# Online Rentals Things

Shivaji Chavan Author[1], Ishwar Devale Author[2], Sangram Pachpute Author[3], Aniket Khandagale Author[4], Mr. H.M. Deshmukh[5]

[1,2,3,4] *Department of Computer Engineering, RGOE College of Engineering, Karjule Harya, India*

[5]*Asst. Prof, Project Guide, Department of Computer Engineering Author, RGOE College of Engineering, Karjule Harya, India*

***Abstract*—This project aims to "Online Rental Things" is a comprehensive platform designed to revolutionize the way people access and share various items and resources. In today's fast-paced world, the concept of ownership is evolving, and this project addresses that shift by providing a convenient and efficient solution for renting items ranging from tools and equipment to electronics and recreational gear. The platform offers a user-friendly website and mobile app, enabling users to easily list items they have available for rent or browse and rent items they need for short-term use. It incorporates robust features, including secure payment processing, user reviews, and a reliable rating system to build trust among the community of users.**

**"Online Rental Things" not only promotes resource sharing and sustainability but also fosters a sense of community by connecting people with shared needs and interests. This project aims to simplify the rental process, reduce waste, and empower individuals to make the most of their belongings while reducing the overall environmental impact.**

**With the potential to disrupt traditional consumption patterns and promote the sharing economy, "Online Rental Things" offers a forward-looking solution to modern living, where access to items is prioritized over ownership, promoting economic efficiency and environmental consciousness.**

**Online rental platforms are expanding choice and convenience, allowing customers to rent from a wide array of providers with the click of a button or tap of a finger. The business of online rental is undergoing rapid change as new online platforms race to capture markets and customers across most of the metropolitan cities in India. The paper aims to investigate attributes for online rental platforms by proposing and empirically testing platform attributes-conversion model, examine how platform characteristics influence the renting decision of a consumer and how it subsequently led to conversion. A mix method design was adopted for the study and a pilot study comprising of 341 respondents was carried out. The study focuses on six key attributes - occupational mobility, psychological ownership, complementary services, social gratification, perceived value, and customization, while identifying the most important attributes for renting online**

***Index Terms*—Online rental things, Access-based Consumption, Sharing economy, Collaborative consumption, Online renting platform**

## I. INTRODUCTION

In today's fast-paced world, the way we consume and interact with fashion is evolving rapidly. Embracing the principles of sustainability, affordability and convenience, our project introduces an innovative solution for buy on rent anything that you want in just few hours. In an era of convenience and resources optimization, our project introduces an innovative solution- an Online Rental Things web-based application. This Application is designed to simplify the process of renting a wide variety of items. Instead of spending money on buying these products, it can be used on a rental basis.

Since the management of rental housing and rental vehicles and rental electronics, fashion has become an important part of modern society, a rental management system is necessary. If you are a stranger in the city and want to rent a house, vehicle, electronics and fashion it is difficult to find a suitable in time, and vehicle in emergency. This is the main motivation behind the project development of Online Rental Things. An online web portal that allows you to manage rental properties, vehicles, electronics and fashion allow tenants to view all properties listed, and search for needs by keywords such as property type, location, and more.

The rising cost of all products, it became painful to own products that are of no use for the long term.

Instead of spending money on buying these products, it can be used on a rental basis. The proposed web application makes it simple for consumers to rent products online. The policy of the android application is "Rent what you need and Rent out what you don't". So, when a person puts his product for rent, all other users can have a look at it.

Online portals provide fashion rental services for a wide range of items, from outfits for special occasions (such as weddings and formal parties) to daily apparel and accessories. Customers can browse hundreds of styles through these portals to choose their desired outfits. Pre-paid shipping services are arranged for the delivery and return of rental items. Returned apparel is cleaned and maintained after every rental. However, the nature of collaborative apparel consumption might be different from that of collaborative consumption in other industry sectors such as automobiles, toys, and/or vacation home rentals—the former may meet consumers' hedonic interests, whereas the latter may satisfy their utilitarian needs.

## II. LITERATURE SURVEY

This chapter contains the existing and established theory and research in this report range. This will give a context for work which is to be done. This will explain the depth of the system. Review of literature gives a clearness and better understanding of the exploration. A literature survey represents a study of previously existing material on the topic. This literature survey will logically explain this system.

Online Rental Housing [Ieee-2021]:
In this paper Sahreen Afzal, Toiba Rouf, Sumaiya Qadir designed the online rental housing system where they give house is on rent for specific period.

Car Rental System [Irjet-2021]:
In this paper Amey Thakur, Department of computer engineering, University of Mumbai, designed a car rental application for give a car is on rent.
Online Rental System [Irjet-2022]:
In this paper Abhishek Hatwar, Vijaya Paunikar, Gauri Sayare, Shruti Ghumade, P.A. Kuchewar designed a online rental system application where they gives car, bike, furniture and etc is in rent.

## III. PROBLEM STATEMENT

"Online Rental Things" seeks to address these challenges by providing a user-friendly, and efficient online platform that connects those with items to rent to those in need of them, promoting resource sharing, reducing waste, and ultimately improving the overall quality of life in a more sustainable and cost-effective manner.

The general problem for the individual is to find the amenities according to their needs. Difficult to locate a place that would suit their basic preferences. Difficult to take out time from the busy schedule. The management of the good is difficult if a person is been shifted from its current location. There is no need to travel and visit different locations in search of rental rooms or things. This will be a one-minute job.

