Research, Society and Development, v. 11, n. 16, e553111638647, 2022
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v11i16.38647

Tecnologia disruptiva e segurança pública: uma análise da produção científica mundial

Disruptive technology and public security: an analysis of the worldwide scientific production

Tecnología disruptiva y seguridad pública: un análisis de la producción científica mundial

Recebido: 28/11/2022 | Revisado: 12/12/2022 | Aceitado: 13/12/2022 | Publicado: 18/12/2022

Denise Fukumi Tsunoda
ORCID: https://orcid.org/0000-0002-5663-4534
Universidade Federal do Paraná, Brasil
E-mail: dtsunoda@ufpr.br
Ana Clara Cândido
ORCID: https://orcid.org/0000-0003-1897-3946
Universidade Federal de Santa Catarina, Brasil
E-mail: ana.candido@ufsc.br

Resumo
Com o objetivo de identificar quais tecnologias disruptivas, com foco na inteligência artificial estão sendo adotadas e pesquisadas no mundo, apresenta-se a pesquisa conduzida de forma integrativa em bases de dados de periódicos (IEEE Xplore, Science Direct, Web of Science, Scopus e Dimensions) e outros mecanismos de busca, como o Google Acadêmico, para complementação de dados sobre os pesquisadores e publicações. Na pesquisa é identificada a preferência pelas publicações em repositórios de preprints, os países, os autores, instituições e editoras com o maior número de publicações. Após realização de análise de conteúdo nos principais documentos, são identificadas as tecnologias e principais aplicações das tecnologias disruptivas, com foco na inteligência artificial em segurança pública. Nas análises conduzidas, as tecnologias que aparecem em destaque são internet of things, big data e blockchain. Os resultados apontam quais e para qual propósito as tecnologias disruptivas, com foco na inteligência artificial, estão sendo adotadas e pesquisadas no mundo. Adicionalmente destaca a legislação como sendo a principal preocupação encontrada nos documentos e as oportunidades e tendências de pesquisas.
Palavras-chave: Inteligência artificial; Machine learning; Internet das coisas; Blockchain; Big data.

Abstract
The objective of this research is to identify which disruptive technologies, focusing on artificial intelligence, are being adopted and researched worldwide. The research conducted in an integrative manner in journal databases (IEEE Xplore, Science Direct, Web of Science, Scopus and Dimensions) and other search engines such as Google Scholar, to complement the data concerning researchers and publications, is presented. The research identifies the preference for publications in repositories of preprints, the countries, authors, institutions and publishers with the largest number of publications. After conducting content analysis on the main documents, the technologies and main applications of disruptive technologies are identified, with a focus on artificial intelligence in public security. In the analyses conducted, the technologies that stand out are the internet of things, big data, and blockchain. The results indicate which disruptive technologies, with a focus on artificial intelligence, are being adopted and researched worldwide, and for what purpose. Additionally, it highlights legislation as the main concern found in the papers and research opportunities and trends.
Keywords: Artificial intelligence; Machine learning; Internet of things; Blockchain; Big data.

Resumen
Con vistas a identificar qué tecnologías disruptivas, centradas en la inteligencia artificial, se están adoptando e investigando en todo el mundo, se presenta la investigación realizada de forma integradora en bases de datos de revistas (IEEE Xplore, Science Direct, Web of Science, Scopus y Dimensions) y otros motores de búsqueda como Google Scholar, para complementar los datos sobre investigadores y publicaciones. La investigación identifica la preferencia por las publicaciones en repositorios de preprints, los países, los autores, las instituciones y las editoriales con mayor número de publicaciones. Tras realizar un análisis de contenido de los principales documentos, se identifican las tecnologías y las principales aplicaciones de las tecnologías disruptivas, centrándose en la inteligencia artificial en la seguridad pública. En los análisis realizados, las tecnologías que aparecen de forma destacada son internet de las cosas, big data y blockchain. Los resultados indican qué tecnologías disruptivas, centradas en la inteligencia artificial, se están adoptando e investigando en todo el mundo y con qué finalidad. Además, destaca la legislación como la principal preocupación encontrada en los documentos y las oportunidades y tendencias de investigación.
Palabras clave: Inteligencia artificial; Aprendizaje automático; Internet de las cosas; Blockchain; Big data.

1. Introdução

Homo digitalis? Segundo Martha Gabriel (Gabriel, 2022) a atual Revolução Digital apresenta esta "nova espécie" – de Homo sapiens a Homo digitalis – que seria um misto de orgânico e digital. Enquanto as revoluções anteriores tiveram o propósito de melhorar a vida humana, a digital tende a mudar o que significa ser humano.

O diferencial da Revolução Digital em relação às grandes revoluções tecnológicas anteriores não é a profundidade do impacto causado, mas a sua velocidade. Todas as demais também surtiram efeitos significativos na humanidade, "mas nenhuma em um ritmo tão vertiginoso quanto o atual" (Gabriel, 2022). Ainda assim, é importante separar o que realmente tem efeito transformador daquilo que é apenas "modismo". O fato de a humanidade ser digital acarreta mais benefícios do que saneamento básico ou energia elétrica? Em uma análise rápida, estas inovações viabilizaram a Revolução Digital. Os impactos do saneamento básico na saúde e qualidade de vida dos seres humanos foram tão ou até mesmo mais significativos que os da atualidade. O que a autora (Gabriel, 2022) apresenta é que cada revolução contribuiu com as inovações e transformações que viabilizaram que o próximo estágio fosse alcançado pela humanidade.

O conceito de inovação disruptiva foi cunhado por Clayton Christensen, em seu livro seminal "O dilema da inovação" (Christensen, 2011), no qual ele analisa como pequenas inovações marginais podem transformar totalmente o setor de mercado em que entram, mudando, inclusive, a relação de poder de líderes. Nesta obra o autor diferencia "inovação incremental" de "inovação de ruptura", explicando que a primeira "introduz melhorias (discretas ou mesmo radicais) aos produtos já estabelecidos. Geralmente entregam ainda mais valor aos mercados e clientes habituais" enquanto que a segunda "traz uma proposição de valor muito diferente daquela disponível até então, mudando totalmente a forma como fazemos ou compreendemos algo".

Quando determinadas inovações tecnológicas transformam radicalmente a sociedade, elas são chamadas de disruptivas, porque representam uma "ruptura" na lógica de funcionamento dos modelos de mundo, alterando completamente as regras sociais e econômicas. Vários exemplos poderiam ser mencionados aqui e a autora (Gabriel, 2022) apresenta a escrita que viabilizou para a "humanidade acumular e trocar conhecimento, relocando os polos de poder econômicos e sociais".

O Anuário de Segurança Pública 2022 (Bueno & Lima, 2022), publicado e atualizado pelo Fórum de Segurança Pública em 02 de agosto de 2022, apresenta algumas estatísticas preocupantes, dentre as quais destacam-se: Brasil tem 2,7% dos habitantes do planeta e 20,4% dos homicídios com vítimas sendo caracterizadas por 77,9% negras, 50% entre 12 e 29 anos e 91,3% do sexo masculino. A Amazônia aparece em evidência com 1/3 das cidades mais violentas e taxa de violência letal é 38% superior à média nacional. Os crimes de violência sexual tiveram aumento de 4,2% em 2021 e somaram 66.020 estupros com 75,5% das vítimas incapazes de consentir, 61,3% até 13 anos e em 79,6% dos casos o autor era conhecido da vítima.

Quanto ao crescimento da violência contra a mulher, foram 230.861 agressões por violência doméstica (aumento de 0,6% em relação ao ano anterior), 597.623 ameaças (aumento de 3,3% em relação ao ano anterior) e 370.209 Medidas Protetivas de Urgência (MPUs) concedidas (aumento de 13,6% em relação ao ano anterior). Foram 1.341 vítimas de feminicídio e destas 68,7% entre 18 e 44 anos, 656,6% morreram dentro de casa, 62% eram negras e em 81,7% dos casos, o crime foi cometido por companheiro ou ex-companheiro.

O mesmo Anuário (Bueno & Lima, 2022) aponta 682.279 agentes policiais no país em 86 corporações sendo 406.384 policiais militares, 91.926 policiais civis, 55.072 bombeiros, 11.615 da polícia federal e 12.324 da polícia rodoviária federal. Os demais são peritos (11.823) e policiais penais federais (919).

Um ponto de atenção foi o fato da palavra inteligência ter 5 ocorrências, na página 38 mencionando os "investimentos significativos" na "modernização da gestão das polícias e a adoção de novas tecnologias e sistemas de inteligência", na Tabela 59 (p. 280) como significado da Agência Brasileira de Inteligência (ABIn), na página 309 e 323 para apresentar o valor total

investido em “Informação e inteligência” (R$ 1.660.294.260,08 em 2021) e na página 482 que explica o sistema CompStat adotado nos Estados Unidos. Percebe-se que o Anuário não aborda como (ou quais tipos de) a “inteligência” está sendo utilizada como suporte à segurança pública no país.

Desta forma, o objetivo desta pesquisa conduzida de forma integrativa em bases de dados de periódicos é identificar como as tecnologias disruptivas, com foco na inteligência artificial estão sendo adotadas e pesquisadas no mundo.

Em 2022, conforme apontando na condução da revisão, algumas tecnologias aparecem em destaque: internet of things (IoT), big data e blockchain. Por este motivo, também foram analisadas e discutidas nos resultados desta pesquisa.

2. Metodologia

As pesquisas foram conduzidas nas bases científicas (IEEE Xplore, Science Direct, Scopus, Web of Science e Dimensions) em 11 de agosto de 2022 pelos termos “tecnologia disruptiva”, “inovação” e “segurança pública”, nos idiomas português e inglês (“disruptive technology”, “innovation” e “public security”). Para a estratégia de busca geral, as strings ficaram assim definidas: (“tecnologia disruptiva” OR “inovação”) AND “segurança pública” (em português) e (“disruptive technology” OR “innovation”) AND “public security”) (em inglês). A pesquisa foi realizada sem filtros de idioma e período (sem recorte temporal), mas foram selecionados os artigos disponíveis em acesso aberto, para viabilizar a leitura dos trabalhos recuperados.

Para a busca em com os termos em português não foram obtidos retornos nas bases pesquisadas e, após a leitura de 50 retornos com os termos em inglês, a estratégia de pesquisa foi atualizada para: ("public security" OR "public safety" OR "national security" OR "law enforcement") AND (innovation OR "disruptive technology") AND (“machine learning” OR “artificial intelligence”). Tal pesquisa foi conduzida, nas mesmas cinco bases de periódicos anteriormente citadas, em 15 de setembro de 2022 e obteve os retornos que estão representados no diagrama PRISMA (Figura 1), seguindo o modelo PRISMA 2020 (Page et al., 2021).

