XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

INTERNET: DINÂMICAS DA SEGURANÇA PUBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

MAIQUEL ÂNGELO DEZORDI WERMUTH

I61

Internet: dinâmicas da segurança pública e internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Maiquel Ângelo Dezordi Wermuth.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-609-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 2. Dinâmicas da segurança pública e internacional. XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

INTERNET: DINÂMICAS DA SEGURANÇA PUBLICA E INTERNACIONAL

Apresentação

Apresentação

É com imensa satisfação que apresentamos a obra que reúne os artigos apresentados no Grupo de Trabalho "INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL I", durante o XXIX Encontro Nacional do CONPEDI, no dia 9 de dezembro de 2022, no Campus de Balneário Camboriú da UNIVALI.

O artigo de Danielle Jacon Ayres Pinto e Rafael Gonçalves Mota, intitulado "A GUERRA CIBERNÉTICA COMO A QUINTA DIMENSÃO DA GUERRA MODERNA E O SEU ENFRENTAMENTO CONSTITUCIONAL NO BRASIL" analisa a relação entre a evolução tecnológica, especialmente a importância que a rede mundial de computadores passou a ter na vida cotidiana dos indivíduos, instituições e estados e os conflitos bélicos, notadamente considerando que a guerra através de meios virtuais e cibernéticos passou a ser a quinta dimensão possível de desenvolvimento bélico, seguindo o mar, terra, ar e espaço.

Ezequiel De Sousa Sanches Oliveira e Greice Patricia Fuller, no artigo "A GUERRA CIBERNÉTICA NO CONTEXTO DAS CIDADES INTELIGENTES NO MUNDO PÓS-PANDÊMICO: PROVOCAÇÃO ANALÍTICA SOB O VIÉS DA CIBERSEGURANÇA /HACKING", abordam o uso da internet no contexto das "Smart Cities", salientando que a rede mundial de computadores é tomada como tecnologia da informação e comunicação, por impactar as ações humanas, razão pela qual deve passar por uma reflexão sob o viés da defesa cibernética no que toca à segurança da informação, notadamente no cenário descortinado pelo mundo pós-pandêmico, marcado pela profusão da cibercultura e da disseminação do universo hacker.

O artigo intitulado "A VIRADA TECNOLÓGICA E O PRINCÍPIO DA NECESSIDADE EM DAVID SCHMIDTZ: A QUESTÃO DA SEGURANÇA PÚBLICA NA ERA DO COVID19", de autoria de Feliciano Alcides Dias, Fabiel dos Santos Espíndola e Ubirajara Martins Flores, a partir da teoria pluralista da justiça de David Schmidtz, destaca que a transição da modernidade para a hipermodernidade é marcada por um descompasso imposto pela rapidez da evolução das ferramentas de tecnologia da informação e da comunicação e pelo desenvolvimento dessas atividades na Segurança Pública. Nesse sentido, a alternativa

encontrada na teoria de David Schmidtz propõe o respeito à individualidade das pessoas que, na sua concepção, significa justiça.

Em “ASPECTOS DIFERENCIADORES EM CURSOS DE FORMAÇÃO BÁSICA POLICIAL MILITAR”, Anderson Morais De Oliveira tematiza a formação policial no Brasil, apontando para a existência dos chamados currículos “ocultos” na formação de soldados da Polícia Militar. O estudo destaca as condições que fomentam o ingresso na carreira policial, alguns aspectos da cultura corporativa interna, bem como o aspecto influenciador nas relações de poder da atividade policial.

O artigo de Maiquel Ângelo Dezordi Wermuth e Fernando Antonio Sodre De Oliveira, sob o título “DA BIOPOLÍTICA DE MICHEL FOUCAULT À NECROPOLÍTICA DE ACHILLE MBEMBE: A FUNÇÃO DO RACISMO NA DIMENSÃO ESTRUTURANTE DA SEGURANÇA PÚBLICA NO BRASIL”, explora a possível conexão entre os conceitos de biopolítica (desenvolvido no percurso filosófico de Michel Foucault) e de necropolítica (que ocupa lugar de centralidade na filosofia de Achille Mbembe), perquirindo qual é a função que o racismo desempenha tanto no exercício do biopoder quanto do necropoder. Além disso, o texto busca-se analisar de que forma o racismo estrutura os Estados a partir da Modernidade, notadamente no que se refere à sua atuação no campo da segurança pública, ainda profundamente marcado pela seletividade étnico-racial.

No artigo “DESAFIOS À LEI GERAL DE PROTEÇÃO DE DADOS NA ERA DA INTELIGÊNCIA ARTIFICIAL: ENTRE O DIREITO À PRIVACIDADE E AS ROBOCALLS”, Matheus Adriano Paulo e Gilson Jacobsen analisam a oferta de produtos e serviços por meio de “Robocalls”, que são uma espécie de Inteligência Artificial desenvolvida para fazer ligações, emulando a ação humana e desafiando a melhor aplicação possível da Lei Geral de Proteção de Dados - LGPD, que pode e deve servir de freio a eventuais violações ao direito de privacidade dos cidadãos.

Em “DIREITO AO ESQUECIMENTO COMO FERRAMENTA TRANSNACIONAL PARA O ARMAZENAMENTO DE DADOS MAIS SUSTENTÁVEL”, Jaine Cristina Suzin, Jardel Anibal Casanova Daneli e Paulo Márcio da Cruz abordam a insustentabilidade do Armazenamento de Dados na Internet perante as dimensões ambiental, social e econômica, em um cenário que pode ser denominado de sociedade da informação transnacional. Nesse contexto, estudam a viabilidade do Direito ao Esquecimento enquanto ferramenta transnacional para a emergência da Sustentabilidade.

O artigo intitulado “ERA DA IA E O 5G: QUAL A VELOCIDADE DA (DES) INFORMAÇÃO?”, de Patrícia da Silva Almêda Sales e Debora Bonat, analisa a relação circunscrita entre a Inteligência Artificial (IA) e o Direito, especialmente no que diz respeito à desinformação na participação democrática com a expansão do 5G, enfocando as possíveis implicações na próxima fase de comunicação e compartilhamento de informações na 5ª geração de banda larga móvel, a exemplo da repressão digital, da vigilância em massa, do perfil de usuário aprimorado e microsegmentação etc.

No texto “FAKE NEWS E O PROCESSO ELEITORAL, A BUSCA PELO ENFRENTAMENTO E DIMINUIÇÃO DO FENÔMENO”, Rennan Gonçalves Silva, Lucas Gonçalves da Silva e Karla Thais Nascimento Santana discutem os impactos das fake news no processo eleitoral e analisam as medidas de enfrentamento a essas notícias durante o período eleitoral.

“O DILEMA DO SUJEITO MONITORADO NO PÓS-MUROS DO SISTEMA PRISIONAL” é o título do artigo e Joice Graciele Nielsson e Adriane Arriens Fraga Bitencourt, que analisa a posição do sujeito em monitoração eletrônica no sistema penal, ressaltando a necessidade de implementação de políticas públicas de apoio a esses sujeitos, com o efetivo acompanhamento de equipe multidisciplinar como condição mínima para a garantia da maior efetividade do sistema de liberdade monitorada.

Em “O DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS PESSOAIS NA SEGURANÇA PÚBLICA E ÂMBITO PENAL: POSSIBILIDADES E DESAFIOS”, Joice Graciele Nielsson e Milena Cereser da Rosa abordam a proteção de dados pessoais enquanto direito fundamental e os desafios e possibilidades para a construção de uma Lei Geral de Proteção de Dados (LGPD) no âmbito da segurança pública e penal, como forma de garantir o direito fundamental a proteção de dados pessoais, diante da necessidade de equilibrar a privacidade e a efetividade da jurisdição penal, de modo a não prejudicar tanto o sistema jurisdicional quanto o titular do direito à proteção dos dados.

