

## ARTICLES

# Artificial Intelligence and Customer Relationship Management

## The Case of Chatbots and Their Legality Framework

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka\*

### Abstract

*In the new digital era as it is formed by the European digital strategy, the explosion of e-commerce and related technologies has led to the formation of tremendous volumes of customer data that could be exploited in a variety of ways. Customer relationship management (CRM) systems can now exploit these data sets to map consumers' behaviour more effectively. As social media and artificial intelligence widened their penetration, firms' interest shifted to chatbots in order to serve their customers' needs. Nowadays, CRM and bots are developed in a parallel way. With the help of these virtual personal assistants, CRM establishes a virtual relationship with consumers. However, the extended collection and use of personal data under this scope may give rise to ethical and legal issues. In this article, the term CRM is defined, followed by an analysis of the way chatbots support CRM systems. In the second part, the legal context of chatbot use will be highlighted in an attempt to investigate whether there are personal data protection issues and whether certain rights or ethical rules are somehow violated. The draft AI Regulation, in combination with the provisions of GDPR and e-Privacy Directive, offers a significant background for our study. The article concludes by demonstrating the use of chatbots as an inherent part of the new digital era and lays special emphasis on the term 'transparency', which seems to penetrate the lawfulness of their use and guarantee our privacy.*

**Keywords:** artificial intelligence, chatbots, CRM, data protection, privacy.

\* Konstantinos Kouroupis: Assistant Professor of European and Data Rights Law, Department of Law, Frederick University, Cyprus. Dimitrios Vagianos: Electrical & Computer Engineer, Laboratory Teaching staff, Department of International and European Studies, University of Macedonia, Greece. Aikaterini Totka: Graduate Student, Department of International and European Studies, University of Macedonia, Greece.

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka

## A Chatbots in Customer Relations Management (CRM)

### I CRM: An Introduction

The birth of the customer relationship management (CRM) system is inextricably linked to the emergence of marketing philosophy. It all started in the 1960s, when firms' interest shifted from recurring sales to the substantial satisfaction of consumer needs. Their goal was thus to identify, through marketing research, the needs of consumers and not to sell a large number of products that did not really meet their needs.<sup>1</sup> This new marketing philosophy contributed to the 'birth' of CRM systems.

In the early 1990s, with the invention of the World Wide Web (www), which allowed Internet users to search for information by moving from one document to another, companies faced many difficulties in organizing the vast amount of data created by customers. In response, specialists developed hardware and software solutions to better handle this huge volume of customers' information. Sales Force Automation (SFA) and customer service support were parts of these new technologies. With their help, firms could analyse consumers' behavioural patterns more effectively and build trustworthy relationships with them. As time passed, marketing specialists started to use the term 'CRM' to refer to the improvement between firms' and customers' relationships.<sup>2</sup>

The extended use of the CRM system led to various definitions as an attempt to describe its main characteristics. At the beginning, as Buttle and Maklan report,<sup>3</sup> Internet experts usually defined CRM as "an information industry term for methodologies, software and usually Internet capabilities that help an enterprise manage customer data in an organized way". For them, CRM was considered a technological tool, which offered the possibility to manage customers' data. Nowadays, companies present CRM not only as a software but also as a process, philosophy and intention to fulfil customers' needs and desires. As they mention, CRM is the process of managing all aspects of interaction a company has with its customers, including prospecting, sales, and service. CRM applications attempt to improve the company/customer relationship by combining all these views of customer interaction into one picture. CRM's primary goal is to improve long-term growth through a better understanding of customer needs and behavior.

This strategic approach emphasizes the whole journey, from gaining a customer to turning him/her into a loyal and profitable advocate.<sup>4</sup> There are also the supporters of the managerial approach, who link the CRM system with the customer experience (CX) movement. This movement attempts to improve the experience of customers as they interact with the company. When a company adopts effective CRM

1 K. Tzortzakis & A. Tzortzaki, *Marketing Principles: The Greek Approach* (in Greek), 2nd ed., Gerakas, Rosili, 2002, pp. 38-39.

2 H. Karjaluoto, H. Kuusela & H. Saarijärvi, 'Customer Relationship Management: The Evolving Role of Customer Data', *Marketing Intelligence & Planning*, Vol. 31, No. 6, 2013, pp. 1-4.

3 F. Buttle & S. Maklan, *Customer Relationship Management: Concepts and Technologies*, 4th ed., Routledge, 2019, pp. 3-4.

4 Buttle and Maklan, 2019, p. 4.

technologies, consumers and customers have the possibility to better interact with that company, by having a greater experience.<sup>5</sup>

## II CRM Use

CRM practices are extremely beneficial not only for the company itself but also for the customer. A host of benefits accrue at both the managerial and the CX levels. The organizational benefits can be considered to be the following:

*Improving Customer Services:* As Mohammadhossein and Zakaria explain,<sup>6</sup> CRM services help firms to manage customers' requests. For example, a call centre software connects customers with employees who can give a solution to their problem. High-quality services boost the company's revenue and increase customer retention.

*Customer Segmentation:* Segmentation is defined as the classification of objects that have similar characteristics into the same groups. In CRM, customers are classified according to certain variables, for example demographics, into target groups. These segments help companies to find more easily and personalize customer needs.<sup>7</sup>

*Improve Customization of Marketing:* As CRM systems can capture customers' needs, a company can possibly invest its resources properly and customize the right product for each customer.<sup>8</sup>

*Organization:* CRM allows firms to organize and automate some of their components such as marketing processes, business analytics of customers' data, business workflows and communication with suppliers. Thus, companies are organized more easily and efficiently.<sup>9</sup>

Proper implementation of CRM strategies can enhance the customer experience and loyalty. For example, with the right application of technologies, which consists partly of operational CRM, a company aims at recognizing better customers' needs or communicating with them more accurately and reliably. Also, when analytical CRM works well, customers receive more personalized and on-time offers, because experts can detect their actual desires.<sup>10</sup> Therefore, they are more satisfied and willing to purchase products or services again from the same firm.