As análises sobre os materiais recuperados foram conduzidas de três formas:

a) com o corpus após a remoção dos termos duplicados, contendo 790 registros, foram realizadas análises por métricas tais como: autores, tecnologias em destaque, países, periódicos que mais publicam o tema, período de publicação e linha de tendência, palavras-chaves, bigramas nos títulos e trigramas nos abstracts;

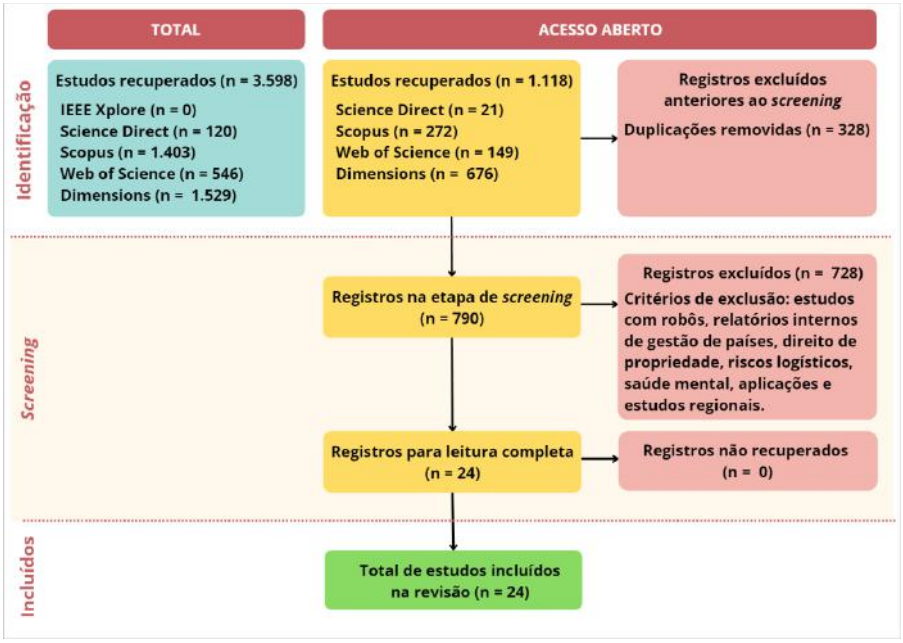
b) com o corpus após a etapa de *screening* (leitura de título, palavras-chaves e abstracts), contendo 24 registros, foi realizada a leitura completa, com análise de conteúdo sem utilização de ferramenta de suporte, dos materiais recuperados para identificação de abordagens, ferramentas, métodos e base de dados utilizadas. Nesta etapa, foi adotado o critério de inclusão de uso de tecnologias disruptiva tais como inteligência artificial, machine learning, mineração de dados aplicados à segurança pública e alguns critérios de exclusão tais como: estudos com foco puramente em robótica; relatórios internos de gestão de países (China, por exemplo); análises de riscos logísticos; revisões sistemáticas de rivalidades entre países (entre China e Estados Unidos, por exemplo); análises de fluxos de inovações financeiras; registros de patentes internos em alguns países; regulamentação interna do uso de tecnologias (a exemplo do complexo agrícola russo); e impactos de uso de tecnologias para trabalhar com processos que envolvem informações jurídicas;

c) as palavras-chaves que identificam tecnologias que apareceram em destaque na análise “a” foram pesquisadas na base de dados lens.org para identificação de crescimento de interesse no tema, países, áreas de conhecimento que estão produzindo sobre o tema, pesquisadores e outros aspectos relevantes.

Trata-se, portanto, de uma pesquisa de revisão sistemática que segue o fluxograma PRISMA - Preferred Reporting Items

for Systematic reviews and Meta-Analyses atualizado em 2021 (Page et al., 2021) com destaque para: bases de dados de periódicos utilizadas, número de artigos recuperados em cada base, número de artigos excluídos antes do *screening* (por ser duplicado ou removido com aplicação dos filtros), artigos rastreados (etapa de *screening*: leitura do título ou título e resumo), artigos excluídos no rastreio, artigos para leitura do texto completo, artigos excluídos na leitura do texto completo e número de estudos incluídos na amostra para a análise de conteúdo.

Figura 1 - Fluxograma PRISMA da condução da pesquisa.



Fonte: Autoras (2022).

Todas as análises foram conduzidas por meio das ferramentas (Figura 2): Office 365 (Microsoft Excel), Biblioshiny (pacote R), o próprio sistema de visualização da base de periódicos Lens, o gerador de nuvem de palavras WordsCloud , a ferramenta Canva para desenho do fluxo PRISMA (Figura 1) e a ferramenta de tradução DeepL para tradução dos artigos em russo e indonésio.

Figura 2 - Bases e ferramentas utilizadas na pesquisa.

Fonte: Autoras (2022).

Uma das ferramentas citadas (Figura 2) é a linguagem Python que foi utilizada para desenvolvimento de dois programas

de suporte. A primeira reúne os padrões BibTeX de 4 das 5 bases de periódicos utilizadas (IEEE Xplore, Science Direct, Web of Science e Dimensions) no padrão da Scopus (a quinta base utilizada) para entrada na ferramenta Biblioshiny do pacote Bibliometrix, disponível para a linguagem de programação R. O Biblioshiny foi utilizado para a geração de diversas estatísticas, como a nuvem de palavras-chave de autores, o volume de produção anual, a avaliação contribuição coletiva de países, redes de cooperação entre autores e diversas outras.

A segunda ferramenta implementada tem o objetivo de aprimorar as análises das terminologias utilizadas dentro do corpus por meio de técnicas de Processamento de Linguagem Natural aplicadas sobre os textos dos documentos do corpus. Estas técnicas foram viabilizadas pelo pacote SpaCy presente no ecossistema da linguagem de programação Python. O SpaCy é um pacote baseado em um modelo de aprendizado profundo e oferece diversas funcionalidades em nível linguístico. O processo seguiu o fluxo apresentado na Figura 3.

Figura 3 - Ferramenta que utiliza NLP para identificação de multigramas

Fonte: Autoras (2022).

Os multigramas extraídos foram trigramas, sequências de três palavras, bigramas, sequências de duas palavras, e unigramas, palavras isoladas, desde que com ao menos duas ocorrências. Os multigramas encontrados em cada sentença do texto foram reunidos e passaram a contar como uma ocorrência dentro do conjunto global do corpus e o conjunto final foi composto pelos multigramas mais frequentes, desde que não constituíssem descritores utilizados nas buscas de artigos.

O passo 1 foi necessário porque o SpaCy não é capaz de operar sobre documentos PDF. Optou-se pelo passo 2 para extrair os multigramas exclusivamente do texto principal dos documentos. O passo 3 foi aplicado para evitar a composição de multigramas que ultrapassem a fronteira de frases, pois estas não fariam sentido para análise, mas poderiam influenciar o resultado. O passo 4 faz uso do recurso do SpaCy de identificar a função sintática das palavras dentro das frases, recurso conhecido como “Part-of-speech tagging”, ou simplesmente “POS-tagging”. Essa estratégia garante que apenas substantivos (adjetivados ou não) e nomes próprios sejam considerados como multigramas potenciais. No passo 5 buscou-se por multigramas que tivessem representatividade dentro da coleção de substantivos e nomes próprios, contabilizando suas frequências em cada documento e no contexto de todo o corpus. Com o passo 6 a contagem do mesmo conceito, que por vezes é representado por sua

sigla, foi corrigida e os multigramas foram ordenados, sendo que os presentes nos termos de busca foram removidos, pois sua presença não traz informação.

O conjunto final de multigramas selecionados, conhecido como bag-of-words (Zhang et al., 2010) serviu como entrada para a geração das nuvens de palavras de título-resumos e serão explicados na próxima seção.

3. Resultados e Discussão

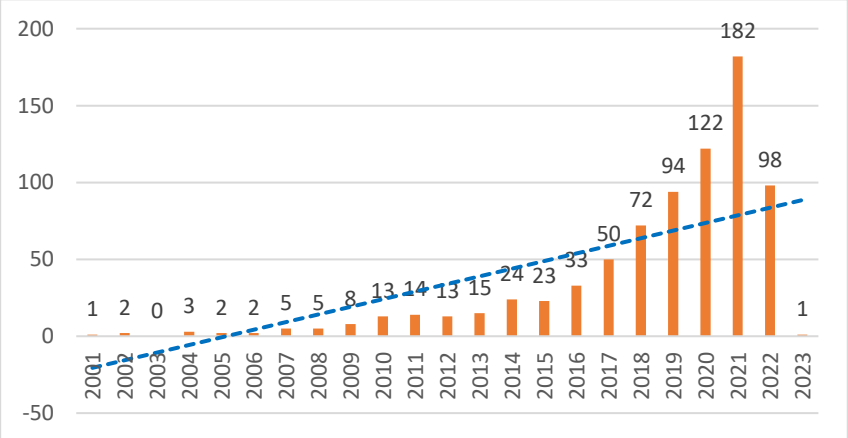
Conforme explicado na seção anterior, foram conduzidos três tipos de análises sobre os corpora recuperados. Desta forma, esta seção está dividida em três principais: análise de métricas utilizando o corpus com 790 registros, análise dos textos completos dos 24 documentos após a etapa de *screening* e análise das tendências das três tecnologias como maior ocorrência nas palavras-chaves dos autores no corpus de 790 registros.

3.1. Corpus completo

Este corpus, com 790 documentos no total, apresentou 521 fontes distintas, 1.015 palavras-chaves de autores, 2.226 autores e destes 292 produziram documentos monográficos, e os que produziram em equipes, houve uma média de 2,95 integrantes por trabalho. Considerando-se os tipos de publicações, 547 (69,24%) são artigos em periódicos e 123 (15,57%) em *preprint*.

Os documentos recuperados datam de 1978 até 2023 (não foram realizados filtros por período) e destas, 8 estão esparsamente distribuídas entre 1978 e 2000. O Gráfico 1 apresenta as produções anuais de 2001 até 2023 e uma linha de tendência (tracejada). Observa-se crescimento contínuo a partir de 2015 e o ano com maior produção foi 2021 com 182 produções. Em 2022 registra-se uma diminuição na produção, mas é importante relembrar que esta pesquisa foi conduzida em 15 de setembro de 2022 de forma que as produções ainda estão sendo depositadas nas bases pesquisadas.

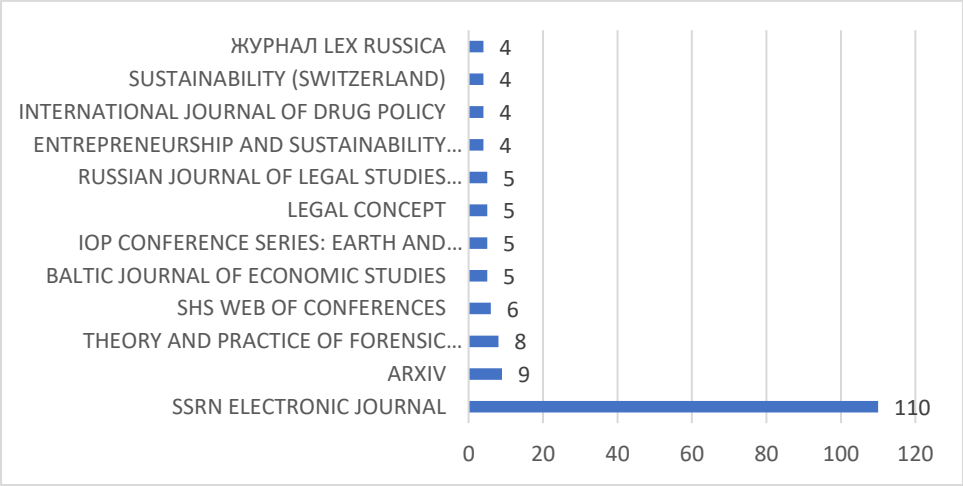
Gráfico 1 - Produção no período, com linha de tendência.