Mariana Chini e Maiquel Ângelo Dezordi Wermuth, no artigo “O “FUTURO” SOBRE CORPOS PENALIZADOS: TECONOLOGIA, SISTEMA PENAL E MONITORAÇÃO ELETRÔNICA DE PESSOAS” abordam os avanços da tecnologia no sistema penal, tendo por escopo central a monitoração eletrônica de pessoas, especialmente no contexto brasileiro, perspectivada a partir da estigmatização de pessoas eletronicamente monitoradas na esfera penal.

“RECONHECIMENTO FACIAL E (IN)SEGURANÇA PÚBLICA: VIOLAÇÃO A DIREITOS DA PERSONALIDADE IMPULSIONADA PELO EXCESSO DE VIGILÂNCIA” é o título do texto de Micaela Mayara Ribeiro, Vinícius Fachin e Zulmar Antonio Fachin, que analisa o uso da tecnologia de reconhecimento facial na segurança pública, aferindo os impactos que o excesso de vigilância pode ocasionar nos direitos da personalidade dos cidadãos

Por fim, Maite Neves Guerra e Thiago Santos Aguiar de Pádua, no artigo intitulado “VALIDADE JURÍDICA DO PRINT SCREEN DE WHATSAPP COMO PROVA NO PROCESSO PENAL”, discutem a necessidade de validação e autenticação de provas digitais, em especial as conversas do aplicativo WhatsApp, sugerindo o auxílio das novas tecnologias.

O(a) leitor(a), por certo, perceberá que os textos aqui reunidos, além de ecléticos, são críticos quanto à realidade a utilização das novas tecnologias na contemporaneidade – notadamente no campo da segurança pública e da segurança internacional–, o que reflete o compromisso dos(as) autores(as) na busca pela adequação do uso dessas tecnologias aos textos convencionais e constitucionais centrados na dignidade da pessoa humana.

Tenham todos(as) uma ótima leitura! É o que desejam os organizadores.

Danielle Jacon Ayres Pinto – UFSC

Maiquel Ângelo Dezordi Wermuth - UNIJUÍ

A GUERRA CIBERNÉTICA NO CONTEXTO DAS CIDADES INTELIGENTES NO MUNDO PÓS-PANDÊMICO: PROVOCAÇÃO ANALÍTICA SOB O VIÉS DA CIBERSEGURANÇA/HACKING

CYBER WARFARE IN THE CONTEXT OF SMART CITIES IN THE POST-PANDEMIC WORLD: ANALYTICAL PROVOCATION UNDER THE CYBERSECURITY/HACKING BIAS

Ezequiel De Sousa Sanches Oliveira
Greice Patricia Fuller

Resumo

A pós-modernidade e a globalização trouxeram uma série de novas axiologias humanas tuteladas pelos Direitos e Garantias Fundamentais, sendo que a Carta da República Federativa de 1988 reflete tais demandas sociais a assegurar uma ordem de ações essenciais à sustentação da vida humana nas cidades (inteligentes ou não), sobretudo, em termos de dignidade. Estas ações precípuas do poder público, que devem passar pela defesa cibernética, também são definidas como imprescindíveis e também por isso ganharam relevância normativa com a promulgação do Código de Defesa do Consumidor, que garante a continuidade dos serviços sob o ângulo de atuação ininterrupta, a par da essencialidade de sua natureza. O uso da Internet nas cidades cada vez mais inteligentes (Smart Cities), cuja rede mundial de computadores é tomada como tecnologia da informação e comunicação, por impactar as ações humanas, deve passar por uma reflexão sob o viés da defesa cibernética no que toca à segurança da informação. No mundo pós-pandêmico, em virtude da pandemia coronavírus COVID-19, tornou-se sobressalente consequências oriundas da rapidez com que avanços das novas tecnologias da informação e comunicação permitiram a escalada da criminalidade informática de forma intensa e jamais vista, acompanhada da profusão da cibercultura e da disseminação do universo hacker no pós-pandemia.

Palavras-chave: Guerra cibernética, Cidades inteligentes, Cibersegurança, Pós-pandemia, Crimes informáticos

Abstract/Resumen/Résumé

Postmodernity and globalization have brought a series of new human axiologies protected by Fundamental Rights and Guarantees, and the Charter of the Federative Republic of 1988 reflects such social demands to ensure an order of essential actions to sustain human life in cities (smart or not), above all, in terms of dignity. These essential actions of the public power, which must go through cyber defense, are also defined as essential and also for this reason they gained normative relevance with the enactment of the Consumer Defense Code, which guarantees the continuity of services under the angle of uninterrupted performance, the par with the essentiality of its nature. The use of the Internet in increasingly intelligent cities (Smart Cities), whose global computer network is taken as information and communication

technology, as it impacts human actions, must undergo a reflection under the bias of cyber defense with regard to information security. In the post-pandemic world, due to the COVID-19 coronavirus pandemic, there have been outstanding consequences arising from the speed with which advances in new information and communication technologies have allowed the escalation of computer crime in an intense and unprecedented way, accompanied by the profusion of cyberculture and the dissemination of the hacker universe in the post-pandemic period.

Keywords/Palabras-claves/Mots-clés: Cyber war, Smart cities, Cybersecurity, Post-pandemic, Computer crimes

INTRODUÇÃO

Este artigo tem como objetivo geral compreender como o fenômeno das guerras cibernéticas provocou, provoca e provocará inúmeras e importantes transformações no seio das cidades, especialmente após a pandemia coronavírus COVID-19 (SARS-COV), que alterou significativamente a forma dos cidadãos se relacionarem entre si e o *locus* urbano.

No contexto pós-pandêmico e tentativa de retorno ao termo cunhado como "novo normal" destaca-se a crescente empreitada de ataques cibernéticos, que tomaram inegável profusão no momento em que a população mundial se recolheu em medida de quarentena e até os presentes dias percebe os impactos de profundas transformações havidas por conta da pandemia mundial sem precedentes, do qual não escapam as cidades (sobretudo as cidades inteligentes - *smart cities*) e seus habitantes do fenômeno conhecido como guerra cibernética.

Se a cidade, notadamente as chamadas inteligentes (*smart cities*) devem garantir o mínimo de bem estar e segurança, de rigor a problematização sob o viés virtual/digital, em que se proliferam os ataques cibernéticos às estruturas/ambientes das cidades, de modo a afetar seus habitantes.

Como objetivo específico, analisaremos os conceitos da cidade inteligente (*smart citie*) em face do preceito da segurança, tal como trazido pelo Estatuto da Cidade (Lei n.º 10.257/2001), bem como o conceitual da guerra cibernética.

A justificativa repousa na necessidade de encetar crítica reflexão sobre a (in)efetividade do preceito segurança pensando não como qualquer segurança, mas como segurança-cibernética, o que demanda sofisticações/adaptações para um cenário tão volátil a propiciar constantes mudanças e consequências na vida do cidadão.

Tal reflexão é acompanhada de problemáticas inerentes à sociedade da informação, assim pensada como sociedade pós-contemporânea e regada às novas tecnologias da informação e comunicação (TICs), que afeta o viés de segurança-cibernética a transpassar o indivíduo, a sociedade como um todo e as cidades que se propõem como inteligentes.

Logo, é inconcebível uma cidade dita inteligente que não garanta o mínimo de segurança cibernética, quando cenários de guerras cibernéticas são transportados dos países-Estados para as cidades, com novas modalidades e espécies de armas a serem utilizadas no ciberespaço.

Assim, dividiu-se o presente artigo em três partes imprescindíveis: 1. Análise conceitual sobre as cidades inteligentes; 2. Guerra Cibernética; 3. Segurança Cibernética à luz do Estatuto da Cidade. Após, as considerações finais seguidas das referências bibliográficas.

