentes em espaços urbanos digitais.

Todo esse cenário, culmina com os estudos de Shoshana Zuboff (2021) sobre o que ela nomeia como capitalismo de vigilância, tendo como base uma arquitetura global de modificação comportamental que altera e desfigura o mundo físico, visto que a nova configuração global tem por fundamento uma estruturação digital por meio dos dados que os usuários “deixam” na Internet e são tratados sem o devido consentimento. A autora exemplifica e discute fortemente o tratamento de dados frente a ausência ou fraco regramento de proteção de dados pessoais e ao desconhecimento tanto da coleta e tratamento de dados quanto dos reflexos na ordem social e futuro digital da sociedade contemporânea. Isso é uma preocupação real quando se pensa em crianças e adolescentes vivendo em cidades inteligentes.

Há que se atentar para a coleta e tratamento de dados e exploração de rastros digitais de crianças e adolescentes, a constante expansão de processos automatizados e plataformas de suporte existentes em cidades inteligentes para as mais diversas atividades, a delegação da tomada de decisão e governança por meio de algoritmos voltados à infraestrutura urbana, as implicações de um ecossistema complexo baseado em *multistakeholders*, o que pode reforçar as desigualdades sociais, ambientais, jurídicas e tecnológicas (GRAAF, 2020, p. 2).



E a existência dos rastros digitais está diretamente ligada a existência de identificadores únicos nos dispositivos digitais. Assim os dados (pessoais, de localização, de consulta, de navegação, entre outros) pelos usuários não são tão anônimos quanto se acredita, sendo que o rastreamento da atividade *online* é extenso, abrangente e persistente, gerando sombras de dados utilizáveis (e, por vezes, comercializáveis) que não precisam de coleta efetiva de dados pessoais para atingir cada usuário, consumidor, seja criança/adolescente ou adulto. Essa rastreabilidade existe tanto em espaços privados quanto em espaços públicos, e há que se ter em mente que cidades inteligentes criam espaços públicos digitais, estabelecendo o ciberespaço propriamente dito daquela cidade.

Considerando-se o exposto, a Tabela 02 apresenta como contribuição um conjunto de elementos jurídico-tecnológicos para auxiliar na garantia de direitos e na proteção de dados pessoais, considerando o ciberespaço de cidades inteligentes como base de um ecossistema de sustentação tanto jurídica quanto tecnológica. O cenário não é simples e muito menos trivial. Resta evidente que a construção de cidades inteligentes que tenham crianças e adolescentes como efetivos cidadãos elaborem projetos que visem à autoproteção no ciberespaço.

Tabela 02: Elementos Jurídico-Tecnológicos para Proteção de Dados Pessoais de Crianças e Adolescentes no Ciberespaço de *Smart Cities*

Elementos do Ciberespaço	Estados Possíveis dos Dados		
	Por transmitir	Em transmissão	Já transmitido
Crianças e Adolescentes	CF/88, LGPD, CDC, ECA, MCI		
Redes	Protocolos, Segurança da Informação, Normas ISO 27000		
Sistemas de informação	Segurança da Informação, Normas ISO 27000, <i>Privacy by Design/Default</i>		

A possibilidade do exercício de autoproteção associado à informação e conhecimento dos riscos a que se submetem quando “navegam” na Internet, ou simplesmente fazem uso dos smartphones, representa uma importante estratégia voltada à proteção integral de crianças e adolescentes. Estratégias autoprotetivas possibilitam o entendimento do risco por meio de visualização e alertas sobre potenciais violações de direitos. Neste caso é fundamental atentar para o desenvolvimento de sistemas baseados em privacidade desde a concepção, artigo 46 da LGPD (BRASIL, 2018), ou ainda, *privacy by design/default* (FREITAS et al., 2021).



Necessário também utilizar linguagem e representação gráfica voltada à faixa etária da criança/adolescente, de modo a engajar cada vez mais o uso de tal ferramental. Não se pode deixar de lado o ferramental tecnológico da família de normas ISO 27000, que tem por base as propriedades básicas da Segurança da Informação, evidenciando os aspectos tecnológicos da proteção de dados pessoais (FREITAS; SANTOS; PASINATO, 2020).