Among the companies that first applied CRM techniques are Apple and Amazon. When consumers buy an Apple device, they are asked to create an Apple

5 *Ibid.*, p. 5.

6 N. Mohammadhossein & H. Zakaria, 'CRM Benefits for Customers: Literature Review (2005-2012)', *International Journal of Engineering Research and Applications*, Vol. 2, No. 6, 2012, p. 1582.

7 *Ibid.*

8 *Ibid.*, p. 1583.

9 J. Kulpa, 'Council Post: Why Is Customer Relationship Management So Important?' [online], *Forbes*, 2017. Available at: [www.forbes.com/sites/forbesagencycouncil/2017/10/24/why-is-customer-relationship-management-so-important/?sh=2e364abb7dac](http://www.forbes.com/sites/forbesagencycouncil/2017/10/24/why-is-customer-relationship-management-so-important/?sh=2e364abb7dac).

10 F. Buttle, *Customer Relationship Management Concepts and Technologies*, 2nd ed., Elsevier, 2009, pp. 178-179.

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka

ID – a unique account that synchronizes their information across all Apple devices they may have.<sup>11</sup> These accounts save their preferences and allow Apple to provide more personalized recommendations on the basis of their interest and previous search history. For consumers this is a convenient and time-saving solution. These accounts constitute a part of Apple's CRM strategy and therefore provide data that allow insights about costumers' needs as well as building the potential for implementing targeted marketing techniques.<sup>12</sup>

Amazon is the most well-known platform for online purchases. One of the main reasons underlying its success is the ideal utilization of the CRM system. When customers purchase an item from Amazon, they need to create a private account. This gives Amazon the possibility to track their purchases and browse their purchasing history to effectively build more personalized marketing and email campaigns. Moreover, Amazon offers the ability to adjust their accounts to carry out purchases in one click. Consumers really appreciate the fast checkout processes and the targeted product proposals. The better experience they have, the more likely they are to become loyal customers.<sup>13</sup>

In recent years the field of artificial intelligence (AI) has been growing rapidly. According to Frankenfield,<sup>14</sup> AI is the simulation of human intelligence in machines that are programmed to act like humans and mimic their behaviours. AI methods and technologies are not used for scientific reasons alone. Nowadays, businesses leverage AI technology for administrative, managerial or marketing purposes. One example is the use of AI 'bots' or, more precisely, 'chatbots', by firms in order to optimize their CRM system.<sup>15</sup>

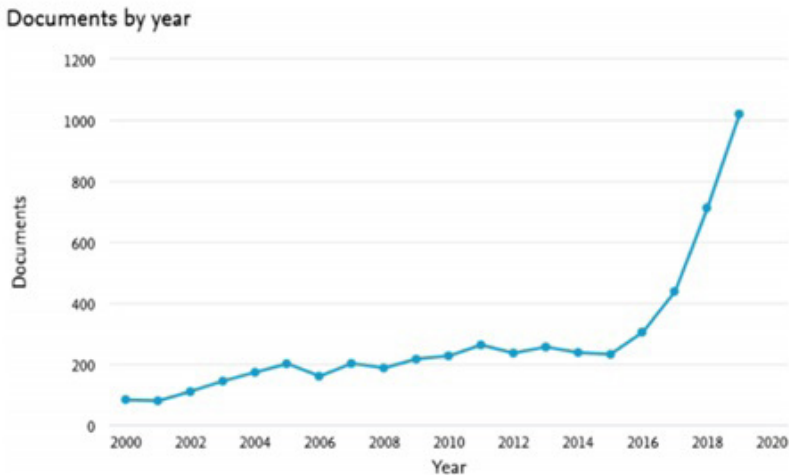
### III *The Rise of Chatbots*

Botadra<sup>16</sup> points out that a bot is also referred to as Web Robot, Internet Bot, Spider or WWW Bot. The first bot in history (1964) was ELIZA, whose purpose was to mimic a psychotherapist by using Natural Language Processing programming. The user asked a question, and ELIZA would answer by following the program code. With time, various bots were introduced: Siri, by Apple in 2013; Alexa, by Amazon in 2014; or Cortana, by Microsoft in 2014. Bots are software applications that automate specific tasks pretty fast<sup>17</sup> and in a seamless way,<sup>18</sup> assigned to them

- 11 R. Binns, 'Case Study: How Apple Have Mastered CRM', Expert Market [online], 2020. Available at: [www.expertmarket.co.uk/crm-systems/apple-crm-case-study](http://www.expertmarket.co.uk/crm-systems/apple-crm-case-study).
- 12 P. Singh, 'Top 5 Customer Relationship Management Examples'. [online] appvizer.com, 2020. Available at: [www.appvizer.com/magazine/customer/client-relationship-mgt/customer-relationship-management-examples#1-apple-crm](http://www.appvizer.com/magazine/customer/client-relationship-mgt/customer-relationship-management-examples#1-apple-crm).
- 13 *Ibid.*
- 14 J. Frankenfield, 'How Artificial Intelligence Works'. [online] Investopedia, 2020. Available at: [www.investopedia.com/terms/a/artificial-intelligence-ai.asp](http://www.investopedia.com/terms/a/artificial-intelligence-ai.asp).
- 15 P. Gentsch, *AI in Marketing, Sales and Service: How Marketers Without a Data Science Degree Can Use AI, Big Data and Bots*, Cham, Springer, 2019, p. 3.
- 16 B. Botadra, 'Web Robots or Most commonly known as Bots', p. 2. Available at: [www.academia.edu/37700458/Web\\_Robots\\_or\\_Most\\_commonly\\_known\\_as\\_Bots](http://www.academia.edu/37700458/Web_Robots_or_Most_commonly_known_as_Bots).
- 17 *Ibid.*
- 18 HubSpot Research, p. 4. Available at: [https://cdn2.hubspot.net/hubfs/53/assets/hubspot.com/research/reports/What\\_is\\_a\\_bot\\_HubSpot\\_Research.pdf?t=1492209311951](https://cdn2.hubspot.net/hubfs/53/assets/hubspot.com/research/reports/What_is_a_bot_HubSpot_Research.pdf?t=1492209311951).

through coding. Bots can be<sup>19</sup> chatbots, crawlers, transaction bots, informational or entertainment bots. On the other hand, they can perform harmful tasks and therefore can be hacking bots, spam bots, scrapers, impersonators or zombie bots (Figure 1).