Fonte: Autoras (2022).

Pesquisando-se quais as fontes de periódicos mais utilizadas pelos autores para as suas publicações, o SRRN Electronic Journal aparece com ampla vantagem com 110 (13,92%) das 790 produções recuperadas e o ARXIV aparece em segundo lugar com 9 (1,14%) do total recuperado.

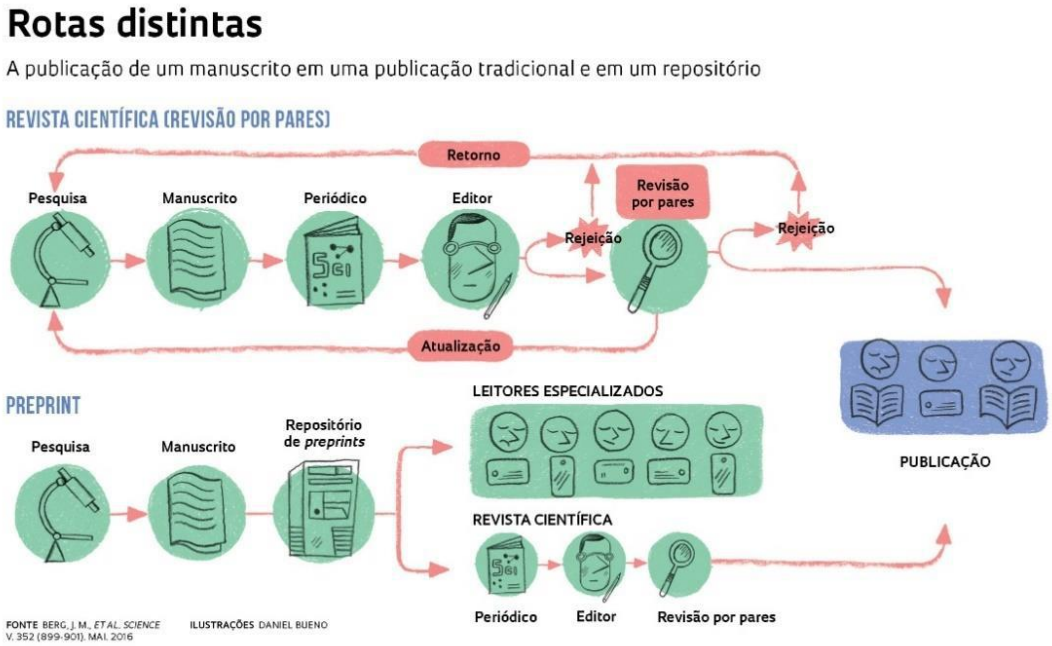
Gráfico 2 - Periódicos com o maior número de produções recuperadas.



Fonte: Autoras (2022).

Reunidas, as duas principais formas de publicação dos trabalhos representam 15,06% do corpus. Tal fato tem sido observado em outras pesquisas pela própria característica destas publicações chamadas *preprints*. A Figura 1, retirada do artigo "Revisão em Praça Pública" de Bruno de Pierro (de Pierro, 2017) ilustra e justificativa a escolha pelo depósito em repositórios considerando o fluxo de publicação que menciona que os documentos são disponibilizados em repositórios eletrônicos públicos e expõem os resultados "à crítica instantânea da comunidade científica". Adicionalmente, o autor pontua que revistas com altíssimo fator de impacto como a Science que, a exemplo de vários outros periódicos, não publica artigos que não sejam originais, admite "publicar bons artigos já depositados em repositórios, como o bioRxiv, de ciências biológicas, ou o arXiv".

Figura 1 - Rotas de Revistas Científicas (revisão por pares) e Preprints.



Fonte: De Pierro (2017).

O depósito nos repositórios para os autores é gratuito e rápido. O SSRN[1] menciona depósito de 1.186.083 trabalhos de pesquisa de 1.058.114 pesquisadores em mais de 65 disciplinas em 09 de novembro de 2022. Desde 2016 a SSRN está sob responsabilidade da Mendeley e Elsevier para coordenação da plataforma. O arXiv[2] é mantido pela Simons Foundation da Cornell University além de instituições parceiras e doadores. Em 09 de novembro de 2022, a plataforma aponta 2.157.488 artigos acadêmicos nas áreas de física, matemática, ciência da computação, biologia, finanças, estatística, engenharia elétrica e economia.

Na sequência da análise foram considerados os países e universidades com as maiores produções. O país que apareceu em primeiro lugar com 10 publicações foi os Estados Unidos, seguido pela Ucrânica (7), Nigéria (6), Rússia (4) e Aústria e Grécia (ambos com 3 publicações cada). Dentre as universidades o destaque ficou para a Boston University com 4 publicações e foi seguida pela Tomsk State University (na Rússia) com 3 publicações.

Na análise dos autores mais produtivos, aparecem em destaque dois professores: Vitaliy Omelyanenko e Viktor Shevchuk. O professor Omelyanenko é pesquisador de economia política na Sumy State Pedagogical University na Ucrânia e aparece com 5 publicações. O professor Shevchuk é pesquisador de economia internacional, aparece com 4 publicações e é da Cracow University of Technology, na Polônia. Considerando as formações dos referidos professores, já se percebe que as publicações dificilmente apresentam foco em inteligência artificial ou *machine learning*, o que de fato pode ser confirmado pelos títulos dos estudos (Quadro 1).

Quadro 1 - Publicações dos dois pesquisados com o maior número de documentos recuperados.

Autor	Ano	Título	Periódico	DOI / URL de acesso
OMELYANENKO V	2019	Institutional strategies of system security of technological & innovation systems	BALTIC JOURNAL OF ECONOMIC STUDIES	10.30525/2256-0742/2019-5-1-150-159
OMELYANENKO V	2019	Security issues of system innovation strategies	SHS WEB OF CONFERENCES	10.1051/shsconf/20196503006
OMELYANENKO V	2018	National strategic innovation security conceptualization	TECHNOLOGY AUDIT AND PRODUCTION RESERVES	10.15587/2312-8372.2018.134242
OMELYANENKO V	2018	Research framework for system security of technological & innovation systems	BALTIC JOURNAL OF ECONOMIC STUDIES	10.30525/2256-0742/2018-4-1-248-254
OMELYANENKO V	2017	Economic diplomacy in the innovation global value chains as the national security providing strategy component	PATH OF SCIENCE	10.22178/pos.20-3
SHEVCHUK V	2021	Innovative optimization directions of investigative (detective) activity in modern conditions	THEORY AND PRACTICE OF FORENSIC SCIENCE AND CRIMINALISTICS	10.32353/khrife.2.2021.02
SHEVCHUK V	2021	Innovative principles of forensic support of law enforcement activity: issues of concept formation	THEORY AND PRACTICE OF FORENSIC SCIENCE AND CRIMINALISTICS	10.32353/khrife.1.2021.01
SHEVCHUK V	2021	Modern state and innovative directions of research of criminalistic technique	INTERCONF	10.51582/interconf.19-20.03.2021.021
SHEVCHUK V	2020	Forensic innovation: concepts, functions, tasks and research prospects	THEORY AND PRACTICE OF FORENSIC SCIENCE AND CRIMINALISTICS	10.32353/khrife.2.2020.02

Fonte: Dados da Pesquisa (2022).

[1] SSRN. Disponível em: https://www.ssrn.com/index.cfm/en/. Acesso em: 09 nov. 2022.

[2] arXiv. Disponível em: https://arxiv.org. Acesso em: 09 nov. 2022.

Após a remoção dos termos utilizados na pesquisa (*public security*, *public safety*, *national security*, *law enforcement*, *innovation*, *disruptive technology*, *public*, *security*, *disruptive*, *safety*, *artificial intelligence* e *machine learning*), foi gerada a nuvem de palavras com a frequência de ocorrência dos bigramas nos títulos (Figura 2), trigramas nos *abstracts* (Figura 3) e palavras chaves dos autores (

Figura 4).

Figura 2 - Bigramas nos títulos

Fonte: Dados da Pesquisa (2022).

Na análise dos bigramas dos títulos um destaque para as preocupações e temáticas: propriedade intelectual, justiça criminal, segurança cibernética, saúde, *smart cities*, economia digital e regulamentação.

Figura 3 - Trigramas nos abstracts

Fonte: Dados da Pesquisa (2022).

Nas análises dos trigramas dos abstracts (Figura 3), novamente destaque para algumas preocupações tais como departamentos de segurança pública, sistema de justiça, segurança nacional e economia internacional.

Figura 4 - Palavras chaves dos autores.

Fonte: Dados da Pesquisa (2022).

Na

Figura 4 é possível observar a preocupação com legislação (*regulation*, *innovation policy* e *law*) e o destaque de algumas tecnologias, por exemplo: *big data*, *internet of things* (IoT) e *blockchain*. Essas tecnologias também apareceram em destaque nos 24 documentos selecionados para leitura completa, conforme detalhado na próxima seção.

3.2 Corpus após *screening*

Este corpus contendo 24 documentos foi lido por completo e aponta-se:

a) três artigos que apresentam abstract e palavras-chaves em inglês estavam com o texto principal redigido em idiomas nos quais as autoras não possuem fluência: indonésio (Mustameer, 2022), ucraniano (Parshyn et al., 2020) e russo (Gnatik, 2021). Neste caso foi utilizado o tradutor DeepL para que a leitura pudesse ser realizada;

b) um artigo, ainda que tivesse elementos para o *screening* é, na verdade, um conjunto de slides de um trabalho apresentado em evento, na International Conference on Computer Science, Engineering and Education Applications (ICCSEEA) em 2019 (Buriachok & Sokolov, 2020);

c) dois documentos não apresentaram abstract. Um deles é semelhante a um editorial (Vardi, 2022) e outro simplesmente inicia na introdução (Robinson et al., 2021);

d) um documento é a revisão de um livro (Roessing, 2020) e também não apresenta abstract;

e) um relatório que avaliar a estratégia da China em se tornar referência em AI até 2030 que apresenta sumário executivo, mas não abstract e palavras-chaves (Kewalramani, 2018).

Apesar das mencionadas particularidades, todos os 24 documentos foram lidos e estão apresentados, discutidos e comparados na sequência.