Finalmente, este trabalho aplicou o método dedutivo, analítica, reflexivo-crítico e jurídico, de acordo com a legislação e bibliografia referenciadas, com o propósito de provocar reflexões quanto à segurança promovida nas cidades inteligentes ante o fenômeno das cidades inteligentes.

1 ANÁLISE CONCEITUAL SOBRE AS CIDADES INTELIGENTES

A conceituação trazida por Vizzotto demonstra a imprescindibilidade de cuidado em relação ao ambiente da cidade, bem como o caráter assegurador de direito e garantia fundamental ao qual, por intermédio da cidade, tantos outros direitos acabam por serem exercitados:

> A cidade é um cenário de vida. Dinâmica e mutante, é formada pela sobreposição de vivências de cuja soma resulta o ambiente urbano. Costuma-se afirmar, para ratificar a noção dessa dinâmica, que a cidade que adormece não é a mesma que desperta. Além disso, a rapidez com que se deterioram os recursos urbano-ambientais levou à tomada de consciência sobre o papel das cidades e o que a civilização dela deseja. Assim, esse palco de vida mereceu atenção especial na Constituição de 1988, seguindo a mesma direção adotada por outros países, especialmente os do continente europeu. A partir de então, no caso brasileiro, a cidade foi alçada à dimensão constitucional,(4) aglutinando no seu âmbito outros direitos fundamentais, entre os quais, o direito à moradia, ao planejamento e à gestão do território e a uma efetiva, eficaz e eficiente política urbano-ambiental. Essa cidade constitucionalizada pressupõe ordenamento sustentável para a presente e futuras gerações. (VIZZOTTO, p. 2, 2014).

Noutra interpretação, com PATROCÍNIO, é destacado o fator do desenvolvimento humano sob perspectivas essenciais para a vida em sociedade mediante a utilização de novas tecnologias:

> (...) Cidade Inteligente, em seu conceito mais nativo (original), smartcity não envolve tão somente a implementação massiva de alta tecnologia mas o uso eficiente dos recursos informáticos (Hardware e Software). Nessa perspectiva o IDH é um instrumento que aponta-nos os dispares sociais e econômicos em uma sociedade contempla o desenvolvimento tecnológico porém sem as respostas práticas as velhas perguntas tais como: Educação, Trabalho e Renda. Por meio de dados práticos (reais) de antigos desafios, essa mensuração ajuda-nos a desenvolver e implementar respostas inovativas e criativas, catapultadas

> pela alta tecnologia, isto é aplicar inteligência no uso das TICS. (PATROCINIO, p. 11, 2016).

No artigo "*Placemaking* nas Cidades: A transformação do espaço público na Sociedade da Informação", é provocada a seguinte conceituação da cidade à partir de perspectivas axiológicas em torno do cidadão e do progresso:

> (...) por mais difícil que seja encontrar uma conotação precisa para definir civilização e cidade, é possível perceber que há dois valores em comum nos significados encontrados acima: cidadão e progresso; são esses os valores basilares e fundacionais de uma cidade, independentemente dos parâmetros que a História encontrou para definir cada etapa da civilização humana, pois, segundo Pinsky (2011) todas se justificam e culminam na luta de cidadãos pelo progresso de algo ou algum lugar.
>
> As cidades representam a grande revolução da humanidade. Elas permitem o trabalho organizado de um grande número de pessoas sob uma liderança que vai adquirindo legitimidade, a ponto de estabelecer sanções para os que se recusam a cumprir as tarefas estabelecidas. (FULLER; SUTTI, p. 4-5, 2021).

Feita esta digressão conceitual sobre a compreensão de *smart cities* e a acepção de como se pode compreender a cidade, é preciso destacar sobre a sofisticação com que, no caso de efetiva realização, a escalada da ofensiva cibernética pode danificar as cidades inteligentes, cujos ataques são passíveis de execução em minutos (senão segundos) a transcender estados-nação, de modo a prescindir de qualquer terrorista ou soldado em solo adversário, o que é agravado pela malha da rede, em que "Os provedores nacionais possuem e operam milhares de quilômetros de cabos de fibra ótica que vão de costa a costa, ligando todas as grandes cidades" (CLARKE, p. 106, 2015), o que possibilita a interligação de cidades inteligentes com outras cidades e países.

Também porque "ao contrário das armas nucleares, em que um atacante pode ser dissuadido pela promessa de retaliação, ou pela contaminação por radiação de suas próprias cidades, um ataque cibernético pode ocorrer com menos riscos" (CLARKE, p. 99, 2015), o que deve ser considerado em termos de cidades como alvo e também de civis.

2 GUERRA CIBERNÉTICA

Num comparativo com a guerra nuclear, as previsões em torno desta não teriam o mesmo grau de eficácia em relação à guerra cibernética, vez que

> A guerra cibernética não tem uma solução tão clara, visto que conquistar a paz no ciberespaço não é uma questão de resolver um problema tecnológico ou

> chegar a um local específico. Ao contrário, exige identificar e resolver uma série de problemas complexos e inter-relacionados. (CLARKE, p. 28, 2021).

Nesse particular, desdobra-se duas modalidades distintas de guerra cibernética (a exemplo do ocorrido na guerra dos EUA contra o Iraque e os ataques israelenses contra a Síria):

> Uma é o uso da guerra cibernética para facilitar um ataque convencional (o exército dos Estados Unidos prefere o termo ataque "cinético"), desativando as defesas do inimigo. A outra é o uso da guerra cibernética para enviar propaganda e desmoralizar o inimigo, distribuindo e-mails e outras mídias da Internet, no lugar da antiga prática de soltar panfletos de aviões (lembrem-se dos milhares de papéis com instruções em árabe e desenhos que foram jogados sobre as forças iraquianas em 1991, explicando-lhes como se render às forças norte-americanas. Milhares de iraquianos trouxeram os panfletos com eles ao se renderem). (CLARKE, p. 30-31, 2015).

Estes "são exemplos do uso militar de *hacking* como uma ferramenta para auxiliar em um tipo de guerra mais familiar". (CLARKE, p. 31, 2015), ou seja, algo de alcance doméstico.

À título de demonstração, de como uma cidade pode se ver no epicentro de uma guerra cibernética, tem-se o caso de Tallin:

> A utilização do espaço cibernético por estados-nação para objetivos políticos, diplomáticos ou militares, no entanto, não tem que ser acompanhada por bombardeios ou batalhas de tanques. Uma pequena amostra de como uma guerra cibernética isolada poderia acontecer veio, surpreendentemente, de uma pequena cidade de quatrocentas mil pessoas da Liga Hanseática às margens do Báltico. A cidade de Tallinn se tornou, mais uma vez, capital da Estônia independente em 1989, quando a União Soviética se desintegrou e muitas de suas repúblicas componentes se dissociaram de Moscou e da URSS. A Estônia tinha sido forçada a se tornar parte da União Soviética quando o Exército Vermelho "libertou" a república báltica dos nazistas, durante o que os russos chamam de "A Grande Guerra Patriótica". (CLARKE, p. 31, 2015).

Tem-se verificado forças-tarefas tais quais as encetadas pelos Estados Unidos da América, em cooperação com o Japão e Coreia do Sul:

> Em algum lugar da burocracia, um oficial americano anunciou publicamente que os Estados Unidos voltariam a realizar um exercício de guerra cibernética conhecido como Cyber Storm (tempestade cibernética), com a finalidade de testar as defesas de suas redes de computadores. O exercício de 2009 envolveria outros países, incluindo o Japão e a Coreia do Sul. A mídia norte-coreana logo respondeu, caracterizando o exercício como uma ação de cobertura para uma invasão da Coreia do Norte. Esse tipo de análise bizarra e paranoica é previsível da Coreia do Norte. Ninguém em Washington pensou duas vezes sobre o assunto. (CLARKE, p. 45, 2015).