**Figure 1** Search results in Scopus by year for ‘chatbot’ or ‘conversational agent’ or ‘conversational interface’ as keywords from 2000 to 2019 (Source: Adamopoulou and Moussiades, 2020, p. 375)



‘Chatbots’ are a category of bots that act online in chat or messaging platforms like Facebook, Messenger and so on. Botadra<sup>20</sup> and Aberer *et al.*<sup>21</sup> explain that these bots have the ability to carry out a conversation with humans. There is a small promise in word ‘chatbots’. These bots are designed to perform a conversation and interact with users via auditory and textual methods. Brandtzaeg and Følstad<sup>22</sup> define chatbots as machine agents that serve as natural language user interfaces to data and services through text or voice. Chatbots allow users to ask questions or make commands in their everyday language and get the needed content or service in a conversational style.

19 Botadra, p. 3.

20 *Ibid.*, p. 7.

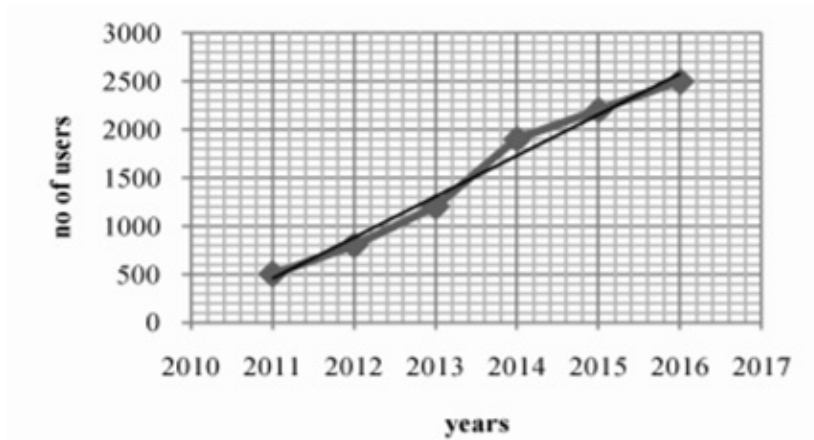
21 K. Aberer, K. Fawaz, H. Harkous & K. Shin, ‘PriBots: Conversational Privacy with Chatbots’, 2016. Available at: [www.researchgate.net/publication/305567688\\_PriBots\\_Conversational\\_Privacy\\_with\\_Chatbotsact\\_com](http://www.researchgate.net/publication/305567688_PriBots_Conversational_Privacy_with_Chatbotsact_com). ‘What Is CRM: A Definition of CRM and Its Meaning’, p. 1. Available at: [www.act.com/what-is-crm](http://www.act.com/what-is-crm).

22 P. Brandtzaeg & A. Følstad, ‘Chatbots: Changing User Needs and Motivations’, *Interactions*, Vol. 25, No. 5, 2018, p. 40.

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka

Chatbots have been around since 1964, but their real expansion was in 2016, when Facebook and Messenger allowed firms to place chatbots on their social networking platforms (Figure 2).<sup>23</sup>

**Figure 2** Graph to show usage of messaging applications (Source: Choudhury et al., 2016; p. 323)



#### IV Chatbots Classification

Chatbots' classification is based on parameters (Figure 3) such as knowledge domain, service provided goal, and input processing and response generation method.<sup>24</sup>

##### 1 Knowledge Domain

This classification concerns the amount of data a chatbot can handle and the level of its knowledge.<sup>25</sup> *Open Domain chatbots* can talk about general topics and respond in an appropriate way. Siri and Alexa are well-known examples of this case.<sup>26</sup> *Closed Domain bots*' knowledge is specified in a particular topic. For example, a restaurant bot would be able to book a table or to take an order but would not be able to tell how the weather is.

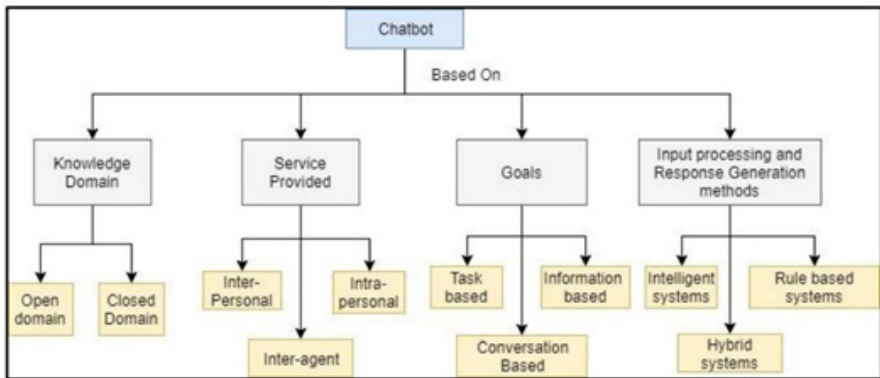
23 Brandtzaeg and Følstad, 2018, p. 38.

24 K. Nimavat & T. Champaneria, 'Chatbots: An Overview. Types, Architecture, Tools and Future Possibilities', *International Journal for Scientific Research & Development*, Vol. 5, No. 7, 2017, p. 1019.

25 E. Adamopoulou & L. Moussiades, 'An Overview of Chatbot Technology', *IFIP International Conference on Artificial Intelligence Applications and Innovations*, 2020, pp. 377-378.