O artigo "A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada" (Gaon & Stedman, 2019) é de 2019, com 30 páginas e descreve um compromisso do governo do Canadá em acelerar o crescimento do "setor de" inteligência artificial (AI) no país. Conforme mencionado, tal tecnologia emergente tem o "potencial para impacto em quase todos os segmentos da economia do Canadá, incluindo segurança nacional, assistência médica, e serviços governamentais". Algumas providências foram destacadas no âmbito da segurança nacional: no Ártico, por exemplo, o Canadá espera implantar "veículos submarinos autônomos para patrulhar e usar sistemas de AI que analisam sons submarinos a fim de se proteger contra intrusos em águas canadenses". Os autores ressaltam que a "AI só deve ser usada para ajudar os seres humanos na tomada de decisões relacionadas a questões de defesa nacional", mas a vigilância para que as AI não se torne autônomas deve ser constante. O documento menciona ainda a cibersegurança como preocupação e relembrou o ocorrido em 2016 quando se veiculou que o governo russo havia explorado a segurança cibernética dos EUA a fim de interferir na eleição daquele país. A sugestão é o uso de sistemas de AI em análises preditivas a fim de antecipar os ciberataques.

O artigo Activities of law enforcement agencies in the context of the introduction of innovative technologies (comparative legal aspect) (Tulinov et al., 2022) é de 2022 e objetiva apontar os mecanismos legais para o uso de tecnologias inovadoras na aplicação da lei e os principais problemas de sua implementação na luta contra o crime. O esquema metodológico do artigo foi o uso de métodos de pesquisa teórica e empírica, bem como comparativa, métodos estruturais e lógicos, análise documental e de sistemas. É estabelecido que os principais tipos de tecnologias modernas utilizadas na aplicação da lei são veículos aéreos não tripulados, inteligência artificial, robótica, biotecnologia, sistemas de informação analítica e geográfica, localizadores de explosão e chatbots. Os autores relembram as tecnologias apontadas no 14º Congresso da ONU sobre o Crime Prevenção e Justiça Criminal com riscos "criminogênicos" e destaca: criptomoedas pelo alto grau de anonimato de uso, o que leva ao financiamento do terrorismo e à lavagem de dinheiro sem impedimentos, mercado de drogas criado através da DarkNet, tráfico ilícito de armas e explosivos através do mercado de moedas criptográficas e da DarkNet, tráfico humano pelo uso dos canais de comunicação para encontrar vítimas e potenciais compradores de bens vivos, abuso e exploração de crianças pelo acesso descontrolado à tecnologia da informação, movimento ilegal de migrantes devido ao uso da tecnologia pelos infratores para estudar as rotas do serviço de fronteira (Nations, 2018). Os autores concluem que os sistemas jurídicos de inovação em diferentes países do mundo podem diferir um do outro por características diferentes e ter diferentes condições de uso legal e prático". E sugerem que se houvesse a introdução uniforme de aplicação de algumas leis em cada país do mundo, ajudaria a combater a criminalidade global no uso de alta tecnologia.

O artigo Artificial intelligence and machine learning: a perspective on integrated systems opportunities and challenges for multi-domain operations (Ravichandran et al., 2021) fornece uma perspectiva global sobre o histórico, inovação e aplicações da Inteligência Artificial e Aprendizagem de Máquina (ML), casos de sucessos e desafios de sistemas e interesses de segurança nacional. Os recentes interesses de segurança nacional em AI/ML têm se concentrado em problemas incluindo operações multidomínio (MDO) e destaca algumas aplicações de guerra: Air Combat Evolution (ACE) tem como objetivo testar um piloto de caça e algoritmos de aprendizagem para avaliar e criar desequilíbrio em jogos complexos tais como os Course Of Actions (COA) para combates. O objetivo para os COAs programados com AI é ajudar as equipes vermelhas a desenvolverem adversários criativos para o treinamento da força azul que, por sua vez, desenvolvem táticas de respostas aos ataques. A DARPA também explora programas de AI/ML para objetivos de missão de controle de rede integrada que informam como as comunicações estão sendo distribuídas na rede. Os autores concluem que a confluência e integração de tecnologias está iniciando tanto na teoria como na prática e os desafios técnicos incluem arquitetura e integração de sistemas, computação, comunicação, cibernética,

dados e representação, gerenciamento de incertezas, informação e tomada de decisões, validação e verificação e modelagem adversária.

Dentre os documentos recuperados está um relatório de 2018, China's quest for AI leadership: prospects and challenges (Kewalramani, 2018) com 30 páginas que avalia a estratégia adotada pelo governo da China em 2017, por meio de um plano para alçar o país como principal centro de inovação mundial de inteligência artificial (AI) até 2030 e apontou a AI como uma indústria estratégica, crucial para a melhoria da economia desenvolvimento, segurança nacional e governança. O relatório examina as peculiaridades do modelo econômico liderado pelo Estado do Partido, juntamente com a evolução geopolítica e falhas econômicas em relação ao comércio e à tecnologia. Além disso, avalia as políticas da China com relação a fatores como tecnologias centrais, pesquisa, de mão-de-obra, dados e o ambiente comercial, que são cruciais para garantir o desenvolvimento da indústria de AI. Conclui que considerando-se o tamanho do mercado chinês, a disponibilidade de capital para investimento, a força de trabalho cada vez mais instruída e com um espírito empreendedor, o fácil acesso a grandes quantidades de dados e um governo que se preocupa em nutrir e alavancar esses fatores é uma receita potente para fomentar inovação. No entanto, menciona que elementos estruturais (enfatizando quantidade em detrimento à qualidade e eficiência), geopolíticos e geoeconômicos são restrições que podem dificultar a busca da China por uma liderança global em AI. Inclusive o plano do Conselho de Estado de 2017 adverte sobre a necessidade de "minimizar os riscos, e garantir o desenvolvimento seguro, confiável e controlável da AI". Essencialmente, isto é uma extensão do dilema estabilidade versus crescimento que os sucessivos líderes chineses têm enfrentado ao longo das décadas.

O trabalho DARLENE: improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions (Apostolakis et al., 2022) apresenta a relação entre realidade aumentada (RA) e a inteligência artificial (AI) com destaque para aplicações em segurança pública nas operações cotidianas de vigilância e perícia. Os autores apresentam o sistema DARLENE, em desenvolvimento na Grécia, com verba da Comunidade Européia e combina hardware e software para "visa preencher as lacunas existentes na aplicação das tecnologias de AR e AI para rápida tomada de decisão tática in situ com margem de erro mínima". O sistema DARLENE incorpora técnicas de AI de visão computacional, tais como reconhecimento de atividades e estimativa, além de, por meio da estrutura de AR predizer conteúdo dinâmico de acordo com nível de estresse e contexto de cada indivíduo. A estrutura foi testada em oficinas de co-criação e em situações simuladas e a avaliação da tomada de decisão foi realizada por especialistas humanos. Como resultados são apontados que os usuários-alvo são positivos para a adoção da solução proposta nas operações de campo, e que o mecanismo de tomada de decisão produz resultados "altamente aceitáveis".

O artigo Data-intensive innovation and the state: evidence from ai firms in China (Beraja et al., 2022) reúne dados sobre empresas e contratos de compras de vídeos de segurança pública na indústria chinesa de reconhecimento facial por meio de AI. Os autores identificaram que contratos "ricos em dados", comparados com "contratos escassos em dados", levam as empresas receptoras a desenvolverem software de AI com maior relevância e retorno financeiro. As conclusões do estudo apontam que o fornecimento de dados governamentais às empresas chinesas de AI que servem o Estado contribuíram para sua ascensão como líderes globais em tecnologias de reconhecimento facial.

O trabalho Digital evidence in *fog computing* systems (Hegarty & Taylor, 2021) foi recuperado em quatro bases de dados pesquisadas (Dimensions, Science Direct, Scopus e Web Of Science) e inicia com a utilidade de Fog Computing ou computação em nevoeiro: saúde personalizada, cidades inteligentes, veículos automatizados e Indústria 4.0. Segundo os autores, o termo computação em nevoeiro foi introduzido em 2012 pela Cisco para infraestruturas de nuvens dispersas e permite lidar com um grande número de dispositivos de Internet das Coisas e grandes volumes de dados para aplicações em tempo real. A fim de investigar os desafios forenses colocados pela computação de nevoeiro foi implantado um protótipo de sistema de nevoeiro que reúne dados ambientais de sensores IoT em um ambiente controlado na Inglaterra. Quanto maior a complexidade dos

sistemas, tais como casas inteligentes, maior o número de dispositivos e, consequentemente, mais complexo o sistema de computação de nevoeiro com a demanda de mais tempo e esforço para buscar evidências. A natureza dos dados e o processamento usado para inferir e deduzir informações exigirá uma mudança de etapa na cooperação entre os provedores e a aplicação da lei, acompanhada de treinamento adicional para capacitar os investigadores a compreender os conceitos por trás dos poderosos motores de inferência empregados no domínio da neblina. Aliado às dificuldades tecnológicas, o aumento das restrições de portabilidade de dados no General Data Protection Regulation (GDPR), equivalente à lei Geral de Proteção de Dados (LGPD) no Brasil, reforçou a exigência de trilhas de auditoria e o direito ao esquecimento nos sistemas de computação de nevoeiro e já é considerado um novo problema para investigações forenses computadorizadas.

Na mesma linha do anterior, o trabalho Digital innovations and smart solutions for society and economy: pros and cons (Sikorski, 2021) destaca que os desenvolvimentos recentes na inteligência artificial (AI) apresentam ameaças significativas à privacidade de dados pessoais, à segurança nacional e à estabilidade social e econômica. O artigo, escrito na Polônia, registra preocupações com as lacunas jurídicas e a falta de gestão e supervisão adequados no desenvolvimento e operação de produtos baseados em AI. Desta forma, a pesquisa reúne vários danos potenciais no uso irresponsável da AI em diversas categorias, das quais aqui se destaca a de defesa e segurança: acessar informações sigilosas, atacar infraestrutura crítica e centros de comando nacionais, ultrapassar o controle, imitando os operadores humanos, gerar pânico, provocando conflitos que afetam a segurança nacional e criar robôs controlados por inteligência artificial incapacitando a segurança nacional. O documento conclui com a análise e discussão das mudanças nos ambientes comercial, legal e institucional necessárias para garantir ao público que as soluções baseadas em AI possam ser confiáveis, sejam transparentes e seguras, e possam melhorar a qualidade de vida.

O documento Disruptive technologies in smart cities: a survey on current trends and challenges (Radu, 2020) explora as "tecnologias disruptivas mais importantes para o desenvolvimento da cidade inteligente". A autora romena aponta que cada cidade inteligente é um sistema "dinâmico e complexo que atrai um número crescente de pessoas em busca dos benefícios da urbanização" e que as Nações Unidas estimam que 68% da população mundial estará vivendo em cidades até 2050, criando desafios relacionados a recursos e infraestrutura limitados (energia, água, sistema de transporte etc.). Para resolver estes problemas, são criadas tecnologias novas e emergentes tais como: Internet das Coisas, *big data*, cadeia de bloqueio, inteligência artificial, análise de dados e aprendizagem de máquina e cognitiva são apenas alguns exemplos. O documento é uma revisão abrangente de literatura que identifica as principais tecnologias disruptivas nas cidades inteligentes. Nas conclusões a autora destaca: IoT, *big data*, AI e *blockchain* como as tecnologias disruptivas mais significativas para a evolução das cidades inteligentes.