## IV. MODULES

- Login Module: Tho's module consists of sign in page, create account page for users.
- Event Listing Module: In this Event Listing Module event which are available for rent are arranged in an organized way. So that users easily can find a suitable thing.
- Booking Module: In this module users need to enter the form and to date and address of their location in order to rent the things.
- Payment Module: On our website payment is done through cards or online

## V. SYSTEM ARCHITECTURE

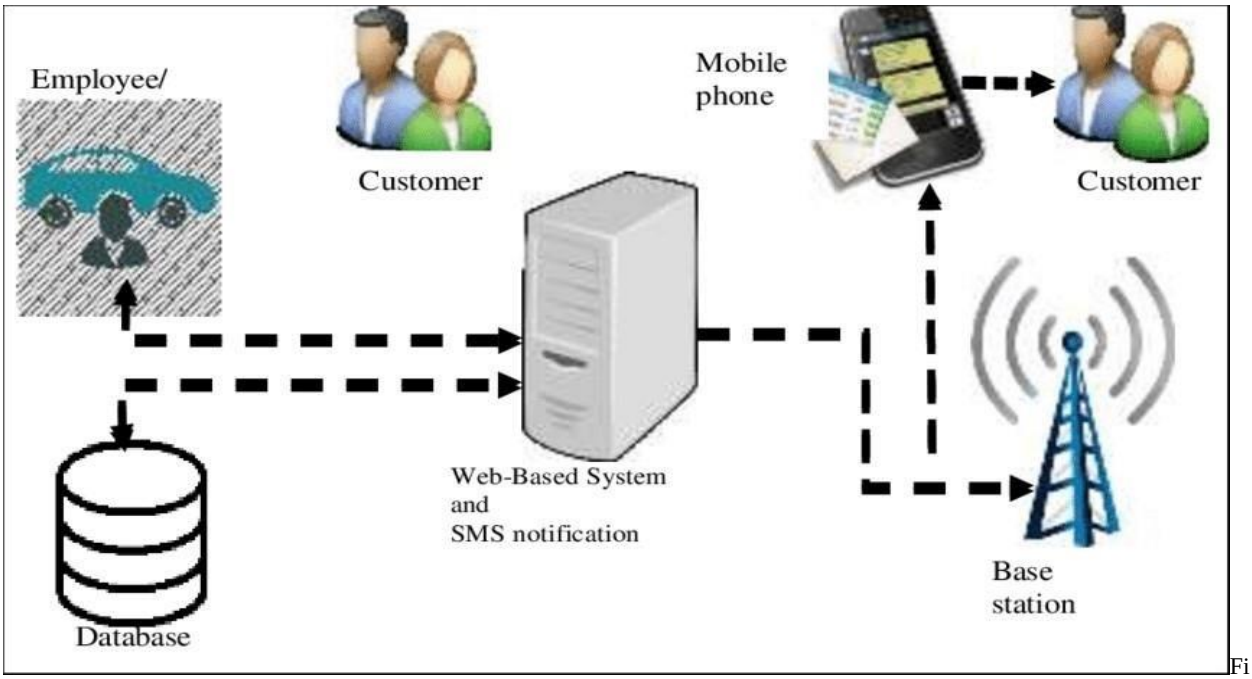



Fig: Architecture of Online Rental Things

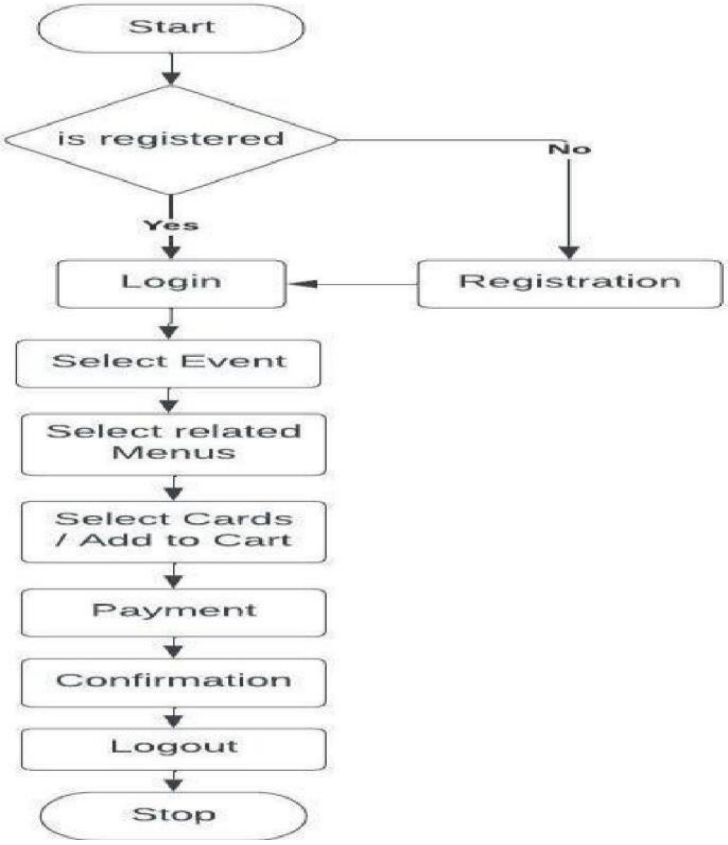
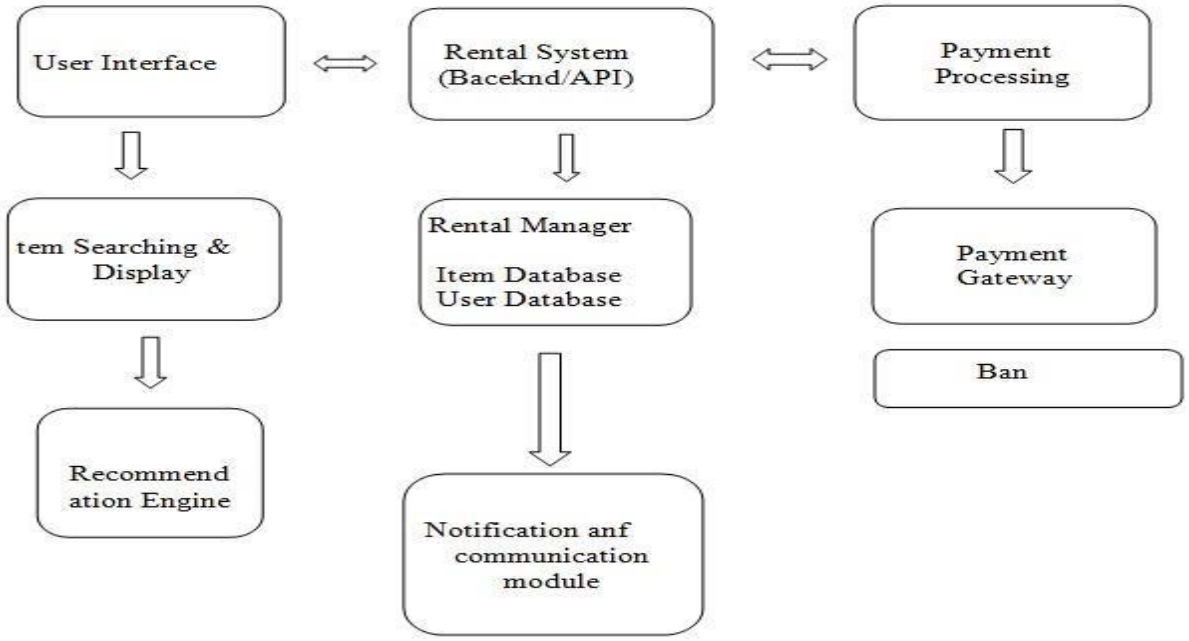



