Victoria, Stanciu; Rindasu, Sinziana-Maria

Article

Artificial intelligence in retail: Benefits and risks associated with mobile shopping applications

Amfiteatru Economic Journal

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Victoria, Stanciu; Rindasu, Sinziana-Maria (2021) : Artificial intelligence in retail: Benefits and risks associated with mobile shopping applications, Amfiteatru Economic Journal, ISSN 2247-9104, The Bucharest University of Economic Studies, Bucharest, Vol. 23, Iss. 56, pp. 46-64,
https://doi.org/10.24818/EA/2021/56/46

This Version is available at:
https://hdl.handle.net/10419/281559

ARTIFICIAL INTELLIGENCE IN RETAIL: BENEFITS AND RISKS ASSOCIATED WITH MOBILE SHOPPING APPLICATIONS

Victoria Stanciu[1] and Sînziana-Maria Rîndașu[2*]
[1)2)] *Bucharest University of Economic Studies, Romania*

Please cite this article as:
Stanciu, V. and Rîndașu, S.M., 2021. Artificial Intelligence in Retail: Benefits and Risks Associated With Mobile Shopping Applications. *Amfiteatru Economic*, 23(56), pp. 46-64.

DOI: 10.24818/EA/2021/56/46

Article History
Received: 29 September 2020
Revised: 30 October 2020
Accepted: 3 December 2020

Abstract
The objective of the study is to examine the practical implications of using artificial intelligence (AI) based solutions in the case of retail mobile applications, to enhance the online shopping experience and improve the engagement by also having in mind the privacy of the users. We examined 117 shopping applications available in the Google Play market and investigated the permissions required for each application and the categories of personal data collected from the users. Based on the information gathered, we provided practical methods to integrate artificial intelligence-based solutions to offer a new set of services, partially unavailable in physical stores. Some of the permissions identified, if exploited by malicious users, can affect individuals' privacy. The fact that artificial intelligence is a fast-developing technology constitutes the main challenge in the effort of creating proper regulations. This research provides practical directions regarding the benefits of integrating artificial intelligence solutions in retail mobile applications in an ethical manner, protecting the users' privacy.

Keywords: artificial intelligence, machine learning algorithms, retail, ethics, privacy, mobile shopping applications

JEL Classification: L81, K40, O33

* Corresponding author, **Sînziana-Maria Rîndasu** – e-mail: sinziana_rindasu@yahoo.com

Introduction

The pandemic changed the consumers' habits, especially in the case of non-essential goods, where the sales volume decreased significantly in the second and third quarter of 2020. Since social distancing continued to represent the leading solution to reduce the exposure of the individuals to the virus, many consumers started using online shopping to the detriment of physical stores (Barnes, 2020; Nguyen et al., 2020). In this context of significant quick changes, retailers' attention is moving to e-commerce in an attempt to respond to the new needs of the individuals. The online shopping has received a significant level of attention during the last years and researchers highlighted that the key aspects important to the consumers are represented by the ease of use, the design of the website or application, and the trust regarding the usage of the personal data collected (Ha and Stoel, 2009; Lian and Yen, 2014; Al-Debei, Akroush and Ashouri, 2015; Natarajan, Balasubramanian and Kasilingam, 2017).

The adoption of artificial intelligence (AI) based solutions in retail and wholesale is rapidly transforming the industry by enhancing the entire process since this domain generates a vast amount of data that can be leveraged using this data-driven technology. Over the years, different studies have investigated the practical ways in which AI-based solutions are being used in retail and wholesale. However, less attention has been paid on leveraging mobile applications to provide a better experience than the one in-store, using AI, especially in this current context where customers tend to avoid unnecessary social interactions. Mobile shopping applications, compared with online shopping by using different browsers, provide more leverage to the companies to increase the engagement (Ho and Chung, 2020; Li, Zhao and Pu, 2020) and facilitate the use of various AI features that can be embedded in the applications.

Theoretically, there is no limit for AI to expand and facilitate enhancements in any industry, so the boundaries should be set by ethical guidelines and principles (Kreutzer and Sirrenberg, 2020) to create a technology that works in favour of the individual and the collective well-being.

The purpose of the current study is to investigate practical implications regarding the use of mobile shopping applications along with AI-based solutions to improve engagement, enhance the online shopping experience, and encourage impulse buying, also focusing on privacy, legal, and ethical implications. A series of mobile shopping applications available in the Google Play market has been examined to achieve the research's objective. This approach is used to determine the main permissions required, which of those permissions can be leverage by using AI, the security implications, and how the personal data collected is used to train machine learning algorithms to better respond to the needs of the users. The current research aims to provide support for retail companies to adopt more AI-based solutions that can be integrated into mobile shopping applications, to increase the business objective ethically.

This paper is structured in four parts. The first part presents the relevant literature review for this research, focusing on current AI solutions used in retail, legal aspects, and ethical challenges. The second part details the methodology used to conduct the research, mentioning the purpose and objectives. The third part reflects the study's results, which present the main permissions of mobile applications that can be exploited by AI solutions, the types of data collected by companies that offer the mobile applications, along with the

main challenges regarding privacy. The last part presents the conclusions, the limits of the present study, and the future research directions.

1. Literature review

Researchers tend to have different approaches when presenting the distinct fields of AI (Buhalis, et al., 2019; Dignum, 2019; Chowdhary, 2020; Girasa, 2020; Kreutzer and Sirrenberg, 2020). While in some studies the types of AI are categorised based on the IT-related functionalities, others are using a taxonomy based on the evolution in time, the principal sub-fields of applications being: natural language processing, natural image processing, expert systems, and robotics. In terms of the capabilities and evolution, researchers classify AI as Weak Artificial Intelligence (or Artificial Narrow Intelligence), Artificial General Intelligence, and Strong Artificial Intelligence. Another classification of AI was given by Hintze (2016), which considers that there are four main categories of AI: reactive, limited memory, theory of the mind, and self-aware.

Machine learning (ML), one of the most known and used AI techniques in the retail field, is part of the robotic sub-field and the narrow AI, having different types of implementation: supervised learning (predicts), unsupervised learning (discovers patterns), reinforcement learning (decision-making), and deep learning (multiple neural networks) (LeCun, Bengio and Hinton, 2015; Goodfellow, Bengio and Courville, 2016; Dignum, 2019; Luce, 2019; Kreutzer and Sirrenberg, 2020), all based on algorithms that are processing data, learning, and developing new models to answer the needs of the companies.