A Guerra Cibernética também deve ser compreendida, sobretudo, como "Guerra de Informação", apesar de negligências deliberadas – tal qual a da Coréia do Norte – em

esquivar-se de investir e desenvolver adequada infraestrutura de rede, enquanto "ela tem investido muito para derrubar a infraestrutura de outros países".

> A Lab 110, suspeita de realizar os ataques cibernéticos de julho, é apenas uma das quatro unidades de guerra cibernética da Coreia do Norte. A unidade Conjunta de Guerra Cibernética do Korean Peoples Army (KPA), Unidade 121, tem mais de seiscentos hackers. O Departamento Secreto para Guerra Psicológica e Cibernética Inimiga, Unidade 204, possui cem hackers e é especializada em elementos cibernéticos para guerra de informação. (CLARKE, p. 50-51, 2015).

Tal mapeamento, com alto poder de ofensividade e potencialidade de comprometimento dos sistemas, se revela altamente sofisticada e mesmo surpreendente, como se denota do seguinte relato:

> O Departamento Central de Investigação do Partido, Unidade 35, é uma unidade cibernética menor, mas altamente capaz, com funções de segurança interna e capacidade ofensiva externa cibernética. A Unidade 121 é de longe a maior e, de acordo com um ex-hacker desertor, a mais bem treinada. Esta é especializada em desabilitar as redes de comunicação, comando e controle militares da Coreia do Sul. Alguns de seus elementos foram posicionados na China, uma vez que as conexões de Internet na Coreia do Norte, além de serem poucas, são facilmente identificadas. Se o governo de Pequim tem conhecimento de toda a extensão da presença norte-coreana e de suas atividades, isso não é claro, mas poucas coisas escapam da polícia secreta da China, especialmente na Internet. (CLARKE, p. 51, 2015).

O quadro geral, de países já acostumados com a maior intensidade da guerra cibernética, como é o caso da Coreia, não olvida no quesito "preparação" dos chamados "guerreiros cibernéticos" numa estrutura e escala de comando:

> Ao todo, o KPA da Coreia do Norte pode ter de seiscentos a mil agentes de guerra cibernética comandados por um tenente-coronel, atuando em células militares na RPC (República Popular da China). A Coreia do Norte seleciona estudantes de elite do ensino fundamental para serem preparados como futuros hackers. Esses alunos aprendem sobre hardware e programação de computadores durante os ensinos fundamental e médio e depois disso são automaticamente inscritos na Universidade de Automatização e Comando em Pyongyang, onde o único foco acadêmico é aprender como invadir sistemas e redes inimigas. Atualmente, setecentos alunos estariam inscritos nessa universidade. Além de alguns se infiltrarem no Japão para aprender habilidades mais recentes em computação, eles conduzem regularmente exercícios simulados de guerra cibernética, uns contra os outros. (CLARKE, p. 51-52, 2015).

Seguramente, a pretensão deste artigo não é a de alarmar o leitor, mas de provocar prudente reflexão acerca de debates num cenário global da guerra cibernética (já iniciadas entre Estados-nação) com potencial de afetar/comprometer o ambiente das cidades, com especial enfoque das cidades informatizadas, logo, inteligentes – a ponto de

considerar atualizações de suas defesas cibernéticas a fim de suplantar cenários para além de mero dissabor.

A par disso, extrai-se cinco preceitos. O primeiro, o da realidade:

> **A guerra cibernética é real.** O que temos visto até agora está longe de ser uma indicação do que ainda pode ser feito. A maioria desses famosos conflitos no ciberespaço utilizou apenas armas cibernéticas primitivas (com uma notável exceção da operação israelense). É uma suposição razoável a de que os atacantes ainda não quiseram revelar suas capacidades mais sofisticadas. O que os Estados Unidos e outras nações são capazes de fazer em uma guerra cibernética poderia devastar uma nação moderna. (CLARKE, p. 54-55, 2015).

O segundo preceito diz respeito à velocidade com que se deflagra a guerra cibernética:

> **A guerra cibernética acontece à velocidade da luz.** Assim como os fótons dos pacotes de ataque que correm pelos cabos de fibra ótica, o tempo entre o lançamento de um ataque e seus efeitos é dificilmente mensurável, sendo, dessa forma, um risco para tomadas de decisão em tempos de crise. (CLARKE, p. 55, 2015).

O terceiro, traz a dimensão global:

> **A guerra cibernética é global.** Em qualquer conflito, quando computadores e servidores de todo o mundo são invadidos e forçados a executar um serviço, os ataques cibernéticos se tornam rapidamente um assunto de interesse global, pois muitas nações são rapidamente envolvidas. (CLARKE, p. 55, 2015).

O quarto preceito, e talvez o mais peculiar e severo, torna irrelevante o *locus* de confronto:

> **A guerra cibernética ignora o campo de batalha.** Os sistemas dos quais as pessoas dependem, desde bancos até radares de defesa aérea, são acessíveis a partir do ciber-espaço e podem ser rapidamente dominados ou desligados, sem precisar derrotar inicialmente as defesas tradicionais de um país. (CLARKE, p. 55, 2015).

Por fim, o quinto preceito aponta para a necessária tomada de consciência sobre o tema problematizado neste artigo, dada a inicialização da guerra cibernética, da qual não escapam as cidades inteligentes:

> **A guerra cibernética já começou.** De forma a se antecipar às hostilidades, as nações já estão "preparando o campo de batalha", invadindo redes e infraestruturas umas das outras, instalando backdoors e bombas-lógicas – tudo isso agora, em tempos de paz. Esse estado permanente de guerra cibernética, essa indefinição entre paz e guerra, acrescenta uma perigosa nova dimensão de instabilidade. (CLARKE, p. 55, 2015).

O vislumbre de cenários caóticos oriundos de guerras cibernéticas e a incidir em cidades inteligentes é acrescido em relação à falta de prevenção de ataques informáticos, que vem com

> o fato de termos a capacidade de desligar o sistema de defesa aéreo chinês torna-se incômodo se pensarmos que, em uma crise futura, os guerreiros cibernéticos do Exército de Libertação Popular serão capazes de desligar o sistema elétrico de várias cidades americanas por semanas, fechar os mercados financeiros por meio da corrupção dos dados e gerar escassez nacional de alimentos e sobressalentes, embaralhando os sistemas de roteamento das grandes ferrovias norte-americanas. (CLARKE, p. 204, 2015).

Por isso, inexistem motivos para afastar o previsível contexto em que a maior parte das guerras cinéticas também envolvam, simultânea e condicionalmente, alguma guerra cibernética, notadamente como operações pontuais, isenta de bombardeios e/ou uso das forças armadas oficiais.

3 SEGURANÇA CIBERNÉTICA À LUZ DO ESTATUTO DA CIDADE

A cidade é um bem humano e não há dúvidas de que deve ser preservada em razão do apogeu cívico e representativo que exerce na sociedade:

> As cidades são o triunfo da condição humana. Nada tem tamanho grau de sofisticação, complexidade nem, ao mesmo tempo e paradoxalmente, tantas contradições e organicidade. Nelas o homem é senhor. Domina e transforma a natureza. As cidades são territórios inabitáveis à maioria das outras espécies. É, definitivamente, o habitat do ser humano. (NEVES, p. 59, 2020).

A questão é como preservar as cidades inteligentes ante um mundo globalizado e pós-contemporâneo em que as novas tecnologias da informação e comunicação se superam e incorporam algo novo, desconhecido e/ou jamais visto, que inclusive permita a sofisticação da já instalada guerra cibernética numa quadra global.

É cediço que a infraestrutura e malha que interliga o cenário das cidades passa pelo conceito trazido pelo seguinte autor:

> A integração dessa malha digital desponta um cenário também já vivenciado nas cidades é o conceito da Web das Coisas ou melhor dizendo a Internet das Coisas (IoT), que é uma das soluções tecnológicas, impulsionadora e altamente utilizada no mercado. O M2M (Machine-to-Machine), de infra-estrutura de comunicação por meio da malha de redes móveis, têm acelerado o processo de interconexão de rede das coisas. Que segundo a Consumer Electronics Association prevê que, até 2014, 70% dos dispositivos de consumo estarão ligados à internet (PATROCINIO, p. 14, 2016).