Fig: System Diagram for Rental Things

Creating a system architecture diagram typically involves visual representation using various symbols and shapes. Here's a simplified textual representation of the components and their interactions for a rental system:




V. COMPONENTS

- User Interface: Represents the front-end where users interact with the system.
- Item Search & Display: Handles user queries, displays items, and may incorporate recommendation engine results.
- Recommendation Engine: Provides personalized recommendations based on user preferences and item popularity.
- Rental System (Backend/APIs): Manages the core logic of the rental system, including rental requests, reservations, agreements, and return processing.
- Rental Manager: Coordinates rental-related operations, communicates with item and user databases.
- Item Database: Stores information about available items, their status, and rental history.
- User Database: Manages user profiles, rental history, and eligibility criteria.
- Payment Processing: Interacts with a payment gateway for secure transaction processing.
- Payment Gateway: Handles payment transactions securely, communicating with banking APIs.
- Notification and Communication Module: Sends notifications to users about rental confirmations, return deadlines, and other updates

This is a high-level representation, and depending on the specific requirements, you might need to include additional components, such as a logging system, security measures, and monitoring tools. Each box in the diagram represents a functional module or service, and the arrows indicate the flow of data or interactions between them.

## VI. IMPLEMENTATION AND ALGORITHMS

A. Implementation:

The core functionality of the system involves tracking crops through the supply chain securely. This is achieved through the following steps:

1. User Registration: At the beginning of the Ecommerce website, each user is registered on the website with a unique identifier, including relevant details such as user name, password.
2. Data Transmission: After collection, data is transmitted to a firebase. This transmission may involve wireless technologies, such as Wi-Fi, cellular networks, or satellite connections, depending on the location and available infrastructure.
3. Data Storage: Data is securely stored on cloud
4. Data Processing and Analysis: The stored data is processed and analysed to derive valuable insights. Data processing may involve analytics, machine learning, and artificial intelligence techniques to identify trends, patterns, and anomalies in the Rental products.
5. Products Recommendation: Products Recommendation algorithms are used to Recommendation products to the users.

6. Payment Gateway: System will provide transaction methods like online, COD etc.

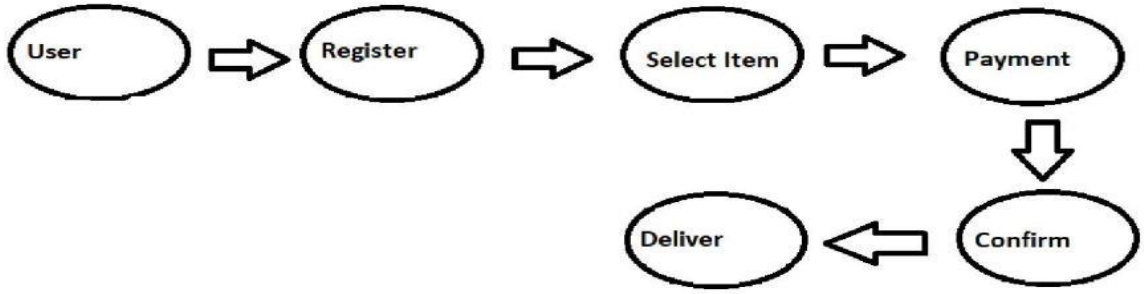



Fig. 3. Data Flow Diagram

B. Algorithms:

Here's a step-by-step theoretical overview of a simplified algorithm for managing rentals:

1. Item Representation: Each rental item is represented in a system, and relevant information such as item ID, type, availability status, and rental history is stored.
2. User Interaction: Users can interact with the system to search for available items, request rentals, and return rented items.
3. Search and Recommendation: Users can search for items based on criteria like type, availability, or other attributes. A recommendation system may suggest items based on user preferences or popular choices.
4. Rental Request: Users initiate a rental request for a selected item. The system checks the item's availability and user eligibility (e.g., account status, rental history).
5. Reservation: If the item is available and the user is eligible, the system reserves the item for the user, marking it as temporarily unavailable to others.
6. Rental Agreement: Users review and agree to the rental terms, including rental duration, fees, and any conditions. The system records the agreement.
7. Payment Processing: Users provide payment information, and the system processes the rental fees. This step may involve secure payment gateways.
8. Notification: Users receive confirmation of their rental along with details such as pickup/delivery instructions and return deadlines.
9. Item Pickup/Delivery: Users pick up the rented item or receive it through a delivery service. The system updates the item status to "rented."
10. Rental Period: The system monitors the rental period, notifying users of upcoming return deadlines and handling any extensions or early returns.
11. Return Request: Users initiate a return request through the system, indicating the item's condition.
12. Return Inspection: The system may conduct an inspection of the returned item, checking for damage or discrepancies from the initial condition.
13. Fee Calculation: Fees, if any (e.g., late fees or damage charges), are calculated based on the rental terms and item condition.
14. Transaction Completion: The rental transaction is completed. Users receive a summary of the transaction, including any additional charges or refunds.
15. Feedback and Ratings: Users may provide feedback and ratings for the rental experience and the rented item. This information can be used for future recommendations.
16. This step-by-step overview provides a high-level understanding of the rental process. Implementation details may vary based on the specific features and requirements of the rental system.

## VII. DISCUSSION

AI techniques are increasingly deployed in different areas and for an increasing number of purposes. This

brings both benefits and risks to society [14]. Among the risks are the use and abuse of AI systems with malicious intent. Even though the capabilities of AIenhanced technology might not always lead to more sophisticated attacks, they certainly have the potential to increase scale and reach. Cybercriminals will progressively integrate AI techniques and the use of AI systems in their plans.