1.1. AI applications in retail

Retailers all around the globe started to adopt AI solutions to support the development in this sector. Amazon was one of the most active pioneers in automating this domain with the use of AI in different areas of retail, from warehouse robots that can move items and prepare orders to be shipped (Bogue, 2016), drones that will bring the goods to the customers (Singireddy and Daim, 2018), anticipatory shipping (patented in 2011), that should address a significant part of the logistical issues (Spiegel, et al., 2011), to checkout-free shops (Polacco and Backes, 2018). The next step might be shipping the products to the client, without an initial order, based on the algorithms' predictions and the users' behaviour and, if the product is not desired by the customer, it can be returned (Shankar, 2018).

Chatbots, also called conversational agents, are becoming extremely attractive to companies due to the applicability as this technology promises to improve engagement, facilitate the interaction, and provide a personalised shopping experience. They can use natural language processing, natural image processing, and ML algorithms. A recent study (Rese, Ganster and Baier, 2020), investigating a series of market research surveys, showed that the acceptance rate of chatbots varies between 10% and 50%.

IoT devices, like the Samsung fridge (Gritti, Önen and Molva, 2019), allow people to avoid a series of activities; the fridge is making a list of goods and sends the orders automatically to the grocery shop for the products needed. However, a recent study focused on autonomous shopping (De Bellis and Johar, 2020) identifies four significant psychological

barriers regarding the adoption of these systems: reduced control and autonomy, reduced meaningful experience, reduced individuality and identity, and reduced social connectedness.

The increasing adoption of augmented reality (AR) applications brings significant benefits to the retail area by allowing customers to visualise products in a completely new and innovative manner by using magic mirrors, virtual fitting rooms, and different techniques that help clients make the best purchase decision and increase their level of satisfaction (Poushneh and Vasquez-Parraga, 2017).

A major drawback for retailers to adopt AI-based solutions was the initial adoption costs. Now there are several companies (Slyce – image search for recommendations, Oracle – chatbots) that started to provide AIaaS (Artificial Intelligence as a Software), aiming to facilitate the integration of these technologies for the retailers. Therefore, the expectations are that during the next years almost all online stores will use AI to enhance the shopping experience.

1.2. Regulating Artificial Intelligence

At the European Union (EU) level, several instruments can be used to regulate the legal impact of the AI applications on individuals and society, both in terms of hard law and soft law. However, the main challenges are derived from the constant expansion and evolution of AI techniques. In this context of fast-developing technologies, the hard law (binding legal instruments and regulations) if applied, might not be sufficient for a medium and long timeframe, while the soft law (agreements, principles, and declarations that are not legally binding) and ethical frameworks, lack an oversight mechanism and create difficulties for programmers to develop AI-based applications.

Since the expansion of AI is touching more and more individuals' personal lives and due to the need for a legal framework, the Council of Europe's Committee of Ministers set up in September 2019 the Ad Hoc Committee on Artificial Intelligence – CAHAI. The objective of CAHAI, established for two years, until 2021, is to examine, through dialogue with stakeholders, "the feasibility and potential elements of a legal framework for the development, design and application of artificial intelligence", so AI applications will respect the compliance with the rule of law. Furthermore, CAHAI should assess whether the current legal instruments are suitable for addressing the present and future challenges brought by the development of AI.

The need for regulating AI arises from the necessity of having personal data processed in a fair, transparent, and accountable manner by avoiding discrimination and creating trust for stakeholders and shareholders. The regulation of AI poses challenges derived from the continuous development of the algorithms. In this respect, the lawmakers and standard setters should be aware that the risk assessment should be carried on a systematic base, using preferably a principle-based approach instead of a rule-based regulation.

The regulation of AI applications impacts the commerce industry that had already embedded in its processes AI solutions. A common issue lately identified in the retail area is price discrimination (PD) that refers to the use of ML algorithms aiming to sell a good or service at the maximum price the consumer is willing to pay. Based on a series of labels that the algorithm assigns to the individuals, based on the past activity and personal data,

researchers showed that some categories of consumers are offered a particular good or service at a higher price (Hannak, et al., 2014; Larson, Mattu and Angwin, 2015; Calvano, et al., 2019). As per this, because of the retail companies' clustering algorithms, some individuals are offered a higher price, even though the delivery costs are the same for every potential client. While PD mechanisms might not use complex AI techniques to target specific categories of individuals, the algorithms can instead use a limited series of attributes, like the location; in theory, AI can use unsupervised learning to obtain a finer-grained PD (Gautier, Ittoo and Van Cleynenbreugel, 2020). The current anti-discrimination laws might not be sufficient for this scenario of indirect discrimination and regulators have to address this issue by highlighting the need for developers to be more accountable for the algorithms that they design, preventing, in this way, PD.

Retailing represents the perfect environment for the use and growth of AI since it collects a significant amount of information regarding consumers and their behaviour. Because of this, the way in which the algorithms are processing the data has received a lot of research attention by studying how the privacy of individuals is affected and possible technical solutions to mitigate the risks (Els, 2017; Alguliyev, Aliguliyev and Abdullayeva, 2019; Hao, et al., 2019; Mazurek and Małagocka, 2019; Kreutzer and Sirrenberg, 2020; Singh, Rathore and Park, 2020; Thinyane and Sassetti, 2020).

1.3. Ethical challenges

AI solutions started to be researched and used since 1950, but the progress became significant in the last two decades, impacting individuals' lives systematically. This incredible progress, however, raised a question: to what point AI can influence humanity? Kreutzer and Sirrenberg (2020) consider that "There are – technically – (almost) no limits to the possible fields of application of Artificial Intelligence. The limits should therefore be set by ethical standards". In the 2019 Artificial Intelligence Index Report (Perrault, et al., 2019) are presented 12 ethical challenges highlighted by researchers that should be addressed in the development of AI-based solutions. The primary concerns are focused on fairness – using a dataset that is not discriminatory and does not contain elements that might lead to algorithmic bias, interpretability – the degree to which the user can understand the cause of the decision and can predict future results, explicability – the active characteristic of the algorithm that brings clarifications regarding the undergoing processes in providing an output, transparency – the level of information provided by an AI-based system, during the decision-making process, accountability – the accountability of the stakeholders involved in developing the algorithms regarding the implications generated by using it, and data privacy – users knowing how their personal data is processed in the developing and usage of the AI-based systems.

One primary technical concern is algorithmic bias, which is represented by a series of systematic and repeated errors, that can lead to discrimination due to using inadequate data (incomplete, unrepresentative, or already biased) to develop the algorithms.