O artigo Emerging technologies and national security: the impact of iot in critical infrastructures protection and defence sector (Pătraşcu, 2021) inicia com menção à dependência da sociedade às facilidades oferecidas pelas tecnologias emergentes tais como proteção das infraestruturas que garantem a disponibilidade de bens e serviços essenciais. O autor romeno destaca a AI, Internet das Coisas, *big data*, robôs, drones, *cloud computing*, *blockchain*, computação quântica, 5G, impressão 3D e machine learning como "soluções viáveis para a dinâmica e otimização do ambiente em que eles são integrados". O estudo aborda o uso destas tecnologias no setor de defesa e segurança nacional e finaliza mencionando que "a arquitetura de sistemas e redes militares poderia desempenhar um papel crítico no desafio de segurança da Internet sem fio" e que a adoção de IoTs no setor de defesa e infraestrutura crítica deve considerar os riscos de segurança associados para que os ciberataques não sejam uma ameaça à segurança nacional".

O trabalho Estonia: a curious and cautious approach to artificial intelligence and national security (Robinson et al., 2021) discorre sobre o plano do governo estoniano de utilizar a inteligência artificial (AI) para julgar pequenas disputas em tribunal, veiculado pela mídia como o "juiz robô", mas também destaca o papel pioneiro da Estônia na governança digital e na cibersegurança por meio de estudos de casos e desenvolvimento do setor público, tanto na indústria quanto nas forças armadas,

este último no contexto de segurança nacional. As Forças de Defesa da Estônia (EDF) utilizam tecnologias habilitadas para AI e diversos sistemas autônomos tais como: veículos aéreos não tripulados (UAVS), sistema de reconhecimento de vigilância terrestre e um sistema de contra-ataque de curto alcance de superfície para mísseis ar, dentre outros. A análise mostrou que a Estônia está "ansiosa para desenvolver soluções nacionais - assim como para alimentar a próxima geração de especialistas em AI - a fim de enfrentar a demanda futura, tanto no setor privado quanto no público".

O documento Geospatial artificial intelligence for early detection of forest and land fires (Purbahapsari & Batoarung, 2022) retrata uma realidade encontrada na Indonésia que utiliza um sistema de predição e detecção automática de incêndios florestais por meio de dados de imagens de satélite fornecidos pelo Nacional de Aeronáutica e Espaço (LAPAN). Os autores mencionam que os resultados são promissores, mas apontam diversas deficiências, principalmente na diferenciação de superfícies quentes de incêndios florestais. Os autores citam que o Ministério do Meio Ambiente e Silvicultura (DGLE MoEF) tem adotado uma abordagem chamada Inteligência Artificial Geospacial (GeoAI) que utiliza dados de imagens de satélites gravadas de 2017 – 2019 para treinamento para reconhecer o padrão e o tom da imagem nas áreas queimadas. Os testes demonstraram que os dados da área queimada processados pelo GeoAI têm melhor precisão do que a contagem de pontos de acesso (*hotspots*) para identificação de florestas e incêndios terrestres. Com vantagem é apontado o aumento da "eficácia e eficiência dos recursos alocados pelos agentes da lei na prestação de serviços públicos melhores e mais ágeis".

O documento Implementation of active learning in the master's program on cybersecurity (Buriachok & Sokolov, 2020) não é um artigo no formato tradicional, mas uma publicação em evento na ICCSEEA 2019 sobre a experiência na oferta de um programa de mestrado em cibersegurança na Ucrânia que utiliza aprendizagem ativa. O documento é um conjunto de slides que resume os trabalhos desenvolvidos pelos discentes do programa, por exemplo: sistema de recomendação de segurança para wi-fi e desenvolvimento de hardware e interface para monitoramento de sistemas sem fio. Aos autores registram na conclusão que aprendizagem ativa permite: conhecer e comparar as normas internacionais dos programas educacionais cibernéticos de segurança, para preparar a tradução da atual versão da norma de segurança da Ucrânia, melhorar o nível de segurança cibernética do estudante e aumentar a competência dos especialistas em cibersegurança e segurança da informação.

Um dos mais relevantes documentos recuperados é o estudo Leveraging deep learning and iot *big data* analytics to support the smart cities development: review and future directions (Ben et al., 2020) que em 29 páginas, 213 referências, escrita de fácil compreensão e diversas ilustrações aborda aspectos de aplicações de Deep Learning (DL) em IoT no contexto de cidades inteligentes. O artigo de abrangência mundial escrito por autores, de laboratórios da Tunísia e Arábia Saudita, iniciam mencionando o rápido crescimento das populações urbanas em todo o mundo que impõe novos desafios à vida cotidiana dos cidadãos, incluindo poluição ambiental, segurança pública, congestionamento rodoviário etc. Na sequência apontam que novas tecnologias foram desenvolvidas para administrar este rápido crescimento por meio do desenvolvimento de cidades mais inteligentes. O trabalho fornece uma revisão da literatura a respeito do uso da IoT e da DL para desenvolver cidades inteligentes. Algumas das tecnologias abordadas são: computação em nuvem, computação em neblina, computação de ponta, *blockchain*, 5G e 6G em aplicações inteligentes na cidade, incluindo casa, saúde, transporte, vigilância, agricultura e meio ambiente. Os autores apresentam ainda as arquiteturas DL populares e seus usos, benefícios, e inconvenientes, as principais plataformas de código aberto desenvolvidas para apoiar as pesquisas em DL e ainda compilam – em uma tabela, diversos *datasets* de DL comumente usados. Concluem com destaque para os desafios e questões abertas para aplicação de DL em IoT com foco em *smart cities*.

O artigo 'New normality' of the Covid-19 era: opportunities, limitations, risks (Gnatik, 2021) está escrito em russo aborda o avanço no desenvolvimento das tecnologias NBIC (Nano, Bio, Novas Tecnologias de Informação e Cognitivas). O autor aponta desenvolvimento sem precedentes dos sistemas de inteligência artificial, tecnologias de vigilância por vídeo, geolocalização e *big data* em tempos de Covid-19 que, em tempo excepcionalmente curto, trouxe problemas existenciais e legais para o mundo todo. O artigo apresenta preocupação que a proclamada ameaça à saúde pública tenha se tornado uma justificativa

para a "introdução de inovações sérias que permitem às elites dirigentes bloquear os direitos civis, em particular, legalizar o uso de sistemas de rastreamento". O artigo enfatiza que a digitalização da aparência e a coleta de informações sobre cidadãos permite criar um gigantesco *dataset*, cujo uso pode ter imprevisíveis consequências, e o problema de seu uso não autorizado não é o principal. Conclui que o poder de algoritmos, que permitem manipular uma pessoa por meio de informações coletadas continuamente sobre ele, "pode se transformar em uma nova e sofisticada forma de genocídio" e que a comunidade científica deveria iniciar uma ampla discussão social e científica, para corrigir o curso de ação, para "limitar as exigências do aparelho estatal coercitivo e para retardar a política de restrição dos direitos fundamentais dos cidadãos".

O documento Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0 (Mustameer, 2022) está escrito em indonésio e, em tradução automática significa "Aplicação da legislação nacional e internacional contra crimes de espionagem cibernética na era da sociedade 5.0". Explica a era da Sociedade 5.0 como uma condição da sociedade que "necessária para resolver vários desafios e problemas sociais, utilizando várias inovações que nasceram na era da Revolução Industrial 4.0, tais como a Internet das Coisas, *big data*, Inteligência Artificial e robôs para melhorar a qualidade da vida humana" e aponta a Espionagem Cibernética como um dos crimes aos quais o Estado é vulnerável, definindo-o como "um ato de espionagem que se aproveita dos avanços da tecnologia e da informação". O estudo apresenta pesquisa jurídica normativa com três abordagens, abordagem conceitual, abordagem estatutária e abordagem comparativa e os resultados apontam que os instrumentos legais nacionais na Indonésia ainda estão limitados à Lei de Informação Eletrônica e Transação (ITE), aos Regulamentos Governamentais sobre sua implementação, aos Regulamentos Presidenciais sobre Defesa Nacional (Perpreshanneg) e à ausência de políticas que regulamentem especificamente os crimes cibernéticos. Concluem apresentando preocupação com a ciberespionagem que ameaça a estabilidade da defesa e da segurança dos países do mundo e ainda é uma oportunidade para os perpetradores realizarem suas ações, especialmente para "países que têm baixa segurança digital e experimentam um vácuo legal em relação às atividades de Espionagem Cibernética em tempo de paz".

O relatório Proposed EU AI act - Presidency compromise text: select overview and comment on the changes to the proposed regulation (Kazim et al., 2022) resume e comenta o "Presidency compromise text" (Union, 2021), uma versão revisada da proposta de lei que reflete a consulta e deliberação pelos estados membros e atores (novembro de 2021). Com a proposta de Lei de Inteligência Artificial da União Européia existe a aspiração dessa em liderar o mundo na regulamentação da AI (abril de 2021). Os principais comentários se concentram em isenções / lacunas da lei com respeito à segurança nacional; mudanças que procuram proteger ainda mais a pesquisa, o desenvolvimento e a inovação; e a tentativa de esclarecer a posição do projeto de legislação sobre manipulação algorítmica. Alguns pontos de atenção estão relacionados aos riscos potenciais para os cidadãos e suas liberdades pelo uso de AI não controlada, tais como tecnologias de reconhecimento facial (FRT).

O trabalho Robust end-user-driven social media monitoring for law enforcement and emergency monitoring (Kirsch et al., 2018) discute as mídias sociais tais como o Twitter como fonte de informação em caso de emergências e situações de crise. Os autores apresentam uma estrutura de monitoramento e análise das mídias sociais que fornece suporte à segurança e está baseado em dois projetos da área de policiamento comunitário e resposta a emergências: Citizen Interaction Technologies Yield Community Policing (CITYCoP) e Evolution of Emergency Copernicus (E2MC). O primeiro visa desenvolver aplicações que facilitem o policiamento comunitário por meio de mineração de mídias sociais para avaliar a qualidade percebida pelos cidadãos e o segundo fornece um alerta precoce e serviços de resposta rápido em caso de emergências. Para os testes foram utilizados três *datasets* de tweets relacionados a três eventos de crise: a inundação em Alberta em 2013, os bombardeios em Boston durante e após a maratona em abril de 2013 e a explosão nas instalações de armazenamento e distribuição da West Fertilizer Company, no Texas, em abril de 2013. O sistema proposto monitora e analisa os fluxos da mídia social, pode ser configurado pelo usuário final e utiliza tecnologia de mineração de texto por meio de rede neural convolucional para detecção de sentimentos e uma extensão da rede neural latente para identificar tópicos relevantes nos tweets.