The risks presented in our overview are especially challenging when cybercriminals exploit systems during periods of societal instability. This is facilitated during the COVID-19 pandemic, which caused a growth in the number of people using online tools to work and socialize. The massive shift of social interaction to the online environment increased security vulnerabilities, which malicious actors already exploit at an alarming rate [126]. Not only were individuals and small businesses targeted; in fact, Interpol identified that cybercriminals focused on critical infrastructure, major corporations, and governments [127]. Given the potential impacts of such attacks, it is vital to consider and mitigate these risks.

Some of the issues presented in this overview have been discussed elsewhere [15], [16]. However, in addition to adding novel types of threats in our typology (e.g. Membership Inference Attacks) and providing salient examples, we also provided a different classification than previous works. We divide the attacks between (1) AI-Enabled/ AI-Enhanced attacks and (2) vulnerabilities of AI models. We submit that such separation is helpful because different strategies can alleviate the risks

Addressing challenges linked to vulnerabilities of AI models is highly dependent on the work of engineers and development teams. Developing robust AI systems is paramount. To this end, teams behind the development of algorithms should adhere to principles such as privacyby-design. Organizations, government bodies, and scholars are developing and fine-tuning impact assessment tools for AI systems [128]–[130]. Such tools help translate relevant principles (such as privacy, transparency and fairness [131]) into practical evaluations. Efforts to identify risks via impact assessments are already conducted for data protection compliance in many countries, and similar initiatives can be helpful to deal with the challenges presented by AI systems.

When discussing ways of dealing with the risks presented by AI-Enabled/AI-Enhanced attacks, more is needed in prevention/proactive measures and adequate response. Given that regulatory frameworks and governance mechanisms might not be formulated at the same pace of technological advancements, it is vital to act proactively to reduce the risks outlined in this paper. Instead of finding one overarching solution, different sectors of society could gradually identify initiatives that can help build more resilience and preparedness. Initiatives with local communities, such as promoting data and information literacy, reducing digital divide gaps, and creating campaigns to raise awareness on AI-related threats can be a starting point.

Finally, we wish to emphasize that when discussing the challengesposedbyAIsystems,oneshouldnotforgetthatt he possibilities are also limited. Some simple and easy tasks for humans (e.g., sensorimotor skills such as developing motor abilities through the senses) can be difficult or even impossible for computers to carry out. At the same time, some functions that are complex to humans can be quickly developed in AI systems (e.g., finding patterns in an extensive data set). This is the basis of what became known as Moravec's paradox: ''it is comparatively easy to make computers exhibit adultlevel performance in solving problems on intelligence tests of playing checkers, and difficult or impossible to give them the skills of a one-year-old when it comes to perception and mobility'' [132, p. 15]. Understanding the actual capabilities and limitations of emerging technologies such as AI is therefore critical for developing effective policies and strategies for living in a safer world.

## VIII. CONCLUSION

In conclusion, developing an ecommerce website for our Smart Rental Application is here to make life easier for everyone. With this app, renting items and services becomes a breeze. We've put in a lot of effort to create something that's user-friendly and super convenient. Now, you can rent what you need, when you need it, and do it all with confidence.

In conclusion, the "Online Rental Things" project represents an innovative and promising solution to the challenges of underutilization of resources,

inefficient access to items, and the growing demand for sustainability in our modern society. By facilitating the sharing of various items and resources through a user-friendly online platform, this project offers a range of advantages, including resource efficiency, cost savings, and community building.

However, it's important to acknowledge the potential limitations and challenges associated with such a venture These challenges include building user trust, ensuring the quality of items addressing regulatory concerns, and competing in a dynamic market

REFERENCES


[1] K. Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. London, U.K.: Yale Univ. Press, 2021.

[2] D. Garcia, ‘‘Lethal artificial intelligence and change: The future of international peace and security,’’ Int. Stud. Rev., vol. 20, no. 2, pp. 334–341, Jun. 2018, doi: 10.1093/isr/viy029.

[3] T. Yigitcanlar, K. Desouza, L. Butler, and F. Roozkhosh, ‘‘Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature,’’ Energies, vol. 13, no. 6, p. 1473, Mar. 2020, doi: 10.3390/en13061473.

[4] I. van Engelshoven. (Oct. 18, 2019). Speech by Minister Van Engelshoven on Artificial Intelligence at UNESCO, on October the 18th in Paris. Government of The Netherlands. Accessed: Apr. 15, 2021. [Online]. Available: https://www.government.nl/documents/speeches/2019/ 10/18/speech-by-minister-van-engelshoven-on-artificial-intelligenceatunesco

[5] O. Osoba and W. Welser IV, The Risks of Artificial Intelligence to Security and the Future of Work. Santa Monica, CA, USA: RAND Corporation, 2017, doi: 10.7249/PE237.

[6] D. Patel, Y. Shah, N. Thakkar, K. Shah, and M. Shah, ‘‘Implementation of artificial intelligence techniques for cancer detection,’’ Augmented Hum. Res., vol. 5, no. 1, Dec. 2020, doi: 10.1007/s41133-019-0024-3.

[7] A. Rodríguez-Ruiz, E. Krupinski, J.-J. Mordang, K. Schilling, S. H. HeywangKöbrunner, I. Sechopoulos, and R. M. Mann, ‘‘Detection of breast cancer with mammography: Effect of an artificial intelligence support system,’’ Radiology, vol. 290, no. 2, pp. 305–314, Feb. 2019, doi: 10.1148/radiol.2018181371.

[8] J. Furman and R. Seamans, ‘‘AI and the economy,’’ Nat. Bur. Econ. Res., NBER, Cambridge, MA, USA, Work. Paper, 2018, doi: 10.3386/w24689.

[9] D. R. Coats, Worldwide Threat Assessment of the U.S. Intelligence Community. New York, NY, USA, 2017, p. 32.

[10] L. Floridi, ‘‘Soft ethics: Its application to the general data protection regulation and its dual advantage,’’ Philosophy Technol., vol. 31, no. 2, pp. 163–167, Jun. 2018, doi: 10.1007/s13347-018-0315-5.

[11] P. S. Chauhan and N. Kshetri, ‘‘2021 state of the practice in data privacy and security,’’ Computer, vol. 54, no. 8, pp. 125–132, Aug. 2021, doi: 10.1109/MC.2021.3083916.