26 Nimavat and Champaneria, 2017.

**Figure 3** Classification of chatbots (Source: Nimavat and Champaneria, 2017; p. 1020).



## 2 Service Provided

This categorization concerns the bots' sentimental proximity to the user, its level of interaction and the task that a bot performs. *Interpersonal chatbots* do not consist of a companion for the user but are designed in order to pass him information about a service such as restaurant booking or flight booking. They are not obliged to be friendly or to remember user's information. *Intrapersonal bots* exist within the user's personal domain such as apps like WhatsApp or Messenger. Their main purpose is to perform tasks related to the user's personal account such as managing calendar, storing the user's opinions or photos and so on. *Inter-agent* bots dominate in the AI area. They have the ability to communicate with other bots. As bots become omnipresent, the need for protocols to achieve such kind of communication is growing rapidly. While a chatbot cannot be completely inter-agent, it can be a service that handles other bots or services. Amazon's bot Alexa is a great example. A user can purchase from Amazon a device that has inside it bot technology and several protocols. When it is time to go to bed, he or she can say, "Alexa, could you please switch off the lights?"<sup>27</sup>

## 3 Goals

Bots can also be classified on the basis of what their goal is. *Informative* bots aim at providing users with information that is already stored or available from a fixed site. Most of the time they are based on an information retrieval algorithm. An example of such a bot is FAQ chatbots. *Conversational chatbots'* purpose is to talk to the user like another human being. Siri, Alexa, and so on can carry out conversations by correctly answering questions in a sentence posed by a human. Eventually, *task-based bots* are capable of performing some specific tasks, such as booking a

27 *Ibid.*, 2017, p. 1020.

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka

flight. Their intelligence lies in asking for information and understanding users' input.<sup>28, 29</sup>

#### 4 *Input Processing and Response Generation Method*

This classification is based on the methods of generating responses and processing inputs. *Intelligent systems* create responses and use natural language systems to understand the question. They are used when ample data are available. *Ruled-based bots* are used when the possible scenarios and outcomes are fixed. *Hybrid bots* do not belong to one category alone. Some bots, for example, have conversational capabilities but can also store data.<sup>30</sup>

#### V *Chatbots and CRM Systems*

The rise of chatbots is inextricably linked with the expansion of social media. On average, people are spending most of their time on messaging platforms like Facebook or Messenger, and 2.5 billion users have at least one messaging app installed in their phones.<sup>31</sup> In 2017, for example, Messenger had 1.2 billion active users.<sup>32</sup> Another interesting fact is the phenomenon of 'app fatigue'. App platforms, such as Apple's Appstore, offer a tremendous number of apps, but users are unwilling to add new apps to their smartphones. A recent study in 2016 has shown that 80% of a person's online time is dedicated only to apps such as Facebook, Messenger, Instagram or Google and that nine out of the top ten most used apps were created by Facebook and Google.<sup>33</sup>

These fundamental changes in the behaviour of online users led companies to adopt the chatbot technology. Nowadays, firms leave aside the creation of new apps and prioritize chatbots in order to reach their audience. Not only technology legends like Google and Amazon but also customer service companies like Starbucks tend to reach their customers using chatbots. By 2021, more than 50% of companies will have invested on chatbot or bot technology rather than on traditional app creation.<sup>34</sup>

The mechanism that led chatbots to be part of the firms' CRM system is explained shortly. Companies consider that, in general, the main motivation for someone to use a chatbot is to obtain specific service or information. In response, they use chatbots mainly for customer support. With customer support a company helps or gives advice to its clients.<sup>35</sup> These humanized interfaces (chatbots) provide

28 Adamopoulou and Moussiades, 2020.

29 Nimavat and Champaneria, 2017, p. 1020.

30 *Ibid.*

31 Aberer *et al.*, 2016.

32 Brandtzaeg and Følstad, 2018.

33 HubSpot Research, pp. 5-6.

34 Brandtzaeg and Følstad, 2018.

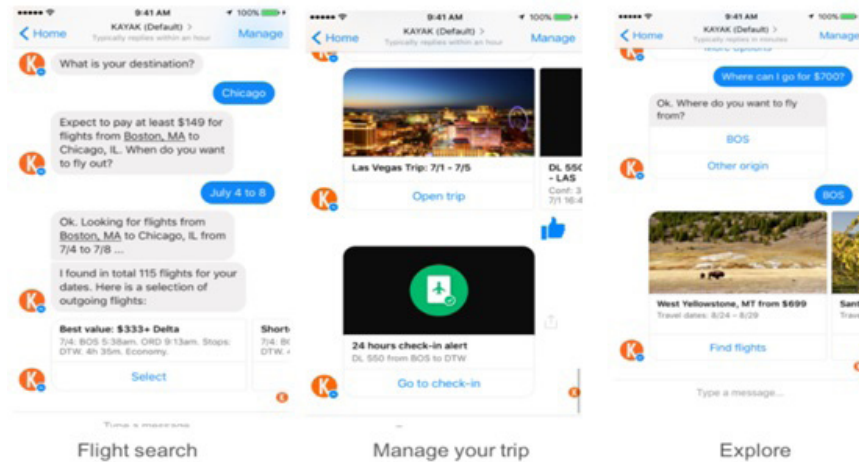
35 A. Følstad, M. Skjuve & P.B. Brandtzaeg, 'Different Chatbots for Different Purposes: Towards a Typology of Chatbots to Understand Interaction Design', in S. Bodrunova *et al.* (Eds.), *Internet Science*, Cham, Springer, 2019, p. 6.



a personalized, more automated 24/7 support.<sup>36</sup> The chatbot learns a lot of things about customers' needs. It acts like a friend who understands their wishes and fulfils them. They are also designed to be fully personalized and to optimize customer satisfaction and increase firms' sales. These automated assistants help the CRM system to fulfil its primary goal, that is, to better understand customers' needs and establish long-term relationships with them.<sup>37</sup>