Uma análise do uso de AI para auxiliar no controle do crime no Paquistão é apresentado no artigo Role of artificial intelligence in eradicating: how artificial intelligence can help to control crime and terror in Pakistan (Rashid & Fatima, 2020). Segundo os autores, apesar do Paquistão ser um país de terceiro mundo e estar atrasado em alguns pontos quando comparado ao restante do mundo, possui diversos especialistas em tecnologia e é um país com uma das maiores populações jovens do mundo, adepta ao uso de tecnologias. Ainda assim, o país figura entre os mais baixos em inovações tecnológicas (posição 105 de 129) e apesar de coletar muitos dados de seus cidadãos, não tem potencial para utiliza-los. O presidente Dr. Arif Alvi escreveu um artigo mencionando que o país não estaria aproveitando a inteligência artificial e disse que a qualidade dos graduados em engenharia de software não estava à altura das necessidades do país, enquanto que a Índia ocupava a terceira posição em termos de qualidade de pesquisa. Por este motivo, iniciou a "Presidential Initiative for Artificial Intelligence and Computing" com o objetivo de remodelar o país por meio da educação, pesquisa e negócios e oferece quatro programas: Inteligência Artificial; Cloud Native e Web Mobile; Blockchain; e Internet das coisas e AI. Em 2020 já eram 21 universidades oferecendo cursos de graduação em AI e todas ligadas à indústria de TI e aos departamentos de segurança do governo. Os autores concluem que o Paquistão é um país com uma alta taxa de criminalidade e terror e "precisa aproveitar ao máximo a AI para erradicar a criminalidade e o terror no país".

O trabalho desenvolvido por pesquisadores da Inglaterra, mas sem limitação territorial, The rise of technology in crime prevention: opportunities, challenges and practitioners perspectives (Anderez et al., 2021) inicia com a frase "A atividade criminosa é uma questão predominante na cultura e na sociedade contemporânea, com a maioria das nações enfrentando níveis inaceitáveis de criminalidade". Na sequência afirma que a inovação tecnológica é essencial para a melhoria das estratégias de controle e prevenção do crime como por exemplo: rastreamento e identificação por GPS, vigilância por vídeo etc. e os autores propõe analisar a recente inovação tecnológica, dentre as quais destacam Internet das Coisas (IoT), machine learning e *edge computing*, na prevenção do crime. Algumas aplicações das tecnologias são citadas como de uso comum, por exemplo as várias aplicações para relatar situações de emergência e coletar evidências dessas situações ou cenários de detecção de violência em ambientes domésticos ou de trabalho por áudio ou câmeras de CFTV. No entanto, os autores apontam que a combinação de tecnologias, "pode ser de grande utilidade para identificar cenários violentos, o que pode levar a prevenção de outras ocorrências e, portanto, à prevenção final da atividade criminosa", mas alertam que não haverá solução única que resolva todas as ocorrências pela "heterogeneidade dos infratores, das vítimas, dos contextos de ofensa e dos padrões ofensivos".

O trabalho, escrito em ucraniano, Use of the information technologies at the international level of public communications (Parshyn et al., 2020) aborda o uso das tecnologias da informação nas diversas atividades de governo da Ucrânia com prioridade para análises de *big data*, inteligência artificial, *cloud computing*, internet das coisas, 5G, sistemas autônomos e realidade virtual e aumentada, chatbots, localizadores de tiros e análise de criminalidade. No contexto do último, aborda o sistema de previsão do crime, chamado de National Data Analysis Solution (NDAS) que utiliza uma combinação de AI e estatísticas para a análise de 1,4 mil características para identificar "possíveis" criminosos. Os algoritmos de AI calculam os riscos e avaliam a probabilidade de uma determinada pessoa cometer um crime com o uso de armas. O dataset de treinamento foi criado por um grupo de especialistas que reuniu mais de um terabyte de dados de bases de dados policiais, incluindo registros de detentos e pessoas procuradas (mais de 5 milhões pessoas), registros criminais, perfis e outros. Os autores concluem mencionando que uma estratégia de criar um espaço único de informação de nível internacional viabilizaria a "tomada de decisões eficazes em um novo nível".

O documento Voluntary safety commitments provide an escape from over-regulation in AI development (Anh et al., 2022) trata da demanda por governança e regulamentação decorrente da introdução da Inteligência Artificial (AI) e tecnologias relacionadas no cotidiano das sociedades. Os autores mencionam que o medo e a ansiedade sobre um possível mau uso, bem como os preconceitos inerentes desde a sua criação podem asfixiar seu desenvolvimento e reduzir os benefícios que poderiam

ser gerados. O documento procura demonstrar como compromissos globais (entre países) voluntários, mas sancionáveis, geram resultados socialmente benéficos em todos os cenários previstos em relação à tecnologia da AI.

No documento Will AI destroy education (Vardi, 2022) o autor, em apenas uma página, apresenta uma importante preocupação relacionada Lei da Iniciativa Nacional de AI tornou-se lei nos Estados Unidos em 1º de janeiro de 2021 com o objetivo de "acelerar a pesquisa e aplicação da AI para a prosperidade econômica e segurança nacional da Nação". Em outono de 2011, aproximadamente 450.000 estudantes se inscreveram em três cursos de ciências da computação oferecidos pela Universidade de Stanford, lançando os Massive Open Online Courses (MOOC). O autor relembra que a disponibilidade de cursos acadêmicos gratuitos ou quase gratuitos é benéfica para os estudantes, mas que tais programas baseados nos MOOCs obtêm lucros nominais apenas "ignorando o verdadeiro custo da mão-de-obra docente envolvida na produção e administração dos MOOCs". A Fundação Nacional de Ciência dos EUA lançou em 2020 vários Institutos de Pesquisa de AI para impulsionar as fronteiras da inteligência artificial e um dos temas desta iniciativa de pesquisa é "AI-Augmented Learning" (Aprendizagem Avançada da AI) com a premissa de que "inovações impulsionadas pela AI melhoram radicalmente a aprendizagem e educação humana". O autor conclui apontando que o sistema educacional é um dos "tesouros da civilização humana" e que a aplicação da atitude de "inovação disruptiva" à educação "corre o risco de causar enormes danos".

Finalmente o documento com o título Disruptive and game changing technologies in modern warfare, development, use, and proliferation (Roessing, 2020) é, na verdade, a introdução do livro editado pela Springer em 2020 com 222 páginas. A obra aborda o papel da tecnologia disruptiva para a segurança nacional e controle de armas. Segundo a autora, trata-se de uma obra voltada para pesquisadores de "relações internacionais interessados nas características tecnológicas das inovações com relevância presente e futura para as capacidades militares, e na arquitetura da segurança internacional". Os temas abordados no livro são: o ambiente estratégico em mudança no qual as operações de segurança são planejadas e conduzidas; sua importância para o planejamento da política científica e tecnológica atual e exercícios preditivos de como a ciência e a tecnologia poderiam contribuir para as escolhas estratégicas interesses dos Estados Unidos em um futuro próximo a médio prazo. Os capítulos individuais apresentam temas diversos, dentre os quais destacam-se aqui os vinculados à análise de dados, machine learning e tecnologia disruptiva: machine learning in the countering weapons of mass destruction fight, attempting to predict the proliferation of lethal autonomous weapons systems: a statistical analysis e protecting army aviation and enabling military dominance through disruptive innovation, dentre outros capítulos. O livro é um ponto de partida informativo para os interessados no papel das tecnologias emergentes para a capacidade militar dos EUA.

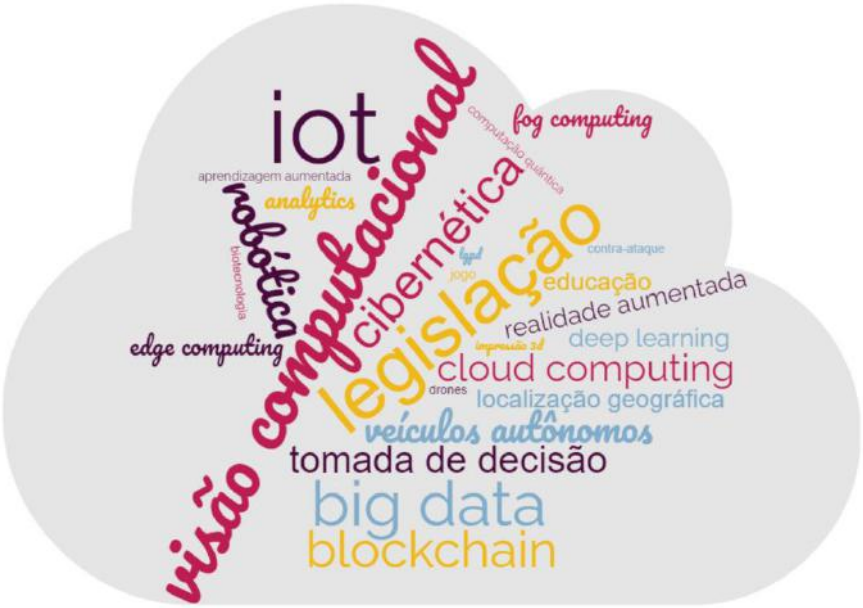
Em uma análise global dos 24 documentos, são 21 (87,5%) em inglês e um russo, um indonésio e um ucraniano (12,5%). Do total, seis abordam o tema de forma global, dois estão com foco na China, dois na Indonésia, dois na Romênia, dois na Ucrânia e dois nos Estados Unidos. Os demais estão distribuídos em: Canadá, Grécia, Inglaterra, Polônia, Estônia, Rússia, Paquistão e legislação da União Européia.

As principais preocupações apontadas nos trabalhos foram: cibersegurança com o uso da darknet para atividades criminosas e privacidade de dados com foco nas lacunas jurídicas. O receio com o mau uso de dados e informações sobre os cidadãos seja por dados demográficos ou imagens, parece em diversos trabalhos.

Todos os trabalhos abordavam aplicações na área de defesa e segurança nacional ou educação e dois destes mencionaram a pandemia Covid-19 (Gnatik, 2021; Kirsch et al., 2018).

Após as análises de conteúdo anteriormente apresentada, foi gerada a nuvem de palavras com os termos que melhor caracterizaram os estudos, conforme Figura 5.

Figura 5 - Nuvem de palavras gerada a partir da análise de conteúdo.



Fonte: Dados da Pesquisa (2022)

A preocupação com legislação ocorreu explicitamente em três trabalhos, ainda que esteja registrada na maioria dos estudos. As áreas que aparecem em destaque são: robótica e cibernética, visão computacional, *cloud computing*, *big data*, IoT e *blockchain*.

Por meio da aplicação do processo de análise das terminologias utilizadas dentro do corpus por meio de técnicas de Processamento de Linguagem Natural aplicadas sobre os textos dos documentos do corpus, conforme **Erro! Fonte de referência não encontrada.**, foram extraídos 3.634 termos com pelo menos duas ocorrências em 23 dos 24 documentos recuperados. O trabalho Implementation of active learning in the master's program on cybersecurity (Buriachok & Sokolov, 2020) não foi utilizado nesta etapa por se tratar de um conjunto de slides e de três artigos (Gnatik, 2021; Mustameer, 2022; Parshyn et al., 2020) foram utilizados apenas os títulos, resumos e palavras-chaves, uma vez que estavam em russo, indonésio e ucraniano.