[12] S. Gordon and R. Ford, ‘‘On the definition and classification of cybercrime,’’ J. Comput. Virol., vol. 2, no. 1, pp. 13–20, Aug. 2006, doi: 10.1007/s11416-006-0015-z.

[13] Cybercrime. United Nations: Office Drugs. Accessed: May 19, 2021. http://www.unodc.org/unodc/en/cybercrime/index.html

[14] M. Brundage, S. Avin, J. Clark, and H. Toner, ‘‘The malicious use of artificial intelligence: Forecasting, prevention, and mitigation,’’ 2018, arXiv:1802.07228.

[15] T. C. King, N. Aggarwal, M. Taddeo, and L. Floridi, ‘‘Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions,’’ Sci. Eng. Ethics, vol. 26, no. 1, pp. 89–120, Feb. 2020, doi: 10.1007/s11948-018-00081-0.

[16] V. Ciancaglini, ‘‘Malicious uses and abuses of artificial intelligence,’’ in Trend Micro Research; United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol’s European Cybercrime Centre (EC3), Nov. 2020. [Online]. Available: https://www.europol.europa.eu/ publications-documents/malicious-uses-and-abuses-ofartificialintelligence

[17] K. D. Fiedler, V. Grover, and J. T. C. Teng, ‘‘An empirically derived taxonomy of information technology structure and its relationship to organizational structure,’’ J Manage. Inf. Syst.,

vol. 13, pp. 9–34, Jun. 1996, doi: 10.1080/07421222.1996.11518110.

[18] N. Bostrom, ‘‘Information hazards: A typology of potential harms from knowledge,’’ Rev. Contemp. Philosophy, vol. 10, pp. 44–79, May 2011.

[19] W. B. Carper and W. E. Snizek, ‘‘The nature and types of organizational taxonomies: An overview,’’ Acad. Manage. Rev., vol. 5, no. 1, pp. 65–75, Jan. 1980.

[20] (Apr. 21, 2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence—Artificial Intelligence Act. European Commission. Accessed: May 19, 2021. [Online]. Available: https://digitalstrategy.ec.europa.eu/en/library/proposal-regulationlaying-downharmonised-rules-artificial-intelligence-artificialintelligence

[21] Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence—Artificial Intelligence Act—Annexes to the Proposal. European Commission. Accessed: May 19, 2021. [Online].

[22] N. Akdemir and C. J. Lawless, ‘‘Exploring the human factor in cyberenabled and cyber-dependent crime victimisation: A lifestyle routine activities approach,’’ Internet Res., vol. 30, no. 6, pp. 1665–1687, Jun. 2020, doi: 10.1108/INTR-10-2019-0400.

[23] P. N. Grabosky, ‘‘Virtual criminality: Old wine in new bottles?’’ Social Legal Stud., vol. 10, no. 2, pp. 243–249, Jun. 2001, doi: 10.1177/a017405.

[24] B. Hibbard, Ethical Artificial Intelligence, 1st ed. Madison, WI, USA, 2015

[25] D. G. Johnson and M. Verdicchio, ‘‘Reframing AI discourse,’’ Minds Mach., vol. 27, no. 4, pp. 575–590, Dec. 2017, doi: 10.1007/s11023-0179417-6.

[26] R. V. Yampolskiy, ‘‘Taxonomy of pathways to dangerous AI,’’ Phoenix, AZ, USA, Tech. Rep., Feb. 2016, pp. 143–148.

[27] A. Guterres. (May 2020). Protection of Civilians in Armed Conflict. United Nations, S/2020/366. Accessed: Jun. 2, 2020. [Online]. Available: https://undocs.org/en/S/2020/366

[28] E. Zouave, T. Gustafsson, M. Bruce, K. Colde, M. Jaitner, and I. Rodhe, ‘‘Artificially intelligent cyberattacks,’’ Swedish Defence Research Agency, FOI, Tech. Rep. FOI-R–4947-SE, Mar. 2020.

[29] J. Luo, T. Hong, and S.-C. Fang, ‘‘Benchmarking robustness of load forecasting models under data integrity attacks,’’ Int. J. Forecasting, vol. 34, no. 1, pp. 89–104, Jan. 2018, doi: 10.1016/j.ijforecast.2017.08.004.

[30] A. Kurakin, I. Goodfellow, and S. Bengio, ‘‘Adversarial machine learning at scale,’’ 2016, arXiv:1611.01236. [31] I. J. Goodfellow, J. Shlens, and C. Szegedy, ‘‘Explaining and harnessing adversarial examples,’’ 2014, arXiv:1412.6572.

[31] A. Kurakin, I. Goodfellow, and S. Bengio, ‘‘Adversarial examples in the physical world,’’ 2016, arXiv:1607.02533.

[32] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, ‘‘Manipulating machine learning: Poisoning attacks and countermeasures for regression learning,’’ in Proc. IEEE Symp. Secur. Privacy (SP), San Francisco, CA, USA, May 2018, pp. 19–35, doi: 10.1109/SP.2018.00057.

[33] O. Schwartz, ‘‘In 2016, Microsoft’s racist chatbot revealed the dangers of online conversation,’’ IEEE Spectr., to be published. Accessed: Apr. 13, 2021. [Online]. Available: https://spectrum.ieee.org/techtalk/artificialintelligence/machine-learning/in-2016-microsofts-racistchatbotrevealed-the-dangers-of-online-conversation

[34] T. Zemčík, ‘‘Failure of chatbot tay was evil, ugliness and uselessness in its nature or do we judge it through cognitive shortcuts and biases?’’ AI Soc., vol. 36, no. 1, pp. 361–367, Mar. 2021, doi: 10.1007/s00146- 02001053-4.

[35] P. Lee. (Mar. 25, 2016). Learning from Tay’s Introduction. Microsoft Blog. Accessed: Apr. 30, 2021. [Online]. Available: https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/

[36] N. Baracaldo, B. Chen, H. Ludwig, and J. A. Safavi, ‘‘Mitigating poisoning attacks on machine learning models: A data provenance-based approach,’’ in Proc. 10th ACM Workshop Artif. Intell. Secur., Dallas, TX, USA, Nov. 2017, pp. 103–110, doi: 10.1145/3128572.3140450.