Ao considerarmos as constantes transformações e possibilidades de interfaces várias, no âmbito da sociedade da informação conectada sob a perspectiva das cidades inteligentes, tem-se interações variadas tais quais os dispositivos que permitem o tráfego de informações por mera aproximação, como o caso de RFID:

> Um desses novos contextos é o NFC: Near Field Comunication, tecnologia que permite a troca de informações com a aproximação física. Essa tecnologia descende do padrão RFID: Radio Frequency Identification uma das principais tecnologias para a implementação do conceito de IoT [Internet of Things – Internet das Coisas] o alcance do RFID passa também pela implementação de SmartCities[Cidade Inteligente] e SmartGrid[Rede Inteligente]. (PATROCINIO, p. 21, 2016).

Se num primeiro momento tais circunstâncias pareçam ampliadas, na medida em que se aprofunda a análise de riscos cibernéticos a questão se revela de impacto global, na medida em que a (in)segurança cibernética fica em xeque, de modo a resultar no questionamento sobre o uso de dados:

Não se trata de avaliar seus "impactos", mas de situar as irreversibilidades às quais um de seus usos nos levaria, de formular os projetos que explorariam as virtualidades que ela transporta e de decidir o que fazer dela. Contudo, acreditar em uma disponibilidade total das técnicas e de seu potencial para indivíduos ou coletivos supostamente livres, esclarecidos e racionais seria nutrir-se de ilusões. Muitas vezes, enquanto discutimos sobre os possíveis usos de uma dada tecnologia, algumas formas de usar já se impuseram. Antes de nossa conscientização, a dinâmica coletiva escavou seus atratores. Quando finalmente prestamos atenção, é demasiado tarde... Enquanto

A idéia, via preparação das *smart cities* sob o viés da segurança informática a fim de superar vulnerabilidades sistêmicas, é justamente evitar a instalação de cenários catastróficos:

> O fato de nossos sistemas vitais serem tão vulneráveis à guerra cibernética também aumenta a instabilidade de crise. Enquanto nossos sistemas econômicos e militares forem tão obviamente vulneráveis à guerra cibernética, nossos oponentes se sentirão instigados a nos atacar em períodos de tensão. (CLARKE, p. 206, 2015).

Sem dúvida que acaso frustrada as possibilidades de detecção de ataques, a preparação também deve funcionar à nível de apuração/investigação dos ataques cibernéticos, numa espécie de caminho de volta (engenharia reversa) das ações sofridas.

Todo este aspecto em se garantir o mínimo de segurança cibernética implica numa relação direta sobre propostas de cidades assim concebidas como "sustentáveis", tal como previsto no Estatuto da Cidade:

> No Brasil, o tema cidades, notadamente com o qualificativo "cidades sustentáveis" passou a ser tratado no Estatuto da Cidade (Lei 10.257/2001) que passou a regulamentar a Política Urbana prevista nos artigos 182 e 183 ambos da Constituição Federal de 1988, disciplinando as diretrizes fundamentais da ambiência artificial, objetivando o bem coletivo, a segurança, o bem-estar dos cidadãos, bem como o equilíbrio ambiental. (FULLER; SUTTI, p. 7, 2021).

A segurança cibernética nas cidades se trata de evidente questão de ordem pública a ser tutelada pelo Estado, vez que a previsão legal é expressa quanto ao interesse social em prol do bem coletivo, o que permite inferir o direito ao meio ambiente cibernético sustentável na Sociedade da Informação caracterizada por intensas e variadas relações digitais:

> CAPÍTULO I
>
> DIRETRIZES GERAIS
>
> Art. 1º Na execução da política urbana, de que tratam os arts. 182 e 183 da Constituição Federal, será aplicado o previsto nesta Lei.
>
> Parágrafo único. Para todos os efeitos, esta Lei, denominada Estatuto da Cidade, estabelece normas de ordem pública e interesse social que regulam o uso da propriedade urbana em prol do bem coletivo, da segurança e do bem-estar dos cidadãos, bem como do equilíbrio ambiental.

Com efeito, o ambiente virtual oriundo da evolução tecnológica e informática representa um novo ambiente (aí inseridas as cidades que cada vez mais incorporam e reinventam a sua "inteligência"), no qual os seres humanos constroem e inovam suas interações. Seja no trabalho, em casa ou no lazer, os usuários de computador entram em ambientes virtuais, ambientes nos quais informações, dados, imagens e sons são armazenados e transmitidos. A tecnologia da informação e a telemática permitem que as pessoas interajam, comuniquem-se, adquiram conhecimento, negociem e façam transações bancárias entre si e com as empresas.

Segundo a Política Nacional do Meio Ambiente, a tutela jurídica é reforçada com a seguinte definição objetiva:

> DA POLÍTICA NACIONAL DO MEIO AMBIENTE
>
> Art 2º - A Política Nacional do Meio Ambiente tem por objetivo a preservação, melhoria e recuperação da qualidade ambiental propícia à vida, visando

> assegurar, no País, condições ao desenvolvimento sócio-econômico, aos interesses da segurança nacional e à proteção da dignidade da vida humana, atendidos os seguintes princípios:
> I - ação governamental na manutenção do equilíbrio ecológico, considerando o meio ambiente como um patrimônio público a ser necessariamente assegurado e protegido, tendo em vista o uso coletivo;
> II - racionalização do uso do solo, do subsolo, da água e do ar;
> Ill - planejamento e fiscalização do uso dos recursos ambientais;
> IV - proteção dos ecossistemas, com a preservação de áreas representativas;
> V - controle e zoneamento das atividades potencial ou efetivamente poluidoras;
> VI - incentivos ao estudo e à pesquisa de tecnologias orientadas para o uso racional e a proteção dos recursos ambientais;
> VII - acompanhamento do estado da qualidade ambiental;
> VIII - recuperação de áreas degradadas; (Regulamento)
> IX - proteção de áreas ameaçadas de degradação;
> X - educação ambiental a todos os níveis de ensino, inclusive a educação da comunidade, objetivando capacitá-la para participação ativa na defesa do meio ambiente.
> Art 3º - Para os fins previstos nesta Lei, entende-se por:
> II - poluição, a degradação da qualidade ambiental resultante de atividades que direta ou indiretamente:
> a) prejudiquem a saúde, a segurança e o bem-estar da população;

É importante extrair a compreensão da cidade sob o ângulo biológico e cíclico, que pode ser apressado ou postergado (a depender das prevenções e segurança em contexto cibernético, variável de peso ao se tratar de cidade inteligente), de maneira a constatar seu nascedouro e eventual finalização, como por Neves problematizado:

> A cidade contemporânea ainda está em construção. O novo conceito, descentralizado, aborda o território em suas múltiplas particularidades. Entendeu-se o potencial econômico e social da ação humana na recuperação de fragmentos dessa cidade. Múltiplos, singulares, em diferentes escalas. Impulsionadas pela associação do capital privado, do regramento público e do poder de mobilização dos próprios cidadãos, as intervenções contemporâneas são precisas, pontuais e atuam sobre todos os aspectos da vida urbana, moradia, educação, lazer, trabalho, segurança, consumo, saúde, mobilidade. Volta-se o olhar para o retrovisor. Para a cidade construída, existente e abandonada pelo ímpeto expansionista e predatório. É preciso entender as cidades pela ótica da biologia. Elas nascem, crescem, envelhecem e, eventualmente, morrem. Precisam de cuidados constantes. (NEVES, p. 66-67, 2020).