Dentre os termos com maior ocorrência, apareceram com mais de 100 ocorrências: *artificial intelligence* (AI) (749), *use* (204), *development* (200), *technology* (197), *information* (181), *order* (163), *time* (155), *applications* (147), *results* (129), *system* (129), *machine learning* (ML) (119), *research* (118), *data* (115), *challenges* (109), *innovation* (106), *security* (105), *devices* (102) e *access* (101). Estes termos *per si* não acrescentam conhecimento à análise. Por este motivo, após remoção manual dos termos pouco significativos, restaram os 30 com maior ocorrência que estão apresentados na Figura 6. O termo com maior ocorrência foi China (128), seguido de *fog computing* (80), IoT (70), Canada (55) e Estonia (55). No entanto, como existe a contagem dentro de um mesmo documento, o termo Estonia, por exemplo, ocorreu 55 vezes dentro do mesmo artigo sobre este país (Robinson et al., 2021).

As cinco tecnologias que aparecem em destaque são: *fog computing* (80), IoT (70), *blockchain* (39), *edge computing* (21) e *big data* (20). Os métodos que deep learning que aparecem em destaque são: CNN (52) e LSTM (36) (Figura 6).

Figura 6 - Nuvem de palavras gerada a partir da análise de extração automática de termos por NLP.

Fonte: Dados da Pesquisa (2022).

Combinados os resultados da análise de conteúdo, análise de extração automática de termos por NLP e os termos que mais ocorreram nas métricas da base completa, a próxima seção verifica a análise de tendência de pesquisas para os termos *big data*, *internet of things* (IoT) e *blockchain*.

3.3 Análise de crescimento dos termos

Para análise de tendências dos termos foi utilizada a base de trabalhos acadêmicos de acesso aberto lens.org, no dia 17 de novembro de 2022 com a restrição de período de 2012-2022.

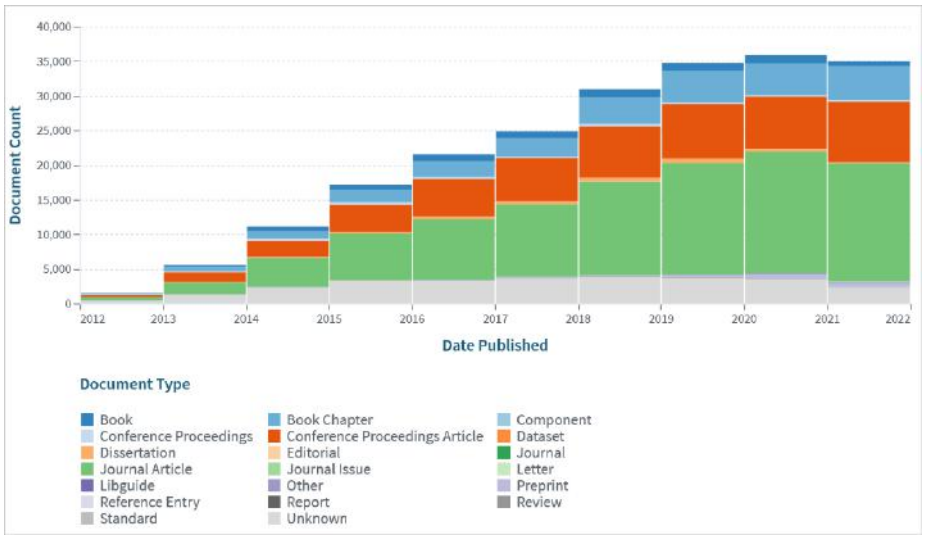
Para o termo "*big data*" a plataforma retornou 218.043 trabalhos acadêmicos e apresenta crescimento constante até 2021 (Gráfico 3) e leve redução em 2022, mas considerando que o ano de 2022 ainda não finalizou e algumas publicações de 2022 acabam sendo registradas ainda no início de 2023, existe a expectativa de contínuo crescimento e interesse no tema. Dentre os tipos de documentos, dois aparecem em destaque: artigos em periódicos e anais de conferências, comprovando a atualidade do tema pela menor publicação em livros. Dentre os 100 principais pesquisadores, a maioria (mais de 95%) são chineses. O professor italiano Alfredo Cuzzocrea, da Universidade de Calabria, é uma das poucas exceções e aparece com 187 publicações, na sexta colocação.

O país que aparece com o maior número de produções é a China (38.757), seguida de Estados Unidos (31.755), Inglaterra (15.171), Austrália (6.211) e Índia (6.120).

As 5 principais editoras que publicam o tema são: IEEE (47.550), Springer (26.588), Elsevier (12.837), ACM (5.157) e Wiley (3.560), um total de 95.692 (43,89%) do total recuperado (218.043). Aqui é importante observar que estão sendo contadas todos os periódicos destas editoras e a IEEE publica diversos anais de conferências, incluindo um dos principais eventos internacionais da área, a IEEE International Conference on Big Data (Big Data)[3] que ocorre desde 2013.

[3] IEEE International Conference on Big Data. Disponível em: https://bigdataieee.org. Acesso em: 17 nov. 2022.

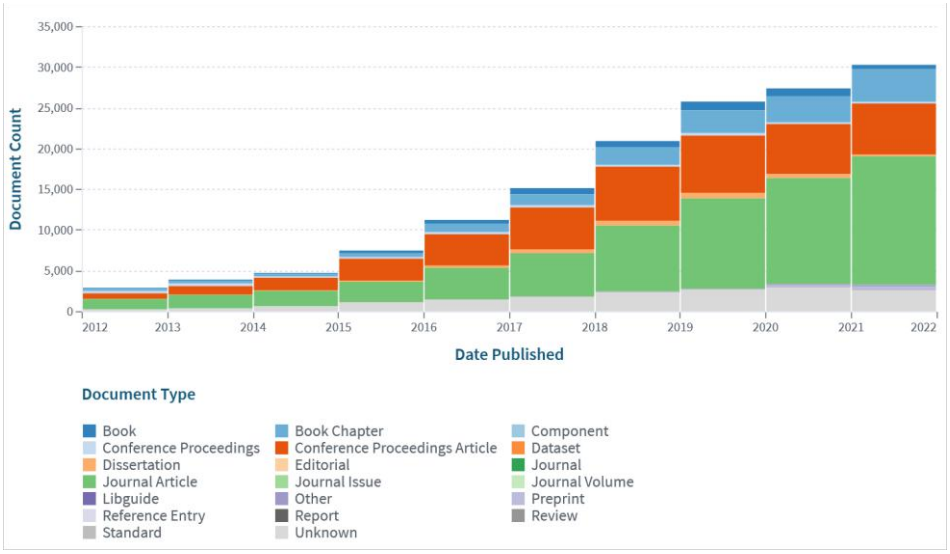
Gráfico 3 - Crescimento das pesquisas em "big data" (2012-2022).



Fonte: Dados da Pesquisa (2022).

Para o termo "*internet of things*" a plataforma retornou 149.385 trabalhos acadêmicos e apresenta crescimento constante até 2022 (Gráfico 4) mesmo sem a finalização deste ano. Dentre os tipos de documentos, novamente dois aparecem em destaque: artigos em periódicos e anais de conferências, comprovando a atualidade do tema pela menor publicação em livros, ainda que apareçam diversos capítulos de livros publicando o assunto.

Gráfico 4 - Crescimento das pesquisas em "internet of things" (2012-2022).



Fonte: Dados da Pesquisa (2022).

O principal pesquisador, professor Mohsen Guizani, da Universidade do Qatar aparece com 254 publicações, seguido pelo professor Wei Wang da Huazhong University of Science and Technology com 195 documentos. Na terceira posição aparece o professor Joel J. P. Coelho Rodrigues da Universidade Federal do Piauí, e um expoente mundial na área inclusive já tendo

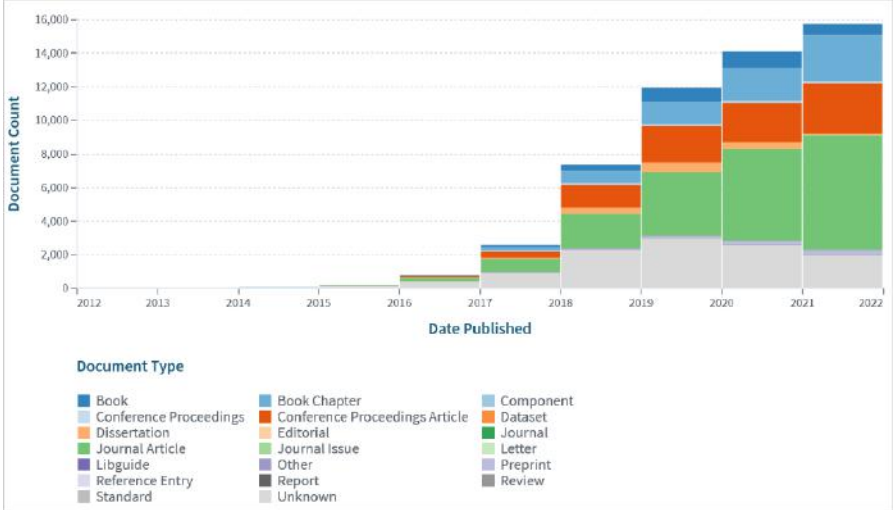
recebido o grau de Fellow do IEEE em 2020 pela comprovada qualidade das pesquisas e mais de 33 mil citações[4] conhecidas na literatura além de reconhecido serviço à comunidade.

Quando considerados os países mais produtivos aparecem nas 5 primeiras colocações: China (23.654), Estados Unidos (15.225), Inglaterra (8.771), Índia (8.272) e República da Coréia (3.894).

As 5 principais editoras que publicam o tema são: IEEE (50.085), Springer (16.440), Elsevier (6.193), ACM (3.836) e MDPI (2.870), um total de 79.424 (79,42%) do total recuperado (149.385).

Finalmente a análise do termo "*blockchain*" retornou 52.631 trabalhos acadêmicos. O Gráfico 5 apresenta o retorno ao longo do período pesquisado, mas percebe-se que até 2015, o número publicações anuais foi inferior a 50 e o crescimento passa a ser constante a partir deste ano. Aqui novamente em 2022 já se registra aumento de publicações em relação ao ano de 2021, ainda que falte um pouco mais e um mês para o término de 2022.

Gráfico 5 - Crescimento das pesquisas em "blockchain" (2012-2022).



Fonte: Dados da Pesquisa (2022).

O autor com maior número de publicações (122) é o professor Neeraj Kumar do Thapar Institute of Engineering and Technology, na Índia. O professor Khaled Salah da Khalifa University of Science and Technology, de Abu Dhabi nos Emirados Árabes Unidos, aparece com 199 publicações seguido pelo professor Dusit (Tao) Niyato da Nanyang Technological University (NTU), a maior universidade de pesquisa de Singapura, com 102 publicações. Ainda assim, na análise de produtividade por países, a China (5.752) aparece em primeiro, seguida pelos Estados Unidos (5.087), Inglaterra (2.425), Índia (2.041) e Austrália (1.353).