No que se refere aos elementos jurídicos, não há que se atentar somente ao ordenamento jurídico brasileiro, mas aos sistemas de garantia de direitos de crianças e adolescentes em nível mundial, visto que é necessário privilegiar a construção coletiva dos fluxos de dados, entre setores privados e públicos, que atuam nas cidades inteligentes. Um projeto de cidade inteligente deve contribuir para o aprimoramento da atuação coletiva, preventiva e autoprotetiva diante dos procedimentos de defesa dos direitos humanos de crianças e adolescentes. Finalmente, há que se pensar a responsabilização, seja de entes públicos ou privados, e para tal há que se estabelecer uma metodologia de produção de provas que garanta prioridade à proteção de crianças e adolescente.

5. CONCLUSÃO

O estudo partiu do problema de pesquisa caracterizado no seguinte questionamento: Como pensar o ciberespaço de cidades inteligentes para crianças e adolescentes levando em consideração a proteção de dados pessoais? Assim, o objetivo geral do artigo foi apresentar elementos jurídico-tecnológicos a serem observados em cidades inteligentes sob a perspectiva da garantia de direitos das crianças e adolescentes.

Para tanto, iniciou-se descrevendo a relação das crianças e dos adolescentes com as Tecnologias de Informação e Comunicação (TICs), visto que o meio ambiente digital é o cenário principal das cidades inteligentes. Pode-se concluir que a relação entre crianças/adolescentes e as TICs ora aponta para uma realidade que privilegia a proteção de dados e a cibersegurança ora aponta para um ambiente vulnerável e inseguro, necessita-se entender as preocupações sob o olhar da proteção de dados pessoais para que o ciberespaço de cidades inteligentes proporcione que as crianças e os adolescentes se relacionem, estudem e cresçam saudáveis e ciberneticamente seguras.

Na sequência, adentrou-se ao estudo da proteção de dados pessoais de crianças e adolescentes no ciberespaço de cidades inteligentes, de modo a refletir sobre a LGPD.



Concluiu-se que a Seção III do Capítulo II da LGPD é sucinta, despertando preocupações no sentido de controles não somente jurídicos, mas tecnológicos, visto que a relação entre crianças e adolescentes com o ciberespaço em cidades inteligentes pode se iniciar a partir da coleta de dados pessoais. Há ainda que se considerar as necessidades de segurança pública, visto que crianças e adolescentes precisam circular em espaços físicos e cibernéticos seguros. As cidades inteligentes não podem ser inteligentes somente para adultos, precisam ser inteligentes para crianças e adolescentes e, portanto, o *smart* precisa se conectar ao cibernético.

E, finalmente, foram apresentados elementos jurídico-tecnológicos para auxiliar na garantia de direitos, na proteção de dados pessoais, considerando o ciberespaço de cidades inteligentes como base de um ecossistema de sustentação tanto tecnológica quanto jurídica. Esses elementos têm por base as pessoas (crianças e adolescentes), as redes e os sistemas de informação, diante do fluxo de dados e considerando-se os estados possíveis dos dados: por transmitir, em transmissão e já transmitido. Concluiu-se que o arcabouço jurídico brasileiro se entrelaça com aspectos tecnológicos advindos da Segurança da Informação, das normas ISO 27000 e da *Privacy by Design/Default* sob uma estratégia coletiva, preventiva e autoprotetiva para crianças e adolescentes, perfazendo um ciclo entre o Direito, as novas tecnologias e a governança em cidades inteligentes.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. Proteção de Dados e Privacidade: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. Decreto nº 10.222, de 05 de fevereiro de 2020, Estratégia Nacional de Segurança Cibernética, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm Acesso em: 26 jun. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 26 jun. 2023.

BRAVO, Rogerio. Segurança da Informação, Cibersegurança e Cibercrime: contributos para um alinhamento de conceitos. v.12. Lisboa, 2021. p. 19. Disponível em:



https://www.academia.edu/40494857/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o_e_ciberseguran%C3%A7a_aspetos_pr%C3%A1ticos_e_legisla%C3%A7%C3%A3o Acesso em: 26 jun. 2023.

CAVOUKIAN, Ann. Privacy by design: The 7 foundational principles: implementation and mapping of fair information practices. Information and privacy commissioner of Ontario, Canada, 2009. Disponível em: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf> Acesso em: 26 jun. 2023.

CETIC.br. Tic kids online brasil 2022: principais resultados. 2023. Disponível em: https://cetic.br/media/analises/tic_kids_online_brasil_2022_principais_resultados.pdf Acesso em: 26 jun. 2023.