Here are some case studies. British Airways has a chatbot in Messenger app. This bot includes events that happen in London, provides hotel discounts and sells tickets. Moreover, a well-known example is the Kayak Facebook Messenger bot (Figure 4), which provides information about discounts on flight tickets and hotels and also keeps records of previous conversations and uses Kayak search history to personalize its content. The fact that this bot has an internal database with customers' previous purchases and reviews makes the communication between the company and its customers more efficient. An extended personalization is achieved with chatbot 'Alexa', which is directly connected to Amazon's CRM. Several of Amazon's devices, such as Amazon Echo, are powered by Alexa, a voice personal assistant that accompanies the user all the time. Some of its main abilities are playing music, informing about the weather, ordering food or finding the nearest store. This bot consists of a digital entity, which acts on behalf of the customers and improves Amazon's CRM by personalizing their profile or storing their data. Hence, Amazon can track their desires and create efficient marketing campaigns.<sup>38</sup>

**Figure 4** Kayak Facebook Messenger Bot (Source: chatbotguide.org).



36 A. Bergner & C. Hildebrand, 'AI-Driven Sales Automation: Using Chatbots to Boost Sales', *NIM Marketing Intelligence Review*, Vol. 11, No. 2, 2019, p. 36.

37 P. Gentsch, *AI in Marketing, Sales and Service: How Marketers Without a Data Science Degree Can Use AI, Big Data and Bots*, Cham, Springer, 2019, p. 113.

38 *Ibid.*, p. 116.

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka

Undeniably, chatbots can be considered ‘tiny’ treasures that help CRM to optimize company’s interactions with its clients. For this reason, a chatbot is designed to be a friendly automated personal assistant with the ability to engage with the customer in more natural dialogue for enhancing his or her trust and experience. A study has shown that many clients put too much trust in advice provided by an automated assistant and are more willing to accept an incorrect recommendation from a chatbot rather than from a traditional adviser. Additionally, a bot is created to personalize customers’ characteristics and store an incredible volume of their data. As a result, by interacting with it, people are not seeing a machine but rather another human who can understand their needs, provide them with a service and suggest solutions to their problems. Hence, consumers have a highly relative and intimate attitude towards a company and are willing to pay higher prices to purchase a product or service (brand loyalty).<sup>39</sup>

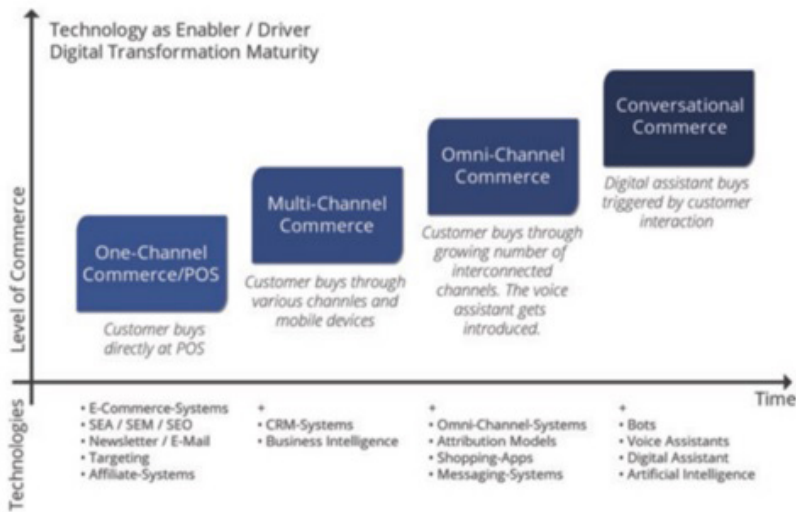
#### *VI Reshaping E-Commerce*

Digitalization is the driving force behind the evolution of e-commerce. As shown in the following Figure 5, in the first stage we had ‘one-channel’ commerce. Customers were buying their products directly from the store. What was new was that they had the possibility to pay using a point of sale (POS). Companies, from their side, were using simple marketing strategies like direct email and advertisement, especially on TV. This level can also be defined as e-commerce 1.0.<sup>40</sup> The extended use of Internet led companies to create online channels such as e-shops or accounts on social platforms.

39 Bergner and Hildebrand, 2019, pp. 38-39.

40 Gentsch, 2019, p. 117.

**Figure 5** *Digital transformation in e-commerce: maturity road to Conversational Commerce (Source: Gentsch, 2019; p. 117).*



This was when ‘multichannel’ commerce or e-commerce 2.0 was born. Firms were now able to sell products or services through different channels.<sup>41</sup> This type of commerce looks like a wheel. At its centre lies the product, and on the rim of the wheel are all the channels from which the customer can find the product, such as retail stores, online catalogues and websites.<sup>42</sup> The problem, here, is that these channels are not connected. The customer has no interaction with the channels, and companies do not control channel integration.<sup>43</sup> Because each channel works separately from the other, customers need to navigate through different ones to find the appropriate information.<sup>44</sup>

In response to this problem, e-commerce 3.0 strode onto the stage. In omnichannel commerce customers can choose products through a rich variety of channels, with which they can interact.<sup>45</sup> Now at the centre of the wheel is the customer, and on its rim are the various interconnected channels.<sup>46</sup> Customers’ experience is enhanced for two reasons: at first, they are not obliged to jump from channel to channel because each one provides the same information and, secondly, companies’ focus on their needs optimizes their experience.<sup>47</sup>

41 N. Beck & D. Rygl, ‘Categorization of Multiple Channel Retailing in Multi-, Cross-, and Omni-Channel Retailing for Retailers and Retailing’, *Journal of Retailing and Consumer Services*, Vol. 27, 2015, p. 174.