[37] T. Gu, B. Dolan-Gavitt, and S. Garg, ‘‘BadNets: Identifying vulnerabilities in the machine learning model supply chain,’’ 2017, arXiv:1708.06733.

[38] N. Carlini, C. Liu, Ú. Erlingsson, J. Kos, and D. Song, ‘‘The secret sharer: Evaluating and testing unintended memorization in neural networks,’’ 2018, arXiv:1802.08232.

[39] M. X. Chen, B. N. Lee, G. Bansal, Y. Cao, S. Zhang, J. Lu, J. Tsay, Y. Wang, A. M. Dai, Z. Chen, T. Sohn, and Y. Wu, ‘‘Gmail smart compose: Real-time assisted writing,’’ in Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, Anchorage AK USA, Jul. 2019, pp. 2287–2295, doi: 10.1145/3292500.3330723.

[40] G. Scopino, AlgoBotsandtheLaw:Technology,Automation,andtheRegulation of Futures and Other Derivatives. Cambridge, U.K.: Cambridge Univ. Press,2020.

[41] T. C. W. Lin, ‘‘The new market manipulation,’’ Emory Law J., vol. 66, pp. 1253–1314, Jul. 2017.

[42] D. Wiener-Bronner. (Feb. 5, 2018). How the Dow Fell 800 Points in 10 Minutes. CNNMoney. Accessed: Jun. 24, 2021. [Online]. Available: https://money.cnn.com/2018/02/05/news/companies/dow-800- points10-minutes/index.html

[43] K. Martin. (May 7, 2020). Flash Crash—The Trading Savant Who CrashedtheU.S.StockMarket. Financial Times. Accessed: Apr. 14, 2021. [Online]. Available: https://www.ft.com/content/5ca93932-8de7-11eaa8ec-961a33ba80aa

[44] S. N. Lynch and D. Miedema. (Apr. 22, 2015). U.K. Speed Trader Arrested Over Role in 2010. Flash Crash. Reuters, Washington, DC, USA. Accessed: Apr. 14, 2021. [Online]. Available: https://www.reuters. com/article/us-usa-security-fraud-idUSKBN0NC21220150422

[45] R. Wigglesworth. (Jan. 9, 2019). Volatility: How ‘algos’ Changed Rhythm Market. Financial Times. Accessed: Jun. 26, 2021. [Online]. Available: https://www-ft-com/content/fdc1c064-1142-11e9-a581-4ff78404524e

[46] A. Zwitter. (Jul. 27, 2017). The Artificial Intelligence Arms Race. Policy Forum. Accessed: Apr. 12, 2021. [Online]. Available: https://www. policyforum.net/artificial-intelligence-arms-race/

[47] J. Cox. (Feb. 16, 2018). The Stock Market Correction Two Weeks Later: How it Happened, and if it Can Happen Again. CNBC. Accessed: Jun. 24, 2021. [Online]. Available: https://www.cnbc.com/ 2018/02/16/the-stock-market-correction-two-weeks-later.html

[48] Y. Yadav, ‘‘The failure of liability in modern markets,’’ Virginia Law Rev.,

[49] R. Webster, J. Rabin, L. Simon, and F. Jurie, ‘‘This person (Probably) Exists. Identity membership attacks against GAN generated faces,’’ 2021, arXiv:2107.06018.

[50] H. Hu, Z. Salcic, L. Sun, G. Dobbie, P. S. Yu, and X. Zhang, ‘‘Membership inference attacks on machine learning: A survey,’’ 2021, arXiv:2103.07853.

[51] F. Mouton, L. Leenen, and H. S. Venter, ‘‘Social engineering attack examples, templates and scenarios,’’ Comput. Secur., vol. 59, pp. 186–209, Jun. 2016, doi: 10.1016/j.cose.2016.03.004.

[52] C. Freitas, F. Benevenuto, S. Ghosh, and A. Veloso, ‘‘Reverse engineering socialbot infiltration strategies in Twitter,’’ in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining, Paris, France, Aug. 2015, pp. 25–32, doi: 10.1145/2808797.2809292.

[53] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, ‘‘Design and analysis of a social botnet,’’ Comput. Netw., vol. 57, no. 2, pp. 556–578, Feb. 2013, doi: 10.1016/j.comnet.2012.06.006.

[54] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, ‘‘The rise of social bots,’’ Commun. ACM, vol. 59, no. 7, pp. 96–104, Jul. 2016, doi: 10.1145/2818717.

[55] S. Rossi. (Dec. 15, 2007). Beware the CyberLover that Steals Personal Data. PCWorld. Accessed: May 11, 2020. [Online]. Available: https://www.pcworld.com/article/140507/article.html

[56] J. Seymour and P. Tully. (2016). Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us16Seymour-Tully-Weaponizing-Data-Science-For-Social-

EngineeringAutomated-E2E-Spear-Phishing-On-Twitter-wp.pdf

[57] A. Bessi and E. Ferrara, ‘‘Social bots distort the 2016 U.S. Presidential election online discussion,’’ 1st Monday, vol. 21, no. 11, Nov. 2016.

[58] G. P. Nobre, J. M. Almeida, and C. H. G. Ferreira, ‘‘Caracterização de bots no Twitter durante as eleições presidenciais no Brasil em 2018,’’ in Anais do VIII Brazilian Workshop Social Netw. Anal. Mining (BraSNAM), Jul. 2019, pp. 107–118, doi: 10.5753/brasnam.2019.6553

[59] M. Kovic, A. Rauchfleisch, M. Sele, and C. Caspar, ‘‘Digital astroturfing in politics: Definition, typology, and countermeasures,’’ Stud. Commun. Sci., vol. 18, no. 1, Nov. 2018, doi: 10.24434/j.scoms.2018. 01.005.

[60] S. Mahbub, E. Pardede, A. S. M. Kayes, and W. Rahayu, ‘‘Controlling astroturfing on the Internet: A survey on detection techniques and research challenges,’’ Int. J. Web Grid Services, vol. 15, no. 2, p. 139, 2019, doi: 10.1504/IJWGS.2019.099561.