4. Considerações Finais

Conforme mencionado na introdução, o Anuário de Segurança Pública 2022 (Bueno & Lima, 2022) apresenta estatísticas preocupantes para o Brasil, tais como apresentar 2,7% dos habitantes do planeta e 20,4% dos homicídios com vítimas sendo caracterizadas por 77,9% negras, 50% entre 12 e 29 anos e 91,3% do sexo masculino. Os crimes de violência sexual tiveram aumento de 4,2% em 2021 que, nominalmente pode parecer um número pequeno, mas somaram absurdos 66.020

[4] Rodrigues, J. J. P. (2022). Citações no Google Acadêmico. https://scholar.google.com.br/citations?user=97WutEsAAAAJ&hl=pt-BR&oi=ao. Acesso em: 17 nov. 2022.

estupros com 75,5% das vítimas incapazes de consentir, 61,3% até 13 anos e em 79,6% dos casos o autor era conhecido da vítima. Um ponto de atenção registrado foi o fato da palavra inteligência ter 5 ocorrências e nenhuma das ocorrências apontar como ou quais tipos de inteligências estão em efetivo uso no país.

Desta forma, esta pesquisa que foi conduzida de forma integrativa em bases de dados de periódicos (IEEE Xplore, Science Direct, Web of Science, Scopus e Dimensions) e outros mecanismos de busca como o Google Acadêmico para complementação de dados sobre os pesquisadores e publicações, aponta quais e para qual propósito as tecnologias disruptivas, com foco na inteligência artificial estão sendo adotadas e pesquisadas no mundo.

A primeira análise, conduzida sobre o corpus com 790 documentos, aponta uma preferência dos autores pelos repositórios preprints, a saber: o SRRN Electronic Journal aparece com ampla vantagem com 110 (13,92%) das 790 produções recuperadas e o ARXIV aparece em segundo lugar com 9 (1,14%) do total recuperado. Neste corpus, o país que apareceu como maior número de produções foram os Estados Unidos (10), seguido pela Ucrânica (7), Nigéria (6), Rússia (4) e Aústria e Grécia (ambos com 3 publicações cada). Dentre as universidades o destaque ficou para a Boston University com 4 publicações e foi seguida pela Tomsk State University (na Rússia) com 3 publicações.

Na análise dos autores mais produtivos, aparecem em destaque dois professores: Vitaliy Omelyanenko e Viktor Shevchuk. O professor Omelyanenko é pesquisador de economia política na Sumy State Pedagogical University na Ucrânia e aparece com cinco publicações. O professor Shevchuk é pesquisador da área de economia internacional, aparece com quatro publicações e é da Cracow University of Technology, na Polônia. A preocupação com legislação (regulation, innovation policy e law) e o destaque de algumas tecnologias, por exemplo: big data, internet of things (IoT) e blockchain aparece na análise das palavras-chaves utilizadas pelos autores.

Na segunda análise, no corpus de 24 documentos após o screening do corpus anterior, destaque para o trabalho Leveraging deep learning and iot big data analytics to support the smart cities development: review and future directions (Ben et al., 2020), ponto de partida para outros pesquisadores interessados tanto em deep learning e internet of things aplicados as smart cities quanto apenas nas duas tecnologias.

Ainda na segunda análise, diversas aplicações com diversas tecnologias apareceram nos estudos: veículos autônomos, drones, robótica, cibernética, biotecnologia, localização geográfica, tomada de decisão, realidade aumentada, visão computacional, fog computing, cloud computing, edge computing, computação quântica, deep learning e aprendizagem aumentada, além dos termos internet of things, big data e blockchain.

Nas três análises conduzidas, as tecnologias que apareceram em destaque: internet of things, big data e blockchain e foram objetos da análise de produção e tendências. Dentre os países mais produtivos, destaque para China, Estados Unidos e Inglaterra na produção dos três mencionados termos com maior publicação em periódicos e anais de eventos, comprovando a atualidade dos temas.

O Brasil aparece na pesquisa com o professor Joel J. P. Coelho Rodrigues da Universidade Federal do Piauí, pela comprovada qualidade das pesquisas e mais de 33 mil citações no tema internet of things. Em todos os outros temas pesquisados e, principalmente no foco da pesquisa que é o uso de tecnologias disruptivas com ênfase em inteligência artificial em segurança pública, o Brasil tem diversas oportunidades de pesquisa e desenvolvimento.

Como continuidade da pesquisa pretende-se melhorar a ferramenta de análise de termos por reconhecimento de linguagem natural e complementar a pesquisa com outras fontes, externas às bases de periódicos científicos. Como extensão da pesquisa realizar-se-á pesquisa integrativa para observação e discussão do uso das tecnologias apontadas neste artigo nas instituições nacionais de segurança pública.

Finalmente, assim como diversas outras tecnologias da história, a inteligência artificial pode trazer muitos benefícios para previsão, precisão e aplicações na saúde, segurança, educação e várias outras áreas, mas, por outro lado, pode se tornar um

fardo se for utilizada como arma para disputa de poder e aumento de desigualdades. Esta preocupação está presente na maioria das pesquisas que mencionam necessidade de atenção com a legislação e proteção dos seres humanos e sociedades.

Referências

Anderez, D. O., Lucy, D., Johnson, S., Amnwar, A., & Kanjo, E. (2021). The rise of technology in crime prevention: opportunities, challenges and practitioners perspectives. ArXiv. https://doi.org/10.48550/arxiv.2102.04204

Anh, T., Lenaerts, T., Santos, F. C., & Moniz, L. (2022). Technology in society voluntary safety commitments provide an escape from over-regulation in AI development. Technology in Society, 68(September 2021), 101843. https://doi.org/10.1016/j.techsoc.2021.101843

Apostolakis, K. C., Dimitriou, N., Margetis, G., Ntoa, S., Tzovaras, D., & Stephanidis, C. (2022). DARLENE – Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions [version 1 ; peer review : 2 approved with reservations].

Ben, S., Driss, M., Boulila, W., & Ben, H. (2020). Leveraging deep learning and iot big data analytics to support the smart cities development : review and future directions. Computer Science Review, 38, 100303. https://doi.org/10.1016/j.cosrev.2020.100303

Beraja, M., Yuchtman, N., & Yang, D. Y. (2022). Data-intensive Innovation and the state: evidence from ai firms in China. The Review of Economic Studies. https://doi.org/10.1093/restud/rdac056

Bueno, S., & Lima, R. S. de. (2022). Anuário brasileiro de segurança pública 2022. https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022.pdf?v=5

Buriachok, V., & Sokolov, V. (2020). Implementation of active learning in the master's program on cybersecurity Volodymyr Buriachok ICCSEEA2019. September 2019. https://doi.org/10.1007/978-3-030-16621-2

Christensen, C. M. (2011). O dilema da inovação: quando as novas tecnologias levam empresas ao fracasso. M. Books.

de Pierro, B. (2017). Revisão em praça pública. Pesquisa FAPESP, 254.

Gabriel, M. (2022). Inteligência artificial: do zero ao metaverso (1st ed.). Atlas.

Gaon, A., & Stedman, I. (2019). A call to action: moving forward with the governance of artificial intelligence in Canada. Alberta Law Review, 56(4), 1137. https://doi.org/10.29173/alr2547

Gnatik, E. N. (2021). 'New normality' of the Covid-19 era: opportunities, limitations, risks. RUDN Journal of Sociology, 21(4), 769–782. https://doi.org/10.22363/2313-2272-2021-21-4-769-782

Hegarty, R., & Taylor, M. (2021). Digital evidence in fog computing systems. Computer Law and Security Review, 41. https://doi.org/10.1016/j.clsr.2021.105576
Kazim, E., Trengove, M., Hilliard, A., Koshiyama, A., Lomas, E., Kerrigan, C., Almeida, D., & Güçlütürk, O. (2022). Proposed EU AI Act—Presidency compromise text: select overview and comment on the changes to the proposed regulation. AI and Ethics, 1–7. https://doi.org/10.1007/s43681-022-00179-z

Kewalramani, M. (2018). China's quest for ai leadership: prospects and challenges. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3414883

Kirsch, B., Rüping, S., Knodt, D., & Giesselbach, S. (2018). Robust end-user-driven social media monitoring for law enforcement and emergency monitoring. SpringerBriefs in Criminology, 29–36. https://doi.org/10.1007/978-3-319-89294-8_4

Mustameer, H. (2022). Penegakan hukum nasional dan hukum internasional. 25(01).

Nations, U. (2018). Fourteenth United Nations Congress on crime prevention and criminal justice. https://doi.org/10.5363/tits.7.8_44

Page, M., McKenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., & Mulrow, C. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ, 372(71). http://www.prisma-statement.org/

Parshyn, Y., Yarmolenko, L., & Parshyna, M. (2020). Use of the information technologies at the international level of public communications. Naukovyy Visnyk Dnipropetrovs Kogo Derzhavnogo Universytety Vnutrishnikh Sprav, 1(1), 321–326. https://doi.org/10.31733/2078-3566-2021-1-321-326

Pătrașcu, P. (2021). Emerging technologies and national security: the impact of IoT in critical infrastructures protection and defence sector. Land Forces Academy Review, 26(4), 423–429. https://doi.org/10.2478/raft-2021-0055

Purbahapsari, A. F., & Batoarung, I. B. (2022). Geospatial artificial intelligence for early detection of forest and land fires. KnE Social Sciences, 312–327–312–327. https://doi.org/10.18502/kss.v7i9.10947

Radu, L.-D. (2020). Disruptive technologies in smart cities: a survey on current trends and challenges. Smart Cities, 3(3), 1022–1038. https://doi.org/10.3390/smartcities3030051

Rashid, M., & Fatima, N. (2020). Role of artificial intelligence in eradicating: how artificial intelligence can help to control crime and terror in Pakistan. Global International Relations Review, III(I), 34–43. https://doi.org/10.31703/girr.2020(iii-i).05

Ravichandran, R., Smith, R. E., & Chong, C.-Y. (2021). Artificial intelligence and machine learning: a perspective on integrated systems opportunities and challenges for multi-domain operations. Proceedings of SPIE, 11746, 1174606–1174617. https://doi.org/10.1117/12.2587216

Robinson, N., Ertan, A., & Hardy, A. (2021). Estonia: a curious and cautious approach to artificial intelligence and national security. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4105328

Roessing, A. (2020). Disruptive and game changing technologies in modern warfare, development, use, and proliferation. Advanced Sciences and Technologies for Security Applications. https://doi.org/10.1007/978-3-030-28342-1

Sikorski, M. (2021). Digital innovations and smart solutions for society and economy: pros and cons. foundations of management, 13(1), 103–116. https://doi.org/10.2478/fman-2021-0008

Tulinov, V. S., Veselov, M. Y., Volobuieva, O. O., Merdova, O. M., & Bilykh, I. V. (2022). Activities of law enforcement agencies in the context of the introduction of innovative technologies (comparative legal aspect). Cuestiones Políticas, 40(72), 145–163. https://doi.org/10.46398/cuestpol.4072.08
Union, E. (2021). Presidency compromise text (Vol. 2021, Issue November). https://www.statewatch.org/media/2962/eu-council-ai-act-compromise-text-14278-21.pdf

Vardi, M. Y. (2022). Will AI destroy education. Communications of the ACM, 65(1), 76–85. https://doi.org/10.1145/3501359
Zhang, Y., Jin, R., & Zhou, Z.-H. (2010). Understanding bag-of-words model: a statistical framework. International Journal of Machine Learning and Cybernetics, 1(1), 43–52. https://doi.org/10.1007/s13042-010-0001-0