42 N. Winkler, ‘Omnichannel Vs Multichannel: What Is the Difference?’ [online] Shopify Plus, 2019. Available at: [www.shopify.com/enterprise/omni-channel-vs-multi-channel](http://www.shopify.com/enterprise/omni-channel-vs-multi-channel).

43 Beck and Rygl, 2015.

44 Omnisend Blog, ‘Omnichannel Vs. Multichannel: How to Know the Difference’, 2020. Available at: [www.omnisend.com/blog/omnichannel-vs-multichannel/](http://www.omnisend.com/blog/omnichannel-vs-multichannel/).

45 Beck and Rygl, 2015, p. 175.

46 Winkler, 2019.

47 Omnisend Blog, 2020.

The last stage is Conversational Commerce. Owing to the extensive use of messenger apps and the advances in AI, e-commerce 4.0 is the new trend. This stage features intelligent personal assistants (chatbots), who can interact with customers and fulfil their needs in an automated way. All the channels of a company are interconnected, but customers can also communicate through these channels with personal assistants to ask questions and purchase a product or service. For example, Uber collaborated with Facebook so that customers could book their rides in a seamless way via a messenger chatbot. In this new era, e-commerce is becoming increasingly automated, and customers are having an even stronger connection with the companies.<sup>48</sup>

### VII Privacy Issues

While users appreciate the guidance and support a chatbot can provide, they also have to share a huge volume of personal information with the chatbot to receive the correct recommendations. By doing this, a firm stores a lot of data about customers, who are sometimes unaware of this. Hence, privacy concerns have been engendered to a great extent. A recent study shows that consumers worry about privacy and security concerning the interaction with chatbots. This concern, according to another study, can limit consumers' willingness to use a chatbot.<sup>49</sup>

Data protectionists criticize the way companies collect and use our data and emphasize that we need to be aware of the data we share.<sup>50</sup> People share a lot of information, such as their location, name and purchasing history, with a chatbot, and, interestingly, they are often unaware of this. Most of them look at the convenience of talking with a bot, ignoring the consequences. For example, new research from the Northeastern University provides support for the idea that Amazon's Alexa records 'accidentally' everything we say.

This personal assistant collects data even when a user does not interact with it. It has been proven that Alexa is self-activated and records as much as 40 seconds of audio information each time.<sup>51</sup> By tracking our location and creating a vast amount of metadata, either accidentally or not, Amazon knows everything about every customer. Although it is beneficial for marketing strategies, Amazon has the possibility to share our information with other organizations.<sup>52</sup>

Another similar example is Google Assistant. This bot recommends nearby places to eat, provides weather updates and personalizes our needs. However, it has been argued that users are sometimes being recorded without saying the trigger phrase 'hey Google'. There are witnesses that personal assistants like Siri, Cortana and Google are activated because they thought that someone said the

48 T. Choudhury, P. Kumar & N. Piyush, 'Conversational Commerce a New Era of E-Business', *International Conference System Modeling & Advancement in Research Trends (SMART)*, 2016, p. 323.

49 C. Ischen, T. Araujo, H. Voorveld, G. van Noort & E. Smit, 'Privacy Concerns in Chatbot Interactions', in A. Følstad *et al.* (Eds.), *Chatbot Research and Design*, Cham, Springer, 2019, pp. 1, 3.

50 Gentsch, 2019, p. 116.

51 S. Morrison, 'Alexa Records You More Often Than You Think'. [online] Vox, 2020. Available at: [www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording](http://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording).

52 S. Kojouharov, 'Chatbots, AI & the Future of Privacy' [online] Medium, 2018. Available at: <https://chatbotslife.com/chatbots-ai-the-future-of-privacy-174edfc2eb98>.

‘wake up’ word. Moreover, it has been argued that Google suggests a search term or an advertisement on the basis of a conversation they had with another person.<sup>53</sup>

The increase in the number of bots on chat platforms is rapid. What is missing is that as these interfaces are evolving, we have a shift in data control from users to Messenger or Facebook. It is not only companies that upload their bots on these platforms that store users’ data but also Facebook and Messenger that have the right to do that, according to their policy. Both of them have the potential to become strong data brokers. All conversations or transactions within these platforms are also stored and filtered on the basis of personal users’ IDs and can be sold to governments or other organizations.<sup>54</sup>

A great example is the Cambridge Analytica scandal, in which, in 2015, a political marketing company collected 50 million Facebook users’ data by using a personal quiz that was initially approved by Facebook. Because of this scandal, developers could not upload temporally new chatbots on Facebook’s platform.<sup>55</sup>

For this reason, Digital Liberties organizations have already expressed their concern about this trends, and several technical ways to solve the problems arising from it have been proposed. One such idea for Facebook could be to introduce private channels with a high level of encryption between the user and the chatbots so that Facebook would know the bots with which a user interacts but not their conversation.<sup>56</sup>

In the following paragraphs, a thorough investigation is attempted to view chatbots through the lens of law protecting users’ privacy, personal data and digital liberties.

## B Legal Framework

### *I Legal Regulation of Chatbots*

While the use of chatbots is constantly increasing, the regulation of their legal framework is not quite clear. As tools that process, collect and store personal data, they endanger our online privacy.

Among the most representative examples of the application of AI is the digital policy of the Union, around which our interest is centred, as it foregrounds the reasonable exploitation of AI. The point of reference and study is the adoption of the first legislative framework for AI by the Commission (Artificial Intelligence Act-section I). AI technology is part of an ongoing evolution and constantly poses

53 Choudhury, Kumar and Piyush, 2016, p. 323; Ischen, Araujo, Voorveld, van Noort, Smit, 2020, pp. 1, 3.

54 H. Harkous, ‘How Chatbots Will Redefine the Future of App Privacy’. [online] Medium, 2016. Available at: <https://chatbotsmagazine.com/how-chatbots-will-redefine-the-future-of-app-privacy-eb68a7b5a329>.