[61] F. B. Keller, D. Schoch, S. Stier, and J. Yang, ‘‘Political astroturfing on Twitter: How to coordinate a disinformation campaign,’’ Political Commun., vol. 37, no. 2, pp. 256–280, Mar. 2020, doi: 10.1080/10584609.2019.1661888.

[62] A. Zwitter. (Jun. 12, 2016). The Impact of Big Data of International Affairs. Clingendael Spectator. Accessed: Apr. 7, 2021. [Online]. Available: https://spectator.clingendael.org/en/publication/impactbigdata-international-affairs

[63] I. Lapowsky. (Nov. 28, 2017). How Bots Broke the FCC’s Public Comment System. Wired. Accessed: Apr. 8, 2021. [Online]. Available: https://www.wired.com/story/bots-broke-fcc-public-comment-system/

[64] C. Thuen. (Oct. 2, 2017). Discovering Truth Through Lies on the Internet—FCC Comments Analyzed. Gravwell. Accessed: Apr. 8, 2021. [Online]. Available: https://www.gravwell.io/blog/discoveringtruththrough-lies-on-the-internet-fcc-comments-analyzed

[65] V. Bakir, ‘‘Psychological operations in digital political campaigns: Assessing Cambridge analytica’s psychographic profiling and targeting,’’ Frontiers Commun., vol. 5, p. 67, Sep. 2020, doi: 10.3389/fcomm.2020.00067.

[66] J. Habgood-Coote, ‘‘Stop talking about fake news!’’ Inquiry, vol. 62, nos. 9–10, pp. 1033–1065, Nov. 2019, doi: 10.1080/0020174X.2018.1508363.

[67] M. Sullivan. (Jan. 8, 2017). It’s Time to Retire the Tainted Term. Fake News, The Washington Post. Accessed: Apr. 29, 2021. [Online]. Available: https://www.washingtonpost.com/lifestyle/style/its-time-toretire-thetainted-term-fake-news/2017/01/06/a5a7516c-d375-11e6- 945a-76f69a399dd5_story.html

[68] E. Zuckerman. (Jan. 31, 2017). Stop Saying ‘Fake News’. It’s Not Helping. Ethan Zuckerman. Accessed: Apr. 29, 2021. [Online]. Available: https://ethanzuckerman.com/2017/01/30/stop-saying-fakenews-itsnot-helping/

[69] S. Alonso García, G. Gómez García, M. Sanz Prieto, A. J. Moreno Guerrero, and C. Rodríguez Jiménez, ‘‘The impact of term fake news on the scientific community. Scientific performance and mapping in web of science,’’ Social Sci., vol. 9, no. 5, p. 73, May 2020, doi: 10.3390/socsci9050073.

[70] J. Pepp, E. Michaelson, and R. Sterken, ‘‘Why we should keep talking about fake news,’’ Inquiry, vol. 65, no. 4, pp. 471–487, Nov. 2019, doi: 10.1080/0020174X.2019.1685231.

[71] S. O. Oyeyemi, E. Gabarron, and R. Wynn, ‘‘Ebola, Twitter, and misinformation: A dangerous combination?’’ BMJ, vol. 349, pp. g6178– g6178, Oct. 2014, doi: 10.1136/bmj. g6178.

[72] J. Roozenbeek, C. R. Schneider, S. Dryhurst, J. Kerr, A. L. J. Freeman, G. Recchia, A. M. van der Bles, and S. van der Linden, ‘‘Susceptibility to misinformation about COVID-19 around the world,’’ Roy. Soc. Open Sci., vol. 7, no. 10, Oct. 2020, Art. no. 201199, doi: 10.1098/rsos.201199.

[73] W. L. Bennett and S. Livingston, ‘‘The disinformation order: Disruptive communication and the decline of democratic institutions,’’ Eur. J. Commun., vol. 33, no. 2, pp. 122–139, Apr. 2018, doi: 10.1177/0267323118760317.

[74] C. Machado, B. Kira, V. Narayanan, B. Kollanyi, and P. Howard, ‘‘A study of misinformation in WhatsApp groups with a focus on the Brazilian presidential Elections,’’ in Proc. Companion Proc. World Wide Web Conf., San Francisco, CA, USA, May 2019, pp. 1013–1019, doi: 10.1145/3308560.3316738.

[75] B. Wilder and Y. Vorobeychik, ‘‘Defending elections against malicious spread of misinformation,’’ in Proc. AAAI, vol. 33, Jul. 2019, pp. 2213– 2220, doi: 10.1609/aaai.v33i01.33012213.

[76] P. Nemitz, ‘‘Constitutional democracy and technology in the age of artificial intelligence,’’ Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci., vol. 376, no. 2133, Nov. 2018, Art. no. 20180089, doi: 10.1098/rsta.2018.0089.

[77] L. Floridi and M. Chiriatti, ‘‘GPT-3: Its nature, scope, limits, and consequences,’’ Minds Mach., vol. 30, pp. 681–694, Nov. 2020, doi: 10.1007/s11023-020-09548-1.

[78] K. McGuffie and A. Newhouse, ‘‘The radicalization risks of GPT-3 and advanced neural language models,’’ 2020, arXiv:2009.06807.

[79] Wordflow AI Articles. Accessed: Apr.

[80] R. Leyva and C. Beckett, ‘‘Testing and unpacking the effects of digital fake news: On presidential candidate evaluations and voter support,’’ AI Soc., vol. 35, no. 4, pp. 969–980, Dec. 2020, doi: 10.1007/s00146-02000980- 6

[81] S. M. Jones-Jang, T. Mortensen, and J. Liu, ‘‘Does media literacy help identification of fake news? Information literacy helps, but other literacies don’t,’’ Amer. Behav. Scientist, vol. 65, no. 2, pp. 371–388, Feb. 2021, doi: 10.1177/0002764219869406.

[82] Association for College and Research Libraries. (2016). Framework for Information Literacy for Higher Education. Accessed: Jun. 29, 2021. [Online]. Available: https://www-ala-org. proxyub.rug.nl/acrl/standards/ilframework

[83] O. J. Gstrein, ‘‘Right to be forgotten: European data imperialism, national privilege, or universal human, right?’’ Rev. Eur. Administ. Law, vol. 13, no. 1, pp. 125–152, May 2020, doi: 10.7590/187479820X15881424928426.