À partir da noção de contemporaneidade, impõe-se desafios a serem resolvidos, tal qual o de garantias entre a privacidade e a segurança, aqui, com especial conotação informática. Dito de outro modo, há de se perquirir o quão segura deve ser uma cidade (inteligente), quanto e como sacrificar a privacidade em nome da segurança e vice-versa. Tal questão é inicialmente problematizada pelo autor italiano da sociedade da vigilância:

> "Menos privacidade, mais segurança" é uma receita falsa, avisa Stefano Rodotá. A propósito, ele recorre com frequência à metáfora do homem de vidro, de matriz nazista. A idéia do homem de vidro é totalitária porque sobre

> ela se baseia a pretensão do Estado de conhecer tudo, até os aspectos mais íntimos da vida dos cidadãos, transformando automaticamente em "suspeito" todo aquele que quiser salvaguardar sua vida privada. Ao argumento de que "quem não tem nada a esconder, nada deve temer", o autor não se cansa de admoestar que o emprego das tecnologias da informação coloca justamente o cidadão que nada tem a temer em uma situação de risco, de discriminação. "Menos cidadãos, mais suspeitos" é a expressão estigmatizante do momento. (...) A vigilância não conhece fronteiras (RODOTÀ, p. 8-9, 2008).

Saliente-se que pensar a segurança cibernética também como fenômeno à luz da capital está na ordem do dia, uma vez considerada a informação incrementada como ativo financeiro e econômico:

> "A melhor cidade que existe é a cidade que existe" é a frase síntese do urbanista Washington Fajardo que melhor define o momento em que nos encontrávamos no processo de planejamento das cidades. O retorno ao centro. A importância de reabilitá-lo e re-habitá-lo. A necessidade de reconstruir, reconectar, reciclar. Sustentabilizar era o norte do caminho que começávamos a trilhar antes da crise causada pela Covid-19. Diversas pandemias cruzaram a História da urbanidade alterando sua trajetória significativamente. Dessa vez não será diferente. Processos urbanos até então em andamento serão interrompidos e alguns novos, incentivados. Será acelerada a emersão de um novo capitalismo. (NEVES, p. 69, 2020).

A sustentabilidade assim vem na pauta da própria Câmara dos Deputados no Brasil:

> A cidade, consequentemente, deve ser usufruída e apropriada da melhor forma possível por aqueles que fazem dela seu local de morada. Contudo, o que faz uma cidade ser verdadeiramente sustentável? Várias são as respostas, e este capítulo é o espaço aberto para essa discussão. Buscamos descobrir o caminho mais favorável para que os cidadãos tenham mais qualidade de vida, e, assim, as cidades se perpetuem. (DEPUTADOS, p. 135, 2021).

Entretanto, encontramos contraposto na visão de Zuboff, que aqui se problematiza não como a existência pela existência da cidade, porque não se trata mais apenas disso, na exata medida em que "Casas, ruas, bairros, vilas, pequenas e grandes cidades: não são mais cenários locais onde vizinhos moram e caminham, onde moradores se encontram e conversam". (ZUBOFF, p. 217, 2019).

O existir pelo existir de uma cidade há de ser gabaritado (em contraposição) com ações do Google, empresa sabidamente regida pelo capital, a mapear todo espaço possível de solo:

> O Google já havia pegado tudo da web, mas o Street View e outras operações de mapeamento da companhia — o Google Maps e o Google Earth (a vista do mundo em 3-D da companhia, usando imagens aéreas e de satélite) — anunciavam uma visão ainda mais ambiciosa. Tudo no mundo devia ser conhecido e renderizado pelo Google, acessado pelo Google e indexado pelo Google em um apetite insaciável por superávit comportamental. A premissa é

> que nada está além das fronteiras do Google. Agora o mundo foi conquistado, está de joelhos, e foi trazido a você pelo Google. (ZUBOFF, p. 218, 2019).

O escopo capitalista é decodificado por Baumann sob a forma de outras modalidades de vigilância:

> E se tudo isso tem a ver com segurança, outros tipos de vigilância, relativos a compras rotineiras e comuns, acesso on-line ou participação em mídias sociais, também se tornam cada vez mais onipresentes. Temos de mostrar documentos de identidade, inserir senhas e usar controles codificados em numerosos contextos, desde fazer compras pela internet até entrar em prédios. A cada dia o Google anota nossas buscas, estimulando estratégias de marketing customizadas. (BAUMANN, p. 5, 2013).

Nos determos na acepção etimológica do termo é essencial para evolução e análise desta pesquisa:

> Vigiar – v.t. do lat. *vigilare*, ter cuidado de, estar de observação, de atalaia, de sentinela. Espreitar, sondar, verificar, velar, estar desperto, estar alerta, atento. Derivs: vigiado, adj.; vigiante, adj. Part. Pres.
> Vigilância – s.f. Cuidado especial sobre alguém ou alguma cousa; atenta observação dos movimentos e actos de alguém; cautela, zelo, diligência. Lat. *vigilantia* de *vigilare*, vigiar. (BUENO, p. 4252, 1974).

Nessa linha de entendimento, a par da ordem econômica e financeira, a Constituição da República Federativa do Brasil de 1988 prevê expressamente os princípios gerais da atividade econômica:

> Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:
> VI - defesa do meio ambiente, inclusive mediante tratamento diferenciado conforme o impacto ambiental dos produtos e serviços e de seus processos de elaboração e prestação; (Redação dada pela Emenda Constitucional nº 42, de 19.12.2003)

Portanto verifica-se como possível a utilização de arsenais inicialmente direcionadas ao contexto macro das guerras cibernéticas (tipicamente utilizados em confrontações entre Estados-Nações) transportados para os microambiente das cidades, com imprevisíveis resultados em termos de segurança ofensiva/defensiva nas cidades inteligentes e seus cidadãos.

Questão que se insurge é como a cibernética, no contexto de uma guerra, se deflagaria ante os (in)imagináveis avanços e engenhos tecnológicos. Nesse ponto, há de se trazer o conceito de cibernética sob a perspectiva utilitária, em um primeiro momento

como instrumento para previsão de fenômenos, fator essencial para o antes, durante e pós-guerra:

> 4ª O quarto aspecto da C. é constituído pelos usos e objetivos que ela pode ter nos mais diversos campos da atividade humana:
> a) Em primeiro lugar, a C. é um poderoso instrumento para explicar e prever fenômenos. Um de seus sucessos mais clamorosos foi visto no campo da genética (v.), em que possibilitou explicar a transmissão dos caracteres hereditários por meio das várias combinações dos elementos de um alfabeto genético constituído pelos ácidos desoxirribonucléicos, que compõem a hélice dupla do DNA (Watson e Crick, 1953). A teoria da evolução (v.), com bases darwinianas, considera que a própria evolução é um processo de variações aleatórias e de sobrevivência seletiva: dois conceitos que, como se viu, são fundamentais na teoria da informação. Em psicologia, antropologia e sociologia, esses conceitos são empregados para explicar qualquer forma de organização e atualmente são generalizados numa teoria dos sistemas, aplicável a todos esses campos (cf., p. ex., W. BUCKLEY, Sociology andModern Systems Theory, 1967, e relativa bibl.). (ABBAGNANO, p. 155, 2012).

Este ponto é essencial sobre aspectos valorativos e compreensão sobre limites e concepções acerca de dignidade humana no contexto de guerras cibernéticas, notadamente quanto ao potencial de Drones e demais Veículos (aéreos, terrestres e/ou aquáticos/marítimos) não tripulados, conquanto se permita a condução remota por pilotos/guerreiros cibernéticos.