55 G. Skandali, ‘Cambridge Analytica: How Will It Play Out for Chatbots?’ [online] Medium, 2018. Available at: <https://medium.com/yellow-hammock/cambridge-analytica-how-will-it-play-out-for-chatbots-5c1d44f4fe29>.

56 Harkous, 2016.

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka

new challenges, which the laws and the rules of each country cannot timely regulate.<sup>57</sup>

Yet, as different functions of AI can affect the right to privacy in several ways, such as data collection without the knowledge and consent of subjects, locating people, extracting and generating sensitive information, producing automated decision-making, profiling, etc., finding an appropriate legal framework is crucial for the protection of personal autonomy and the exercise of other fundamental rights.<sup>58</sup> In addition, as privacy has a broad content, including the processing of personal data and while the use of chatbots includes similar procedures, the GDPR is applicable (section 2).

## II Regulatory Framework on Artificial Intelligence

On 21 April 2021, the European Commission ('Commission') adopted a proposal for a "Regulation laying down harmonized rules on Artificial Intelligence" ('AI Regulation'), which sets out how AI systems and their outputs can be introduced to and used in the European Union. The draft AI Regulation is accompanied by a proposal for a new Regulation on Machinery Products, which focuses on the safe integration of the AI system into machinery, as well as a new Coordinated Plan on AI outlining the necessary policy changes and investment at the member state level to strengthen the EU's leading position in trustworthy AI.<sup>59</sup>

AI receives a wide definition in the official European text. Following Article 3,

*'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I ('machine learning', 'logic- and knowledge-based' and 'statistical' approaches) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations or decisions influencing the environments they interact with;*

According to the official press release published by the European Commission regarding the new rules for AI,<sup>60</sup> risk categories are adopted on the basis of the intended purpose of the AI system, in line with the existing EU product safety legislation. The criteria for this classification include the extent of the use of the AI application and its intended purpose, the number of potentially affected persons, the dependency on the outcome and the irreversibility of harms, as well as the extent to which existing Union legislation provides for effective measures to prevent or substantially minimize those risks.

As explicitly predicted, the Commission proposes a risk-based approach, with four levels of risk:

57 J. Isaak & M.J. Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection', *Computer Magazine*, Vol. 51, 2018, pp. 56-59. Available at: [www.computer.org/csdl/magazine/co/2018/08/mco2018080056/13rRUxbCbmn](http://www.computer.org/csdl/magazine/co/2018/08/mco2018080056/13rRUxbCbmn).

58 K.M. Manheim & L. Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy", *Yale Journal of Law & Technology*, Vol. 21, 2019, p 106.

59 At the time being the draft AI Regulation is being processed by the European Parliament and Council.

60 The official press release is available at [https://ec.europa.eu/commission/presscorner/detail/en/QANDA\\_21\\_1683](https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683).

*Unacceptable Risk:* A very limited set of particularly harmful uses of AI that contravene EU values because they violate fundamental rights (e.g. social scoring by governments, exploitation of vulnerabilities of children, use of subliminal techniques and – subject to narrow exceptions – live remote biometric identification systems in publicly accessible spaces used for law enforcement purposes) will be banned.

*High-Risk:* A limited number of AI systems defined in the proposal, creating an adverse impact on people's safety or their fundamental rights (as protected by the EU Charter of Fundamental Rights) are considered to be high-risk. Annexed to the proposal is the list of high-risk AI systems, which can be reviewed to align with the evolution of AI use cases (future-proofing).

These also include safety components of products covered by sectorial Union legislation. They will always be high-risk when subject to third-party conformity assessment under that sectorial legislation.

In order to ensure trust and a consistent and high level of protection of safety and fundamental rights, mandatory requirements for all high-risk AI systems are proposed. Those requirements cover the quality of data sets used; technical documentation and record keeping; transparency and the provision of information to users; human oversight; and robustness, accuracy and cybersecurity. In case of a breach, the requirements will allow national authorities to have access to the information needed to investigate whether the use of the AI system complied with the law.

The proposed framework is consistent with the Charter of Fundamental Rights of the European Union and in line with the EU's international trade commitments.

*Limited Risk:* For certain AI systems specific transparency requirements are imposed, for example where there is a clear risk of manipulation (e.g. via the use of chatbots). Users should be aware that they are interacting with a machine.

*Minimal Risk:* All other AI systems can be developed and used subject to the existing legislation without additional legal obligations. The vast majority of AI systems currently used in the EU fall into this category. Voluntarily, providers of those systems may choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.

Regarding the use of chatbots, the draft AI Regulation reserves a relevant provision, namely, "*for some specific AI systems, only minimum transparency obligations are proposed, in particular when chatbots or 'deep fakes' are used*". The aforementioned transparency obligation is thoroughly exposed in Article 52 of the text, whose paragraphs 1 and 3 are quite relevant. In this vein, *providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use*. It is easily extracted that the nature of such 'information' corresponds directly to 'transparency', which can be described as the opposite of opaqueness and secretiveness. In this context,

according to Advocate General R.J. Colomer in the case C-110/03,<sup>61</sup> *transparency is concerned with the quality of being clear, obvious and understandable without doubt or ambiguity*. It should also be noticed that the provision of such quality constitutes the main responsibility of administrators of AI systems. More specifically, in order to achieve an adequate and sufficient level of information for users of AI systems, their administrators shall disclose to the user that “the content has been artificially generated or manipulated”.<sup>62</sup> It is of primary value that the subject recognizes, without any doubt, the existence of ‘bots’ during any process or type of communication. Widely approaching the issue, we could claim that not revealing to the person that ‘deep fake’ content could result in legal damages to the administrator of AI systems. In that context, transparency could be given a legal binding status appearing as a general principle of law.<sup>63</sup>

Furthermore, since chatbots are intensively used in e-commerce, it should be underlined that the transparency obligation is imposed by other European legal texts, such as the Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. The Regulation imposes new rules on parties operating online trading platforms and similar services and taking on the role of an intermediary. According to EU officers, as regards *transparency*, platforms are required to use *plain and intelligible* terms and conditions for the provision of their online intermediation services. They should provide a *statement of reasons* each time they decide to restrict, suspend or terminate the use of their services by a business user. Furthermore, platforms should publicly disclose the main parameters determining the *ranking of business users* in search results, as well as any *differentiated treatment* that they grant to goods and/or services offered directly by them or through any business falling within their remit. They should also disclose the description of the main economic, commercial or legal considerations for restricting the ability of business users to offer *different conditions to consumers outside the platform*.<sup>64</sup>

Additionally, there is also the Digital Services Act, which establishes certain transparency standards.