CLARINVAL, Antoine; SIMONOFSKI, Anthony; HENRY, Julie; VANDERROSE, Benoît; DUMAS, Bruno. Introducing the Smart City to Children: Lessons Learned from Hands-On Workshops in Classes. Sustainability, Vol. 15, 1774, 2023. Disponível em: <https://www.mdpi.com/2071-1050/15/3/1774> Acesso em: 26 jun. 2023.

FLORIDI, Luciano. The 4th Revolution: How the Infosphere is Reshaping Human Reality. New York: Oxford University Press, 2014.

FREITAS, Cinthia Obladen de Almendra; SERRATO, Ana Paula; TORRES, Bruno Max Müller; SACOMAN, Cleiton; FERREIRA, Dâmares. A Abordagem Privacy by Design/Default no Desenvolvimento de Software e a Lei Geral de Proteção de Dados Pessoais. In: Rhodrigo Deda Gomes. (Org.). Direito e Inovação - Volume 5. 1ed. Curitiba: OABPR, 2021, v. 5, p. 201-237.

FREITAS, Cinthia Obladen de Almendra; SANTOS, Henrique Guilherme; PASINATO, Rita. A Segurança da Informação como Ferramental Técnico da Proteção de Dados Pessoais. In: Mariana Pereira Faria; Rafael Aggens Ferreira da Silva; Rhodrigo Deda Gomes. (Org.). Direito e Inovação - Volume 3. 1ed. Curitiba: NCA - Comunicação e Editora LTDA, 2020, v. 3, p. 233-265.

FREITAS, Cinthia Obladen de Almendra; ALMADA, Giovanna Michelato. How Can Nudging Solve Some of the Internet Data Privacy Issues. Revista Direito e Desenvolvimento, v. 10, 6-19, 2019.

FREITAS, Cinthia Obladen de Almendra; BARBOSA, Claudia Maria; SANTIN, Altair Olivo. Aliciamento Sexual de Crianças e Adolescentes na Internet sob a Perspectiva da Teoria da Comunicação Ludibriante. Revista Magister de Direito Penal e Processual Penal, v. 70, p. 13-32, 2016.

GRAAF, Shenja van der. The Right to the City in the Platform Age: ChildFriendly City and Smart City Premises in Contention. Information, Special Issue – The Future of Human Digitization, Vol. 11, 285, 2020. Disponível em: <https://www.mdpi.com/2078-2489/11/6/285> Acesso em: 26 jun. 2023.



OCDE. Foresight and Anticipatory Governance in Practice: Lessons in effective foresight institutionalisation. Strategic Foresight Unit, Office of the Secretary-General OCDE, 2022.

ONU. Convenção sobre os Direitos da Criança, 1989.

PARISER, Eli. O filtro invisível: O que a Internet está escondendo de você. 1. ed. Rio de Janeiro: Zahar, 2012.

PORTUGAL. Estratégia Nacional de Segurança do Ciberespaço 2019-2023, Resolução do Conselho de Ministros (RCM) n.º 92/2019, 2019. Disponível em: <https://dre.pt/dre/detalhe/resolucao-conselho-ministros/92-2019-122498962> Acesso em: 26 jun. 2023.

PRENSKY, Marc. Digital Natives, Digital Immigrants. On the Horizon, MCB University Press, Vol. 9, No. 5, October, 2001.

SAFERNET. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. 2023. Disponível em: <https://indicadores.safernet.org.br/index.html> Acesso em: 26 jun. 2023.

STOEBERL, Cristiane Aparecida; FREITAS, Cinthia Obladen de Almendra; PAMPLONA, Danielle Anne. Smart Cities sob a Perspectiva dos Direitos da Criança: um olhar na cibersegurança e proteção de dados pessoais. Revista Direito da Cidade (no prelo).

UOL. Discord: PF identifica 10 vítimas de tortura; app remove conteúdo negativo, 26 de junho 2023. Disponível em: <https://www.bol.uol.com.br/noticias/2023/06/26/discord-pf-identifica-10-vitimas-de-tortura-app-remover-conteudonegativo.htm> Acesso em: 26 jun. 2023.

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância. Trad. George Schlesinger. Rio de Janeiro: Editora Intrínseca Ltda., 2021.