Vai daí um cotejamento acerca de constructos informáticos em crescente escalada de sofisticação e mudanças para desempenho em guerra cibernética com efeitos devastadores para além da mera cibernética, o que resulta celeuma em torno dos limites (entre transmissões de “0s” e “1s” para assumir o controle dos sistemas) entre homem e máquina:

> b) Em segundo lugar, a C. é utilizada para a construção de máquinas cada vez mais complexas, às quais são confiadas operações e tarefas que, até pouco tempo, eram consideradas próprias do homem. Sobre os limites e as possibilidades dessas máquinas, as opiniões de cientistas e filósofos são díspares. Há quem considere que, em futuro mais ou menos próximo, elas poderão substituir o homem na solução de todos os seus problemas, inclusive nas escolhas decisivas que dizem respeito ao futuro ou à sobrevivência do gênero humano. Outros expressam dúvidas sobre essa possibilidade ilimitada, que entre outras coisas parece ser desmentida pelo teorema de Gõdel (v. MATEMÁTICA), entre cujas implicações está a de que não é possível construir uma máquina que resolva todos os problemas. Além disso, insiste-se na diferença entre o homem e a máquina, em vista da presença, no homem, do fator consciência (v.). Raymond Ruyer, por ex., afirmou que "sem consciência não há informação" e que, por isso, se o mundo físico e o mundo das máquinas ficassem entregues a si mesmos, "espontaneamente tudo se tornaria desordem e essa seria a prova de que nunca houve ordem verdadeira, ordem consistente, ou em outros termos, que nunca houve informação" (La cybemétique et lorigine de 1'information, 1954). (ABBAGNANO, p. 155, 2012).

E é disso que se trata: mudanças tais quais a de um caleidoscópio, que ao girar de ínfimos milímetros, todo o cenário/contexto é alterado o que enseja perplexidades como as que são postas:

> ¿Quién no admiraría a este nuestro camaleón? O, en general, ¿quién admiraría más alguna otra cosa? Con justa razón Asclepio de Atenas dijo que éste, a causa de su naturaleza mutable y que se transforma a sí misma, era simbolizado por Proteo en los mistérios. De aquí las bien conocidas metamorfosis celebradas entre los judíos y los pitagóricos. (MIRANDOLA, p. 83, 2018).

Se é de mudança que a revolução digital se alimenta e retroalimenta, há bens intangíveis passíveis de serem assegurados à luz do Estatuto da Cidade, com especial fim de prevenção a ataques maliciosos em expediente de guerra ou não, bem como qualquer outro tipo de ameaça a comprometer os sistemas de *smart cities*:

> Na quarta revolução industrial, a conectividade digital possibilitada por tecnologias de software está mudando profundamente a sociedade. A escala do impacto e a velocidade das mudanças fazem que a transformação seja diferente de qualquer outra revolução industrial da história da humanidade. O Conselho da Agenda Global do Fórum Econômico Mundial sobre o futuro do Software e da Sociedade realizou uma pesquisa com 800 executivos para avaliar quando os líderes empresariais acreditariam que essas tecnologias revolucionárias poderiam chegar ao domínio público em grau significativo e para compreender plenamente as implicações dessas mudanças para indivíduos, organizações, governo e sociedade. O relatório de pesquisa Mudança Profunda – Pontos de Inflexão Tecnológicos e Impactos Sociais foi publicado em setembro de 2015.88 Com o fluxo incessante de dados, preocupações emergem quanto aos riscos dessa hiperconectividade89, uma vez que "a IoT pode ser vista em diferentes dimensões pelos diferentes setores da academia e da indústria; qualquer que seja o ponto de vista, a IoT ainda não atingiu a maturidade e é vulnerável a todos os tipos de ameaças e ataques."90 São preocupações perenes e com as quais o Estado se defrontará. Por outro lado, Schwab enumera as seguintes mudanças e inovações tecnológicas com empolgante potencial disruptivo:
>
> (i) tecnologias implantáveis; (ii) presença digital; (iii) a visão como uma nova interface; (iv) tecnologias vestíveis; (v) computação ubíqua; (vi) supercomputadores que cabem no bolso; (vii) armazenamento para todos; (viii) A Internet das coisas e para as coisas; (ix) casas conectadas; (x) cidades inteligentes; (xi) big data e tomadas de decisão; (xii) carros autoguiados; (xiii) a Inteligência Artificial aplicada às tomadas de decisão; (xiv) a Inteligência Artificial aplicada às funções administrativas; (xv) a relação entre robótica e serviços; (xvi) a ascensão das criptomoedas; (xvii) a economia compartilhada; (xviii) a relação entre governos e blockchain; (xix) impressão 3D e fabricação; (xx) impressão 3D e a saúde humana; (xxi) impressão 3D e os produtos de consumo; (xxii) seres projetados; (xxiii) neurotecnologias. (BARBOSA; BRAGA NETTO; SILVA; FALEIROS JÚNIOR, p. 46-47, 2021).

Os posicionamentos acima são referendados pelas lições trazidas por Castells quando às inovações tecnológicas em trajetória irregular:

> (...) a explicação contextual para a trajetória irregular da inovação tecnológica parecer ser muito ampla e aberta a interpretações alternativas. Hall e Preston,

> ao analisarem a mudança geográfica da inovação tecnológica entre 1846 e 2003, mostram a importância de fontes *locais* de inovação, das quais Berlim, Nova York e Boston são coroadas como "centros mundiais de alta tecnologia industrial" entre 1880 e 1914, enquanto "Londres no mesmo período era uma sombra pálida de Berlim". O motivo disso encontra-se na base territorial para a interação de sistemas de descobertas e aplicações tecnológicas, isto é, nas propriedades sinérgicas do que é conhecido na literatura como "meios de inovação". (CASTELLS, p. 72-73, 1999).

Essa assimetria encontra amparo com Lévy, ao produzir os seguintes questionamentos:

> Por que inventar um "universal sem totalidade" quando já dispomos do rico conceito de pósmodernidade? Justamente porque não se trata da mesma coisa. A filosofia pósmoderna descreveu bem o esfacelamento da totalização. A fábula do progresso linear e garantido não possui mais curso nem em arte, nem em política, nem em qualquer outro domínio. (LÉVY, p. 128, 2010).

No atual estágio da arte, emergem dissensos em que a própria identidade humana é desafiada sobre a forma de se entender tais interações que tanto podem levar à guerra como cessá-la, quiçá, via de extermínio, o que enseja análises essenciais se – de fato – serão iniciadas, continuadas ou finalizadas por humanos ou por máquinas, se revela como problemática na ordem do dia da pós-contemporaneidade:

> Também são muitos os que insistem, com fundamentos vários (muitas vezes de natureza metafísica ou moral) na diferença entre o homem e a máquina, mas, em geral, reconhece-se que as máquinas têm as mesmas limitações do homem, ainda que em grau inferior, e que se distinguem do homem pela enorme "complexidade" do cérebro humano e pela capacidade que tem este último de prever, em proporção correspondentemente maior, os acontecimentos futuros. Wiener insistiu na exigência de uma simbiose entre o homem e a máquina, para a qual é necessário que o homem tenha uma clara ideia dos objetivos que devem ser preestabelecidos na programação e no uso das máquinas. De fato, obedecendo a um programa, uma máquina pode pôr em atividade certas operações que, diante de circunstâncias imprevistas, podem voltar-se contra os interesses e a própria vida do homem. Wiener observou que mesmo uma máquina que possa aprender e tomar decisões com base em conhecimentos adquiridos não será obrigada a decidir no mesmo sentido que nós, nem a tomar decisões que nos sejam aceitáveis:
>
> "Para quem não tem consciência disso, deixar suas responsabilidades a cargo da máquina (que possa ou não aprender) significará confiar suas próprias responsabilidades ao vento e vê-las de volta entre os turbilhões da tempestade" (The Human Use of Human Beings, 1950, cap. XI; cf. também God & Golem, Inc., 1964). Os problemas da C. estão intimamente ligados aos problemas da ontologia, da gnosiologia e da ética. (ABBAGNANO, p. 155-156, 2012).