In the relevant literature, several examples of algorithmic biases can be found (Bozdag, 2013; Lambrecht and Tucker, 2019; Taati, et al., 2019). However, in some cases, it is uncertain if the bias was created by the inadequate dataset used to train the algorithms or if the algorithms have learned to maximise the chances of achieving the objective. Although

not all forms of algorithmic biases are discriminatory, there is an ethical need to address this issue.

Shopping represents a therapeutic activity for individuals (Babin, Darden and Griffin, 1994) and retailers are nowadays focusing on enhancing the customers' experience. However, there is a fine line between shopping therapy and compulsive purchases (Hirschman, 1992), so companies should focus their efforts on supporting a correct shopping behaviour, especially in the context of introducing AI-based solutions that are capturing easier the attention of individuals.

Another critical aspect that is supported by ML algorithms in the retail area is to predict the users' needs and provide anticipatory delivery of the products, not in the warehouse, but directly to the customers, that can return the goods if they are not satisfied with them~~,~~; however, this seems to impact the control of the individual over the decisions made to acquire a good. While this is not a trespassing of privacy, it raises concerns regarding the impact that this might have on the individuals' personal lives.

2. Research methodology

Taking into consideration that smartphones gained a tremendous amount of popularity, have an extremely favourable acceptance rate (Deloitte, 2019), and provide significant support to the retailers, we considered appropriate to explore the relationship between AI solutions and mobile applications, especially now when the customers' behaviour changed as a result of the pandemic, the number of visits to physical stores decreased worldwide, and the online shopping started to be preferred, the smartphones being a significant vector in this switch.

This research aims to identify practical solutions for the use of mobile shopping applications for both essential and non-essential goods, together with solutions based on AI systems, to increase customer engagement, encourage impulse buying, provide a significantly better shopping experience, and analyse potential risks that may affect the confidentiality of data collected from the users. Thus, the general and specific research's objectives we set out were:

- **O1.** Analysing how privacy can be affected by using mobile applications. To achieve this goal, we have refined the research direction through the following specific objectives:

- **O1.1.** Identifying the mobile applications' permissions that may affect the confidentiality of data provided by users.

- **O1.2.** Examining the privacy policies of the companies that sell products through mobile applications, to determine the main types of information collected, the risks and how the data is protected.

- **O2.** Identifying how the AI used in mobile shopping applications supports the development of competitive advantage. To achieve this goal, we have refined the research direction through the following specific objectives:

- **O2.1.** Analysing the permissions of mobile applications to determine which of them can be used in conjunction with AI solutions to increase customer engagement.

- **O2.2.** Identifying permissions of mobile applications that can be exploited through the use of AI to encourage impulse buying and provide consumers with a better experience compared to physical store purchases.

The general approach of the research consists of conducting a cross-sectional study; the objective is to capture several perspectives on the data collected from mobile shopping applications, in order to provide practical recommendations to achieve the study's aim. Currently, in the Google Play store, there are over three million applications deployed, from which over 110.000 are included in the shopping category and, by looking at the popularity in terms of numbers of downloads, around 200.000 of them (6.67%) have been downloaded more than 100.000 times.

In this exploratory research, we analysed 117 shopping applications available in Google Play, randomly selected exclusively based on the popularity. The criteria taken into consideration when selecting the application was to have at least 100.000 downloads. Within the selected applications, products from different categories are sold (table no. 1). The data has been collected during July-August 2020. Some of the applications analysed are: Zalando - Shopping & Fashion, iHerb, The Home Depot, Best Buy, The Kroger, Decathlon International, and PetSmart. Since the AI solutions are diverse and have a high degree of complexity, for the selection of the applications included in this study the existence or lack of usage of AI was not taken into account. Although in some cases users can clearly identify the existence of an AI-based program, such as searching for a product by uploading an image, conversational robots, or personalised recommendations, AI is much more complex and even if the user is not informed about the programs used by the company to determine a specific response, this does not indicate that these applications do not use AI. For these reasons, we have not exclusively selected applications whose description and functionality suggested the use of ML algorithms or any other program in the field of AI.

Table no. 1. Distribution of the applications analysed by category and number of downloads

Category of applications/ Number of downloads	100k+	500k+	1mil+	5mil+	10mil+	50mil+	100mil+	Total
Clothes, shoes, and accessories	4	6	19	6	10	-	1	46
Electronics	-	-	2	-	1	-	-	3
Groceries	-	3	16	-	2	-	-	21
Home improvement	-	2	4	-	3	-	-	9
Multiple categories	-	-	7	4	3	1	-	15
Pet shops	-	-	4	-	-	-	-	4
Skincare and perfumes	5	2	6	1	2	-	-	16
Sportswear and equipment	-	-	2	-	-	-	-	2
Vehicle and accessories	-	-	1	-	-	-	-	1
Total	9	13	61	11	21	1	1	117

From these 117 applications analysed, 15 of them refer to multiple categories of products, including clothes, cosmetics, sports, home improvement, electronics, and many others. Since it was difficult to allocate these applications to a particular category based on the market share, we considered appropriate to assign them into a distinct category.

The companies that own these applications are from 30 different countries: Australia, Brazil, Canada, Chile, Hong Kong, India, Israel, Japan, Nigeria, Russia, South Africa, South Korea, Switzerland, Turkey, United Arab Emirates, United Kingdom, United States of America, and 13 countries from the EU (Austria, Czech Republic, Finland, France, Germany, Italy, Latvia, Netherlands, Poland, Portugal, Romania, Spain, and Sweden). To have a complete understanding of what kind of data and permissions are requested by the retailing companies, we considered necessary to have a view from different countries that have a separate set of regulations regarding personal data.

The data collected from the applications and privacy policies have been analysed from different perspectives based on the research's purpose, for all of the 117 applications included in this present study. By examining the permissions and privacy policies, we used a content analysis to capture all the information put at the disposal of the smartphones' users, as this research method has an adequate level of applicability in the retail area, because it supports the avoidance of biased results and "provides an empirical starting point for generating new research evidence" (Kolbe and Burnett, 1991). We have also used statistical methods for the data collected to test if there is a significant difference between applications, depending on the companies' location.

3. Results and discussion

By analysing the permissions requested by the applications, we identified 63 different kinds of permissions, from 13 different categories: photos/media/file, storage, Wi-Fi connection information, camera, location, microphone, phone, device ID & call information, identity, device ID & app history, contacts, calendar, and others. In the Google Play market, there is a particular category, called others, where are presented the permissions that cannot be included in one of the 12 categories listed above. After collecting the data from all the applications, 1.854 permissions have been identified, an application having, on average, 16 different permissions (table no. 2).