[84] H. Allcott and M. Gentzkow, ‘‘social media and fake news in the 2016 election,’’ J. Econ. Perspect., vol. 31, no. 2, pp. 211–236, May 2017, doi: 10.1257/jep.31.2.211.

[85] C. Shah. (Mar. 10, 2021). It’s Not Just a Social Media Problem—How Search Engines Spread Misinformation. The Conversation. Accessed: Jun. 29, 2021. [Online]. Available: http://theconversation.com/itsnotjust-a-social-media-problem-how-search-enginesspreadmisinformation-152155

[86] C. Arun, ‘‘Facebook’s faces,’’ in Forthcoming Harvard Law Review Forum, vol. 135. Mar. 2021, doi: 10.2139/ssrn.3805210.

[87] G. De Gregorio, ‘‘Democratising online content moderation: A constitutional framework,’’ Comput. Law Secur. Rev., vol. 36, Apr. 2020, Art. no. 105374, doi: 10.1016/j.clsr.2019.105374.

[88] R. T. Garcia. (Jun. 19, 2020). Anonymous Twitter Accounts in Brazil are Pressuring Advertisers to Drop Conservative Media Campaigns. Insider. Accessed: Jun. 29, 2021. [Online]. Available: https://www.insider.com/sleeping-giants-brasil-borrowing-us-tacticforfighting-misinformation-2020-6

[89] J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, and M. Niessner, ‘‘Face2Face: Real-time face capture and reenactment of RGB videos,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, Jun. 2016, pp. 2387–2395.

[90] M. Westerlund, ‘‘The emergence of deepfake technology: A review,’’ Technol. Innov. Manage. Rev., vol. 9, no. 11, pp. 39–52, Jan. 2019, doi: 10.22215/timreview/1282.

[91] T. Greene. (Apr. 21, 2020). Watch: Fake Elon Musk Zoom-Bombs Meeting Using Real-Time Deepfake AI. Neural | The Next Web. Accessed: Apr. 7, 2021. [Online]. Available: https://thenextweb.com/ neural/2020/04/21/watch-fake-elon-musk-zoom-bombs-meetingusingreal-time-deepfake-ai/

[92] L. Guarnera, O. Giudice, C. Nastasi, and S. Battiato, ‘‘Preliminary forensics analysis of DeepFake images,’’ 2020, arXiv:2004.12626.

[93] M.-H. Maras and A. Alexandrou, ‘‘Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake

videos,'' Int. J. Evidence Proof, vol. 23, no. 3, pp. 255–

[94] D. O'Sullivan. (Aug. 10, 2019). The Democratic Party Deepfaked Its Own Chairman to Highlight 2020 Concerns. CNN. Accessed: May 11, 2020. [Online]. Available: https://www.cnn.com/2019/08/09/ tech/deepfake-tom-perez-dnc-defcon/index.html

[95] D. Fonseca. (Jan. 18, 2021). BrunoSartori:OReiDASDeepfakes. Revista Trip. Accessed: Jun. 28, 2021. [Online]. Available: https://revistatrip. uol.com.br/trip/webstories/bruno-sartori-o-rei-das-deepfakes

[96] J. Compton, ''Inoculation theory,'' in SAGE Handbook of Persuasion: Developments in Theory and Practice. Newbury Park, CA, USA: Sage, 2012, pp. 220–236, doi: 10.4135/9781452218410.n14.

[97] W. J. McGuire, ''Inducing resistance to persuasion: Some contemporary approaches,'' in Advances in Experimental Social Psychology, vol. 1, L. Berkowitz, Ed. New York, NY, USA: Academic, 1964, pp. 191–229.

[98] D. Guera and E. J. Delp, ''Deepfake video detection using recurrent neural networks,'' in Proc. 15th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS), Auckland, New Zealand, Nov. 2018, pp. 1–6, doi: 10.1109/AVSS.2018.8639163.

[99] R. Chesney and D. K. Citron, ''Deep fakes: A looming challenge for privacy, democracy, and national security,'' SSRN J., pp. 1753–1820, 2018, doi: 10.2139/ssrn.3213954.

[100] V. Elliott and M. Tobin. (Jan. 10, 2022). China Steps up Efforts to Ban Deepfakes. Will it work? Rest World. Accessed: Mar. 1, 2022. [Online]. Available: https://restofworld.org/2022/china-steps-upeffortsto-ban-deepfakes/

[101] K. Zetter. (Nov. 19, 2010). Wiseguys Plead Guilty in Ticketmaster Captcha Case. Wired. Accessed: Jun. 2, 2020. [Online]. Available: https://www.wired.com/2010/11/wiseguys-plead-guilty/

[102] K. Trieu and Y. Yang. (2018). Artificial Intelligence-Based Password Brute Force Attacks. [Online]. Available: http://aisel.aisnet.org/ mwais2018/39

[103] D. Gibert, C. Mateu, and J. Planes, ''The rise of machine learning for detection and classification of malware: Research developments, trends and challenges,'' J. Netw. Comput. Appl., vol. 153, Mar. 2020, Art. no. 102526, doi: 10.1016/j.jnca.2019.102526.

[104] AV-TEST. (2021). Malware Statistics & Trends Report. AV-TEST: The Independ. IT-Security Inst. Accessed: Jun. 22, 2021. [Online]. Available: https://www.av-test.org/en/statistics/malware/

[105] (2018). DeepLocker—Concealing Targeted Attacks with AI Locksmithing. Black Hat USA. Accessed: Apr. 22, 2021. [Online]. Available: https://www.blackhat.com/us18/briefings/schedule/#deeplocker— concealing-targeted-attacks-withai-locksmithing-11549262, Jul. 2019, doi: 10.1177/1365712718807226. [95] D. O'Sullivan. (Aug. 10, 2019). The Democratic Party Deepfaked Its Own Chairman to Highlight 2020 Concerns. CNN. Accessed: May 11, 2020. [Online]. Available: https://www.cnn.com/2019/08/09/ tech/deepfake-tom-perez-dnc-defcon/index.html [96] D. Fonseca. (Jan. 18, 2021). BrunoSartori:OReiDASDeepfakes. Revista Trip. Accessed: Jun. 28, 2021. [Online]. Available: https://revistatrip. uol.com.br/trip/webstories/bruno-sartori-o-rei-das-deepfakes