Diante destes excertos, fica evidenciado que não há escapatória quanto ao necessário dever de cuidado de nossas cidades – sobretudo quando estas são guindadas ao patamar de *smart citie*s – o que impõe o desafio de repensar o lugar de cada um dos cidadãos, que inevitavelmente passa pela ambiente da cidade.

O desassossego diuturno refletido neste trabalho, mais especificamente sobre a potencialidade de deflagrações de guerras cibernéticas (desde a perceptíveis às não perceptíveis), vai na linha do desabafo humanista de Picco della Mirandola sobre reflexões desafiadoras:

> (...) responderé a quienes se molestan por el gran número de cuestiones propuestas, como si este peso recayera en sus hombros, cuando, más bien, sólo yo tengo que soportar esta fatiga por grande que sea. Es algo verdaderamente inconveniente y muy fastidioso querer imponer un límite a los esfuerzos de otros y –como dice Cicerón– desear la mediocridad en aquello que cuanto más grande es mejor. Ante una empresa tan vasta, era absolutamente absolutamente necesario que yo sucumbiera o lo lograra; si lo llegara a lograr, no veo por qué lo que es loable conseguir en diez cuestiones, sea reprobable si ha sido conseguido aun en 900. Si no lo llegara a lograr, tendrán de qué acusarme si me odian, y si me aman, de qué disculparme: que un adolescente de ingenio débil y limitada cultura haya fracasado en una cosa tan difícil y tan grande será más digno de perdón que de acusación. Más bien, como dice el poeta: "Si faltan las fuerzas, ciertamente la audacia será un motivo de alabanza: en las grandes empresas hasta haber querido es bastante". Y si en nuestros días muchos, imitando a Gorgias de Leontinos, suelen organizar discusiones con aprobación no sólo sobre 900 cuestiones, sino sobre todas las cuestiones de todas las artes, ¿por qué a mí no se me permitiría discutir, incluso sin culpa, sobre muchas sí, pero ciertas y determinadas cuestiones?

CONSIDERAÇÕES FINAIS

Na sociedade da informação as ocorrências se dão em transmissões de "0s" e "1s" para assumir o controle dos sistemas, principalmente no contexto de uma guerra cibernética.

O expediente de treino e testagens em cenários emulados de Guerra Cibernética devem encampar as políticas públicas das cidades com desiderato previsto no Estatuto da Cidade, como medida de controle e correção de eventuais falhas.

Apagões cibernéticos que desdobrarão em uma série de outros apagões de serviços essenciais a comprometer os transportes públicos, sistemas de trânsito, hospitais, abastecimento alimentar, saneamento básico e segurança pública, quando não o envide de "bombas relógios" armadas remota e telematicamente.

Não há escapatória quanto ao necessário dever de cuidado de nossas cidades – sobretudo quando estas são guindadas ao patamar de *smart cities* – o que impõe o desafio de repensar o lugar de cada um dos cidadãos, que inevitavelmente passa pela ambiente da cidade, que deve ser pensado sobretudo de forma preventiva.

As mudanças tecnológicas se operam tal qual um caleidoscópio, que ao girar de ínfimos milímetros, todo o cenário/contexto é alterado, o que impacta o cenário das cidades no aspecto da segurança, sobretudo a segurança da informação.

A revolução digital se alimenta e retroalimenta, há bens intangíveis passíveis de serem assegurados à luz do Estatuto da Cidade, com especial fim de prevenção a ataques maliciosos em expediente de guerra ou não, bem como qualquer outro tipo de ameaça a comprometer os sistemas de *smart cities.*

Finalmente, a cibernética, no contexto de uma guerra, é passível de perquirições quanto a sua deflagração ante os (in)imagináveis avanços e engenhos tecnológicos, em meio a veículos não tripulados e guerreiros cibernéticos remotos, notadamente quanto a quem iniciaria, continuaria, finalizaria ou exterminaria via guerra cibernética: se o ser humano ou a máquina.

REFERÊNCIAS

ABBAGNANO, Nicola. **Dicionário de filosofia /** Nicola Abbagnano; tradução da 1.ª edição brasileira coordenada e revista por Alfredo Bosi; revisão da tradução e tradução dos novos textos Ivone Castilho Benedetti. – 6.ª ed. – São Paulo: Editora WMF Martins Fontes, 2012.

BARBOSA, Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito digital e inteligência artificia**l [recurso eletrônico] : diálogos entre Brasil e Europa / A. Barreto Menezes Cordeiro ... [et al.] ; coordenado por Felipe Braga Netto ... [et al.]. versão do Kindle. - Indaiatuba, SP: Editora Foco, 2021.

BAUMANN**,** Zygmunt; LYON, David. **Vigilância Líquida.** Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BRASIL. Lei n.º 6.938, de 31 de agosto de 1981. **Política Nacional do Meio Ambiente.** Brasília, DF: Presidência da República, 1981. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6938.htm. Acesso em: 16 out. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 out. 2022.

BRASIL. Lei n.º 10.257, de 10 de julho de 2001. **Estatuto da Cidade.** Brasília, DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10257.htm. Acesso em: 16 out. 2022.

BUENO, Francisco da Silveira. **GRANDE DICIONÁRIO ETIMOLÓGICO – PROSÓDICO da Língua Portuguesa**. Vocábulos, Expressões da Língua Geral e Científica-Sinônimos, Contribuições do Tupi-Guarani. Santos-SP: Editora Brasília Limitada, 1974.

CASTELLS, Manuel. **A sociedade em rede /** Manuel Castells. Tradução: Roneide Venâncio Majer; atualização para 6.ª edição: Jussara Simões – (A era da informação: economia, sociedade e cultura; v. 1) São Paulo: Paz e Terra. ISBN 85-219-0329-4, 1999.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito.** Brasport. ISBN Digital: 978-85-7452-737-6 Edição do Kindle, 2015.

CLARKE, Richard A.; KNAKE, Robert K. **O Quinto Domínio: Defendendo Nosso País, Nossas Empresas e Nós Mesmos na Era das Ameaças Cibernéticas.** 1ª edição. Editora: Alta Books. Edição do Kindle, 2021.

DEPUTADOS, Câmara dos. **Cidades Inteligentes: Uma abordagem humana e sustentável.** Edições Câmara. Edição do Kindle, 2021.

FULLER, Greice Patricia; SUTTI, Alessandra Arantes. PLACEMAKING NAS CIDADES: A TRANSFORMAÇÃO DO ESPAÇO PÚBLICO NA SOCIEDADE DA INFORMAÇÃO. DOI: 10.12957/rdc.2021.44787. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rdc/article/view/44787/39688. Acesso em 17 out. 2022.

LÉVY, Pierre. **Cibercultura.** Tradução de Carlos Irineu da Costa. Editora 34, 2010.

MIRANDOLA, Giovanni Pico Della. **Discurso sobre la dignidade del hombre.** Editora Universidad Nacional Autónoma de México, Dirección General de Publicaciones y Fomento Editorial. Edição do Kindle, 2018.

NEVES, José Roberto de Castro. **O mundo pós-pandemia : reflexões sobre uma nova vida /** organização José Roberto de Castro Neves. -- 2. ed. -- Rio de Janeiro : Nova Fronteira, Edição do Kindle, 2020.

RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje /** Stefano Rodotà. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008.

PATROCÍNIO, Cláudio. **Cidades Inteligentes: Smart City for Smart Planet (Cidade Inteligente para o Planeta Inteligente: Série Smart City Livro 1).** Cláudio Patrocinio. Edição do Kindle, 2016.

VIZZOTO, Andrea Teichmann. **A Lei de improbidade administrativa e o artigo 52 do Estatuto da Cidade.** 2014. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2014;1001054235. Acesso em 16 out. 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância. A luta por um futuro humano na nova fronteira do poder.** E-ISBN 978-65-5560-145-9. Edição do Kindle – São Paulo: Editora Intrínseca, 2019.