Table no. 2. Distribution of the number of permissions of the applications analysed by category and number of downloads

Category of applications/ Number of downloads	100k+	500k+	1mil+	5mil+	10mil+	50mil+	100mil+	Average
Clothes, shoes, and accessories	49	79	300	94	177	-	31	16
Electronics	-	-	46	-	22	-	-	23
Groceries	-	35	282	-	41	-	-	17
Home improvement	-	26	51	-	52	-	-	14
Multiple categories	-	-	87	87	43	16	-	16
Skincare and perfumes	60	24	92	16	35	-	-	14

Category of applications/ Number of downloads	100k+	500k+	1mil+	5mil+	10mil+	50mil+	100mil+	Average
Pet shops	-	-	65	-	-	-	-	16
Sportswear and equipment	-	-	26	-	-	-	-	13
Vehicle and accessories	-	-	18	-	-	-	-	18
Average number of permissions per number of downloads	12	13	16	18	18	16	31	-

To achieve the **specific objective O1.1.**, we examined the 63 different types of permissions requested by the applications following their specifics. We then computed the frequency, and classified them into three categories (low, medium, and high), based on the risk of personal or sensitive data collection and exposure, correlated with the technical functionality. The majority of the permissions have a medium and high level of exposure (53.96%), while 29 permissions do not pose any significant threat to personal data.

To examine whether there is a difference between EU and non-EU countries, in terms of the number of total permissions and the number of medium and high-risk permissions per application, we conducted a one-way ANOVA test (single-factor analysis of variance) (table no. 3), using the Statistical Package for Social Sciences (SPSS). We have also included UK companies in EU countries, due to the fact that they comply with the same personal data protection regulation.

Table no. 3. ANOVA Test

Descriptive

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Min.	Max.
						Lower Bound	Upper Bound		
Total_ number_of_ permissions	Non-EU	52	17.15	5.308	.736	15.68	18.63	8	31
	EU	65	14.80	4.342	.539	13.72	15.88	6	25
	Total	117	15.85	4.916	.454	14.95	16.75	6	31
Number_of _medium_ and_high-risk_ permission	Non-EU	52	9.88	3.507	.486	8.91	10.86	3	21
	EU	65	8.20	2.694	.334	7.53	8.87	2	13
	Total	117	8.95	3.181	.294	8.37	9.53	2	21

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
Total_number_of_ permissions	1.760	1	115	.187
Number_of_medium_ and_high-risk_permission	2.926	1	115	.090

ANOVA

		Sum of Squares	Df	Mean Square	F	Sig.
Total_number_of_ permissions	Between Groups	160.062	1	160.062	6.964	.009
	Within Groups	2643.169	115	22.984		
	Total	2803.231	116			
Number_of_medium _and_high-risk_ permission	Between Groups	81.985	1	81.985	8.636	.004
	Within Groups	1091.708	115	9.493		

The result of the ANOVA analysis is showing that usually, the applications analysed where the company is in the EU have generally fewer permissions than the applications deployed by companies from countries outside the EU. This result might be an effect of the General Data Protection Regulation (GDPR) adopted in all EU states in 2018, that reinforced personal data processing rules. Although states from all over the world have privacy laws, the regulations' effect is more visible in Europe.

The application are making constant efforts to detect any malicious application. However, there has been evidence that the initial screening performed by the specialists was not always successful and led to the deployment of malware applications that had the potential of affecting the users' privacy (Rahman, et al., 2017; Bhat and Dutta, 2019), as the ability of such programs is evolving and manages to bypass the security measures (Wadkar, Di Troia and Stamp, 2020).

The awareness level of the users regarding the risks generated by the usage of mobile applications have been assessed during the last years, and the studies have highlighted that the majority is not concerned with the permissions of the applications that they are installing, or they fail to understand them (Felt, et al., 2012; Ramachandran, et al., 2017; Ngobeni and Mhlongo, 2019).

In terms of the functionality of the applications examined in this paper, we identified four substantial risks that can significantly affect the users' privacy:

- Eavesdropping – 21% of the sample analysed include this feature (record audio) to facilitate the vocal search, but malicious applications can use this permission to eavesdrop on users. Even though this phenomenon has not been identified at a large scale, it is, however, possible for an application that received this permission to eavesdrop on users (Kröger and Raschke, 2019). Analysing the companies' privacy policies that deployed these applications, we have not identified information regarding the storing methods of audio records or their future use.

- Secretly transferring data – 12% of the applications have the permission to connect and disconnect from Wi-Fi and 5% are allowed to change the network connectivity and both of these, in association with another permission, "Full network access" (that is present in all applications requiring an internet connection) can act as a malware, secretly collect, then transmit the user's data. In relation to mobile shopping, these two permissions are used to increase the customers' exposure to the offers and shopping applications.

- Install malware without the users' knowledge – in 6% of the applications analysed we identified the permission called "Download files without notification" that allows the applications to download and install programs without the knowledge of the user, even malware programs that can then be used to spy on the activity and then leak private data. Online shopping applications will use this permission to download mandatory updates without first notifying the users, avoiding, in this way, scenarios in which they might access a non-functional application.

- Gather unprovided data without the users' knowledge – a permission called "Read sensitive log data" has been identified in five cases. This allows the application to read the data provided and stored by the other applications installed and might access personal data of the user. This feature can be used to collect more information regarding the consumers and give a better personalised shopping experience, but if the data has not been provided with the users' knowledge, this practice raises some ethical questions.

Through this analysis of medium and high-risk permissions in terms of the ability to affect privacy, we achieved the specific **objective O1.1.** of the research.

The **specific objective O1.2**. imposed the retailers' privacy policies that deployed these applications. For this purpose, we identified the main types of personal data collected: full name, profile picture, delivery address, phone number, email address, credit/debit card information, passport ID, and drivers' license number. Besides these categories of data, other types of information were collected, such as location, postal code, gender, age, date of birth, hobbies, buying preferences, estimated income, shopping patterns and behaviours, the reason for purchasing a particular product, and in one case we identified that the company was storing information about the customers' education level. All these details are needed by the retailers to address the users' needs better, but they should protect personal privacy by using the best current available solutions to avoid data leakages. The majority of the companies specified in the privacy policy that they are using encryption methods to protect the data of the users transmitted via the internet, usually Secure Sockets Layer (SSL), an encryption-based Internet security protocol, but researchers have highlighted that this technology has a series of vulnerabilities, that might affect the accuracy of the data transmitted (Ramírez-López, et al., 2019; Tang, et al., 2019). Only in a limited number of cases details about how the data stored is protected were provided.

A recent experiment carried out by a well-known cybersecurity expert, Bob Diachenko, showed that unprotected databases are usually attacked 18 times per day and during the first eight hours after deploying the database, 175 attacks have been performed by hackers (Bischoff, 2020).

There are several techniques that companies can use to protect the privacy of the users, such as leveraging AI, to identify earlier data breaches and sending red flags to respond faster to a possible attack. Also, developers can train ML algorithms to categorise data based on the level of confidentiality to use the proper encryption techniques, testing and identifying potential risk areas and automatically apply patches. Since the majority of mobile applications analysed collect information about the credit/debit cards used by the customers to make payments, AI-based solutions can be used to detect any fraudulent activity based on the previous behaviour and preferences of the users.

In two cases, we identified that the retailers were collecting data about the users' income, and in one situation, information about the education level was stored. Although it might seem harmless, this kind of data can encourage algorithms to provide a biased outcome that might result in PD. Moreover, in some of the privacy policies was mentioned that the company would store any data that the user provides, an aspect that raises concerns regarding the way the information is being processed and the output provided. Wiener highlighted in 1960 that "we had better be quite sure that the purpose put into the machine is the purpose which we really desire". Although this quote is more than 60 years old, it has a pearl of significant wisdom for the current status of automation, where narrow intelligence algorithms are using all the data provided and generate an outcome based on that, so developers should act with diligence and avoid any inappropriate data processing.

The achievement of the **specific objectives O1.1. and O1.2**. led to the accomplishment of the first general research objective formulated; thus, we were able to perform an analysis of how privacy can be affected by the usage of mobile shopping applications.

Aiming to achieve the **specific objective O2.1.** we conducted a brief analysis of the main elements that determine consumers to make impulse purchases, then we examined what permissions within the analysed mobile applications can be exploited by using AI techniques to encourage the impulse buying. We also identified permissions that can be used to improve the online shopping experience.

Shoppers tend to make more impulsive purchases in stores than online (First Insight, 2019), but the reasons behind this behaviour are not fully understood. Perceived experience and a series of organic variables are making consumers keener to engage in impulse purchasing (Liu, Li and Hu, 2013), and the current shift generated by the pandemic influenced the impulsive buying habits as well (Roggeveen and Sethuraman, 2020), so retailers should find appropriate ways to create favourable environments for the clients to embrace more online shopping. While browsing on websites using smartphones can be difficult for consumer, mobile applications are more user-friendly and provide a better online shopping experience.

The main attributes that facilitate the engagement in online impulse buying are: visual appeal, ease of use, product availability, facilitated payment process, promoting intensity, and a series of organic variables such as normative evaluation and instant gratification (Liu, Li and Hu, 2013; Leong, Jaafar and Ainin, 2018). Recommendation algorithms can improve impulse buying (Hostler, et al., 2011) by gathering the users' preferences and making predictions based on previous purchases. However, developers and retailers should keep in mind that impulse buying is unplanned and spontaneous, so they should avoid obnoxious advertising and send pop-ups or notifications only at a suitable time.

Two of the applications analysed have a permission called "Read battery statistics", which allows battery data collection and, in this way, developers can predict, with the use of ML algorithms, when it is a suitable time for sending notifications so they can receive more attention from the user. This is a low-level risk permission and companies should use it more to increase the exposure time. A permission called "Reorder running apps", identified in only five applications, can be exploited to gain the clients' attention and encourage impulsive buying behaviours by exposing more the user to that application. Another permission, "Control vibrations", is present in 81% of the cases analysed and the main purpose is to draw the users' attention to the notifications sent by the application so the developers can leverage this; however, this might be considered slightly intrusive. "Run at

startup", identified in 56% of the cases, allows the application to be more visible to the consumer and increases the chances of impulsive shopping, being an efficient feature to improve the chances of accessing the online store application. Nevertheless, this advertising should be carried out ethically, without severely influencing the control of the users.

One of the most accepted applications that AI provides is augmented reality (AR) to support the decisions of the users (Alves and Reis, 2020) like the tool created by IKEA, that customers can use to decide whether a particular piece of furniture or decoration will be suitable for their house. Analysing the data collected, we identified that 79% of the applications require the permission to take pictures and videos, most of them using this feature to allow the users to upload photos and videos with their reviews, but the companies can leverage this permission by using AR techniques to allow the customers to virtually try an outfit and reduce the return ratio for clothes, shoes, and accessories. Also, for skincare and cosmetics, pictures can be uploaded for the user to decide what makeup shade to select. Another practical application to improve the shopping experience is to put at the disposal of the client AI algorithms (natural image processing and ML) that will assist them in making the right decision when looking for a particular product, based on the client's preferences. For example, the user can upload a picture with a specific outfit (85% of the applications have the permission to read the storage space) and the algorithm can make suggestions by trying to find the best match available at that particular moment.

To increase the ease of use and improve the experience, the developers could leverage another permission identified in 11% of the cases, "Create accounts and set passwords", which allows the users to connect to a specific store, without manually having to create an account, by linking the new account to the personal data stored on the phone. Although the risk of this permission is medium, using it in a proper ethical manner, the users' personal data should be collected and stored transparently.

The achievement of the **specific objective O2.2.** imposed the analysis of permissions, which, along with AI, can support increasing the level of customer engagement. We started from the idea that improving customer engagement is a critical objective in the retail industry, and companies are now interested in introducing chatbots to facilitate the interactions and provide real-time availability to the users to handle their queries. In terms of functionality, these programs can use a text-based or voice-based search (speech to text transcription). As presented above, 21% of the applications analysed asked for permission to record audio – this feature can be used by the client to discuss with the chatbots or even to do vocal searches for the products needed. Also, the users can have the possibility to review whether their demand has been solved and if the output was in line with the expectations and, in this way, the ML algorithms behind the chatbots can improve after each interaction with the client and be able to generate personalised outputs. While chatbots' acceptance rate is still relatively low, trust can be increased by being transparent with the users.

Data analytics techniques available in the online shopping applications gather data regarding the time spent by a user viewing a particular item and also how many times the application has been accessed. As presented above, the majority of the applications studied had permission to control vibration to advise the user about the notifications received. Using ML algorithms, the companies can analyse if the advertising is intrusive or not and if it can affect the clients' behaviour – for example, it can be examined if the notifications are being deleted without accessing the data. In this way, the application can be programmed to

send only several notifications per month instead of daily. By doing so, companies can improve the rating from the client by avoiding obnoxious advertising.

Conclusions

After conducting the current research, we were able to draw several conclusions regarding the practical implications and opportunities of using AI-based solutions for mobile shopping applications. From a total of 63 distinct permissions examined after analysing the 117 applications included in the study, we identified several permissions that retailers can use to enhance the online shopping experience, improve engagement, and encourage impulse buying. However, the majority of these permissions that can be successfully leveraged using AI-based solutions have been encountered only in a limited number of cases. Companies should focus more on mobile applications to facilitate the shopping experience being now able to provide a series of new services to their customers such as virtual fitting rooms, chatbots that can provide instant product recommendation and ML algorithms that search for a particular product after analysing an image provided by the user. One major drawback of the integration of AI in e-shopping seems to be the cost of adoption, an issue that we consider will start to fade once the number of AIaaS solutions increases. The majority of companies are already using a series of data analytics services provided by search engines, such as Google, to gather non-personal data about their clients, so the expectations are that most retailers will start on the medium-term leveraging AI-based solutions.

Another finding was that some of the applications ask for permissions that can affect the privacy of the users and if these permissions are exploited maliciously, they can even eavesdrop on the user, secretly collect data, and install malware programs on the personal smartphones or tablets. Therefore, it is essential for retailers when deploying AI solutions to keep in mind the customers' privacy, as data breaches pose both financial and reputational risks. Also, the statistical analysis performed showed that in the case of EU based companies, there is a lower number of total and possible harmful permissions, which highlights that these retailers might be a little more cautious regarding the privacy of individuals, even though similar regulations as in the EU started to be adopted by the majority of the countries worldwide.

After examining the privacy policies of the companies focusing on the types of data they can leverage to improve the ML algorithms for products recommendations and predict the future needs of the users, we identified that some of the companies are collecting data that can lead to biased or discriminatory algorithms, such as estimated income and level of education. Retailers have at their disposal a wide range of information to successfully develop algorithms, but they must collect only the data they will need for conducting business in an ethical manner.

Grasping AI-based solutions by embedding them in mobile shopping applications represent an excellent opportunity for retailers as the customers' preferences change and they opt for a personalised shopping experience more suitable to their needs. Since AI is a fast-developing technology, ethical and legal challenges are the main concern for researchers and developers. As the retail companies have a vast amount of structured and unstructured data at their disposal, they can lead the way in the development of ethical AI solutions that will be used for the individual and collective well-being.

In the relevant literature, the issue of privacy of the personal data provided by users represented an intensely researched topic (Rahman, et al., 2017; Bhat and Dutta, 2019;

Kröger and Raschke, 2019), as well as the analysis of the reasons that determine a consumer to make a purchase or not (Liu, Li and Hu, 2013; Leong, Jaafar and Ainin, 2018; Ho and Chung, 2020), including AI elements. However, we have not identified in the literature any study that analyses the potential of mobile application permissions to encourage the impulse buying, provide a better experience compared to visiting a physical store, and to increase customer engagement in an ethical manner, focusing on the personality and confidentiality of data provided by users to online retailers. Therefore, our study brings an element of originality to AI research in the field of retail.

The main limitation of this study is caused by the partial lack of transparency in the privacy policies, drafted by companies that use these applications for online shopping. Although these policies are public, companies, for competitiveness reasons do not fully present the processes in which they use anonymized user data; therefore, this aspect did not allow us to determine the possibility of developing subjective or discriminatory algorithms.

The present research can be continued in two directions: (1) extending the study over a more extended period to see to what extent the shopping experience has been improved as a result of using mobile applications for online commerce; and (2) analysing medium and high-risk permissions, through a comparative study in countries that have adopted GDPR and those that have not.

References

Al-Debei, M.M., Akroush, M.N. and Ashouri, M.I., 2015. Consumer attitudes towards online shopping: The effects of trust, perceived benefits, and perceived web. *Internet Research*, [e-journal] 25(5), pp.707-733. https://doi.org/10.1108/IntR-05-2014-0146.

Alguliyev, R.M., Aliguliyev, R.M. and Abdullayeva, F.J., 2019. Privacy-preserving deep learning algorithm for big personal data analysis. *Journal of Industrial Information Integration*, [e-journal] 15, pp.1-14. https://doi.org/10.1016/j.jii.2019. 07.002.

Alves, C. and Reis, J.L., 2020. The Intention to Use E-Commerce Using Augmented Reality-The Case of IKEA Place. In: Á. Rocha, C. Ferrás, C. Montenegro Marin and V. Medina García, *The 2020 International Conference on Information Technology & Systems*. Bogota, Columbia, 5-7 February 2020. Cham: Springer.

Babin, B.J., Darden, W.R. and Griffin, M., 1994. Work and/or fun: measuring hedonic and utilitarian shopping value. *Journal of consumer research*, [e-journal] 20(4), pp.644-656. https://doi.org/10.1086/209376.

Barnes, S.J., 2020. Information management research and practice in the post-COVID-19 world. *International Journal of Information Management*, [e-journal] 55, pp.1-4. https://doi.org/10.1016/j.ijinfomgt.2020.102175

Bhat, P. and Dutta, K., 2019. A survey on various threats and current state of security in android platform. *ACM Computing Surveys*, [e-journal] 52(1), pp.1-35. https://doi.org/ 10.1145/3301285.

Bischoff, P., 2020. *Unsecured databases attacked 18 times per day by hackers*. [online] Available at: <https://www.comparitech.com/blog/informati on-security/unsecured-database-honeypot/> [Accessed 12 August 2020].

Bogue, R., 2016. Growth in e-commerce boosts innovation in the warehouse robot market. *Industrial Robot*, [e-journal] 43(6), pp. 583-587. https://doi.org/10.1108/IR-07-2016-0194.

Bozdag, E., 2013. Bias in algorithmic filtering and personalization. *Ethics and information technology*, [e-journal] 15(3), pp.209-227. https://doi.org/10.1007/s10 676-013-9321-6.

Buhalis, D., Harwood, T., Bogicevic, V., Viglia, G., Beldona, S. and Hofacker, C., 2019. Technological disruptions in services: lessons from tourism and hospitality. *Journal of Service Management*, [e-journal] 30(4), pp.484-506. http://dx.doi.org/10.1108/JOSM-12-2018-0398.

Calvano, E., Calzolari, G., Denicolò, V. and Pastorello, S., 2019. Algorithmic pricing what implications for competition policy?. *Review of industrial organization*, [e-journal] 55(1), pp.155-171. https://doi.org/10.1007/s11151-019-09689-3.

Chowdhary, K.R., 2020. *Fundamentals of Artificial Intelligence*. New Delhi: Springer Nature.

Council of Europe, 2020. *CAHAI Ad Hoc Committee on Artificial Intelligence*. [pdf] Council of Europe. Available at: <https://rm.coe.int/leaflet-cahai-en-june-2020/16809ed7fd> [Accessed 28 July 2020].

De Bellis, E. and Johar, G.V., 2020. Autonomous Shopping Systems: Identifying and Overcoming Barriers to Consumer Adoption. *Journal of Retailing*, [e-journal] 96(1), pp.74-87. https://doi.org/10.1016/j.jretai.2019.12.004.

Deloitte, 2019. *Technology, Media, and Telecommunications Predictions 2020* [pdf] Deloitte Development LLC. Available at: <https://www2.deloitte.com/global/en/insights/industry/technology/technology-media-and-telecom-predictions> [Accessed 12 August 2020].

Dignum, V., 2019. *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*. New Delhi: Springer Nature.

Els, A.S., 2017. Artificial Intelligence as a Digital Privacy Protector. *Harvard Journal of Law & Technology*, 31(1), p.217.

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D., 2012. Android permissions: User attention, comprehension, and behavior. In: USENIX Association, *Proceedings of the eighth symposium on usable privacy and security*. Washington, D.C., U.S.A., July 2012. New York: Association for Computing Machinery

First Insight, 2019. *The State of Consumer Spending: In-Store Impulse Shopping Stands the Test of Time*. [online] Available at: <https://www. firstinsight.com/white-papers-posts/the-state-of-consumer-spending-report> [Accessed 12 August 2020].

Gautier, A., Ittoo, A., and Van Cleynenbreugel, P., 2020. AI algorithms, price discrimination and collusion: a technological, economic and legal perspective. *European Journal of Law and Economics*, [e-journal] pp.1-31. https://doi.org/10.1007/s10657-020-09662-6.

Girasa, R., 2020. AI as a Disruptive Technology. In: R. Girasa ed., 2020. *Artificial Intelligence as a Disruptive Technology*. Cham: Palgrave Macmillan, pp.3-21.

Goodfellow, I., Bengio, Y. and Courville, A., 2016. *Deep learning (Vol. 1)*. Cambridge: MIT press.

Gritti, C., Önen, M. and Molva, R., 2019. Privacy-preserving delegable authentication in the internet of things. In: ACM (Association for Computing Machinery), *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*. Limassol, Cyprus, 8-12 April 2019. New York: Association for Computing Machinery.

Ha, S. and Stoel, L., 2009. Consumer e-shopping acceptance: Antecedents in a technology acceptance model. *Journal of business research*, [e-journal] 62(5), pp.565-571. https://doi.org/10.1016/j.jbusres.2008.06.016.

Hannak, A., Soeller, G., Lazer, D., Mislove, A. and Wilson, C., 2014. Measuring price discrimination and steering on e-commerce web sites. In: ACM (Association for Computing Machinery), *Proceedings of the 2014 conference on internet measurement conference*. Vancouver, BC, Canada, 5-7 November 2014. New York: Association for Computing Machinery.

Hao, M., Li, H., Luo, X., Xu, G., Yang, H. and Liu, S., 2019. Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE Transactions on Industrial Informatics*, [e-journal] 16(10), pp.6532-6542. https://doi.org/10.1109/TII.20 19.2945367.

Hintze, A., 2016. *Understanding the four types of AI, from reactive robots to self-aware beings*. [online] Available at: <http://theconversation .com/understanding-the-four-types-of-ai-fromreactive-robots-to-self-aware-beings-67616> [Accessed 14 August 2020].

Hirschman, E.C., 1992. The consciousness of addiction: Toward a general theory of compulsive consumption. *Journal of Consumer Research*, [e-journal] 19(2), pp.155-179. https://doi.org/10.1086/209294.

Ho, M.H.W. and Chung, H.F., 2020. Customer engagement, customer equity and repurchase intention in mobile apps. *Journal of Business Research*, [e-journal] 121, pp.13-21. https://doi.org/10.1016/j.jbusres.2020.07.046

Hostler, R.E., Yoon, V.Y., Guo, Z., Guimaraes, T. and Forgionne, G., 2011. Assessing the impact of recommender agents on on-line consumer unplanned purchase behavior. *Information & Management*, [e-journal] 48(8), pp.336-343. https://doi.org/10.1016/ j.im.2011.08.002.

Kolbe, R.H. and Burnett, M.S., 1991. Content-analysis research: An examination of applications with directives for improving research reliability and objectivity. *Journal of consumer research*, [e-journal] 18(2), pp.243-250. https://doi.org/10. 1086/209256.

Kreutzer, R.T. and Sirrenberg, M., 2020. *Understanding Artificial Intelligence*. Switzerland: Springer Nature Switzerland AG

Kröger, J.L. and Raschke, P., 2019. Is my phone listening in? On the feasibility and detectability of mobile eavesdropping. In: S. Foley, *33th IFIP Annual Conference on Data and Applications Security and Privacy*. Charleston, U.S.A., 15-17 July 2019. USA: Springer.

Lambrecht, A. and Tucker, C., 2019. Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads. *Management Science*, [e-journal] 65(7), pp.2966-2981. https://doi.org/10.1287/ mnsc.2018.3093.

Larson, J., Mattu, S. and Angwin, J., 2015. Unintended Consequences of Geographic Targeting. *Technology Science*, [e-journal]. http://dx.doi.org/10.7910/DVN/ VEBPCZ.

LeCun, Y., Bengio, Y. and Hinton, G., 2015. Deep learning. *Nature*, [e-journal] 52, pp.436-444. doi:10.1038/nature14539.

Leong, L.Y., Jaafar, N.I. and Ainin, S., 2018. The effects of Facebook browsing and usage intensity on impulse purchase in f-commerce. *Computers in Human Behavior*, [e-journal] 78(1), pp.160-173. https://doi.org/10.1016/j.chb.2017.09.033.

Li, X., Zhao, X. and Pu, W., 2020. Measuring ease of use of mobile applications in e-commerce retailing from the perspective of consumer online shopping behaviour patterns. *Journal of Retailing and Consumer Services*, [e-journal] 55, pp. 1-12.

Lian, J.W. and Yen, D.C., 2014. Online shopping drivers and barriers for older adults: Age and gender differences. *Computers in Human Behavior*, [e-journal] 37, pp.133-143. https://doi.org/10.1016/j.chb.2014.04.028.

Liu, Y., Li, H. and Hu, F., 2013. Website attributes in urging online impulse purchase: An empirical investigation on consumer perceptions. *Decision Support Systems*, [e-journal] 55(3), pp.829-837. https://doi.org/10.1016/j.dss.2013.04.001.

Luce, L., 2018. *Artificial Intelligence for Fashion: How AI is Revolutionizing the Fashion Industry.* San Francisco: Apress.

Mazurek, G. and Małagocka, K., 2019. Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, [e-journal] 6(4), pp.344-364. https://doi.org/10.1080/23270012.2019.1671243.

Natarajan, T., Balasubramanian, S.A. and Kasilingam, D.L., 2017. Understanding the intention to use mobile shopping applications and its influence on price sensitivity. *Journal of Retailing and Consumer Services*, [e-journal] 37, pp.8-22. https://doi.org/10.1016/j.jretconser.2017.02.010.

Ngobeni, A. and Mhlongo, S., 2019. Towards Enhancing Security in Android Operating Systems–Android Permissions & User Unawareness. In: IEEE, *2019 2nd International Conference on Computer Applications & Information Security*. Riyadh, Saudi Arabia, 1-3 May 2019. Riyadh: IEEE

Nguyen, H.V., Tran, H.X., Van Huy, L., Nguyen, X.N., Do, M.T. and Nguyen, N., 2020. Online Book Shopping in Vietnam: The Impact of the COVID-19 Pandemic Situation. *Publishing Research Quarterly*, [e-journal] 36, pp.437-445. https://doi.org/10.1007/s12109-020-09732-2

Perrault, R., Shoham, Y., Brynjolfsson, E., Clark, J., Etchemendy, J., Grosz, B., Lyons, T., Manyika, J., Mishra, S. and Niebles, J.C., 2019. *Artificial Intelligence Index Report 2019*. [pdf] Stanford: Stanford University. Available at: <https://hai.stanford.edu/sites/default/files/ai_index_2019_report.pdf> [Accessed 28 July 2020].

Polacco, A. and Backes, K., 2018. The amazon go concept: Implications, applications, and sustainability. *Journal of Business and Management*, [e-journal] 24(1), pp.79-92. http://dx.doi.org/10.6347%2fJBM.201803_24(1).0004.

Poushneh, A. and Vasquez-Parraga, A.Z., 2017. Discernible impact of augmented reality on retail customer's experience, satisfaction and willingness to buy. *Journal of Retailing and Consumer Services*, [e-journal] 34, pp.229-234. https://doi.org/ 10.1016/j.jretconser.2016.10.005.

Rahman, M., Rahman, M., Carbunar, B. and Chau, D.H., 2017. Search rank fraud and malware detection in Google Play. *IEEE Transactions on Knowledge and Data Engineering*, [e-journal] 29(6), pp.1329-1342. https://doi.org/10.1109/TKDE.2017.2667658.

Ramachandran, S., Dimitri, A., Galinium, M., Tahir, M., Ananth, I.V., Schunck, C.H. and Talamo, M., 2017. Understanding and granting android permissions: A user survey. In: J. Ortega-Garcia, *2017 International Carnahan Conference on Security Technology*. Madrid, Spain, 23-26 October 2017. Spain: IEEE.

Ramírez-López, F.J., Varela-Vaca, Á.J., Ropero, J., Luque, J. and Carrasco, A., 2019. A Framework to Secure the Development and Auditing of SSL Pinning in Mobile Applications: The Case of Android Devices. *Entropy*, [e-journal] 21(12), p.1136. https://doi.org/10.3390/e21121136.

Rese, A., Ganster, L. and Baier, D., 2020. Chatbots in retailers' customer communication: How to measure their acceptance?. *Journal of Retailing and Consumer Services*, [e-journal] 56, pp.102-176. https://doi.org/10.1016/j.jretconser. 2020.102176.

Roggeveen, A.L. and Sethuraman, R., 2020. How the COVID Pandemic May Change the World of Retailing. *Journal of Retailing*, [e-journal] 96(2), pp. 169-171. https://doi.org/10.1016/j.jretai.2020.04.002.

Shankar, V., 2018. How artificial intelligence (AI) is reshaping retailing. *Journal of retailing*, [e-journal] 94(4), pp.vi-xi. https://doi.org/10.1016/S0022-4359(18)30076-9.

Singh, S.K., Rathore, S. and Park, J.H., 2020. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*, [e-journal] 110, pp.721-743. https://doi.org/10.1016/j. future.2019.09.002

Singireddy, S.R.R. and Daim, T.U., 2018. Technology Roadmap: Drone Delivery–Amazon Prime Air. In: T. Daim, L. Chan and J. Estep eds., 2018. *Infrastructure and Technology Management*. Cham: Springer, pp. 387-412.

Spiegel, J.R., Mckenna, M.T., Lakshman, G.S. and Nordstrom, P.G., Amazon Technologies Inc., 2011. *Method and system for anticipatory package shipping*. U.S. Pat. 8,086,546.

Taati, B., Zhao, S., Ashraf, A.B., Asgarian, A., Browne, M.E., Prkachin, K.M., Mihailidis, A. and Hadjistavropoulos, T., 2019. Algorithmic bias in clinical populations – evaluating and improving facial analysis technology in older adults with dementia. *IEEE Access*, [e-journal] 7, pp.25527-25534. https://doi.org/10.1109/ACCESS.2019. 2900022.

Tang, J., Li, J., Li, R., Han, H., Gu, X. and Xu, Z., 2019. SSL Detecter: Detecting SSL Security Vulnerabilities of Android Applications Based on a Novel Automatic Traversal Method. *Security and Communication Networks*, [e-journal] 2019, pp.1-21. https://doi.org/10.1155/2019/7193684.

The New York City Council, 2017. *A Local Law in relation to automated decision systems used by agencies. Technical Report*. [pdf] The New York City Council. Available at: <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=313781 5&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0> [Accessed 28 July 2020].

Thinyane, H. and Sassetti, F., 2020. Towards a Human Rights-Based Approach to AI: Case Study of Apprise. In: UNU-CS United Nations University Institute on Computing and Society, *11th International Development Informatics Association Conference*. Online, 25-27 May 2020. Macau: Springer Nature Switzerland AG.

Wadkar, M., Di Troia, F. and Stamp, M., 2020. Detecting malware evolution using support vector machines. *Expert Systems with Applications*, [e-journal] 143, p.1-22. https://doi.org/10.1016/j.eswa.2019.113022.

Wiener, N., 1960. Some moral and technical consequences of automation. *Science*, 131(3410), pp.1355-1358.