In general, EU digital strategy incorporates specific rules offering businesses a more transparent, fair and predictable online platform environment. Chatbots have a dominant role to play in the achievement of the EU digital strategy’s goals. The draft AI Regulation dedicates a specific provision to their legal use and can therefore be considered as the main legal source. Transparency is the key factor that penetrates the lawful use of chatbots. While it has been thoroughly analysed, it is equally worthy to mention GDPR relevant provisions that fulfil the regulatory framework.

61 C-110/03, Judgement of the Court (Third Chamber) of 14 April 2005, *Kingdom of Belgium v. Commission of the European Communities*.

62 See para. 3 of the Art. 52 of the draft AI regulation.

63 See T. Tridimas, *The General Principles of EU Law*, 2nd ed., Oxford, Oxford University Press, 2006, p. 242.

64 Information available at [www.consilium.europa.eu/en/press/press-releases/2019/02/20/increased-transparency-in-doing-business-through-online-platforms/](http://www.consilium.europa.eu/en/press/press-releases/2019/02/20/increased-transparency-in-doing-business-through-online-platforms/).



### III *The Contribution of the General Data Protection Regulation*

Since chatbots collect and process a considerable amount of personal information, it is easily conducted that the General Data Protection Regulation is applied. In fact, we should focus on certain general principles relating to the processing of personal data.

Firstly, Article 5 of GDPR is of primary value as it establishes the fundamental prerequisites for the lawful processing of data. So on, data must be

- 1 processed lawfully, fairly and in a transparent manner ('Lawfulness, Fairness and Transparency');
- 2 collected only for specified, explicit and legitimate purposes ('Purpose Limitation');
- 3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed ('Data Minimization');
- 4 accurate and where necessary kept up to date ('Accuracy');
- 5 not kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the data is processed ('Storage Limitation');
- 6 processed in a manner that ensures its security, using appropriate technical and organizational measures (6: 'Security, Integrity and Confidentiality').

There are two additional principles, which can be found at Articles 12 and 13 of the GDPR and which can also be added to this list. These set forth the requirement that personal data:

- shall not be transferred to another country without appropriate safeguards being in place ('Transfer Limitation'); and
- be made available to data subjects, for them to exercise certain rights in relation to their Personal Data ('Data Subject's Rights and Requests').

One of the most crucial issues that comes into consideration when using chatbots is cookies<sup>65</sup> as their administrators often choose to pair their conversational assistants with cookies, in order to ensure continuity of experience for the human on the receiving end of the conversation – even in cases where the user decides to refresh the web page or open a new tab, for instance.

The EU's legislation offers a solid basis for the lawful processing of cookies.<sup>66</sup> Firstly, the GDPR predicts in recital 30 that natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

65 For further details about the different types of cookies and their management from users, see the official page of European Union [https://europa.eu/european-union/abouteuropa/cookies\\_en](https://europa.eu/european-union/abouteuropa/cookies_en).

66 See a brief analysis of the European regulatory framework regarding cookies at <https://gdpr.eu/cookies/>.

In this vein, cookies – as well as chatbots as an inherent part of their function – are, in principle, legitimate. Moreover, companies do have a right to process their users' data as long as they receive consent or if they have a legitimate interest, which can be interpreted according to the specific provisions of Article 6 of GDPR.<sup>67</sup>

Apart from GDPR, the main regulatory binding text for cookies is the e-Privacy Directive,<sup>68</sup> widely known as the 'cookie law'. The most important amendment to the prior Directive of 2002 is included in Article 5§3 of the text. Instead of allowing users to opt out of cookie storage, the revised Directive requires consent to be obtained for cookie storage.<sup>69</sup> The aforementioned requirement means that any time that one device contains chatbots its administrator (who is the processor of personal data) has to receive users' content, which must be unconditioned, clear and explicit as well as subject to potential withdrawal from the data subject.<sup>70</sup>

At this point, we should underline the recent guidelines published by the French Data Protection Agency (CNIL – Commission Nationale Informatique & Libertés) as well as the Italian Data Protection Authority (Garante), which illustrate the principles provided for the lawful use of cookies.<sup>71</sup> In particular, both the guidelines mandate that consent must be requested through a clearly distinguishable banner, through which users must also be offered the possibility to continue browsing without being tracked in any way. Furthermore, the guidelines clarify that simply scrolling down the web page does not constitute consent and that, in any case, the user should have the right to withdraw consent at any time. Moreover, the guidelines further specify that information provided to users must also indicate any other recipients of personal data and the period for which their data will be retained. In addition, the guidelines confirm that such information can be provided in different formats, such as through videos or pop-ups. The European Court of Justice has reaffirmed those principles through significant decisions in case law,

67 For example, a legitimate interest can be declared when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (case (c) of Art. 6 of GDPR).

68 In 2002, the European Union launched the Directive on Privacy and Electronic Communications (e-Privacy Directive), a policy requiring end users' consent for the placement of cookies, and similar technologies for storing and accessing information on users' equipment. In 2009, the law was amended by Directive 2009/136/EC, which will be eventually replaced by the ePrivacy Regulation.

69 As it is explicitly predicted, "*Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*"

70 See Art. 7 of GDPR regarding the conditions for consent.

71 CNIL published its guidelines on 1 October 2020 and Garante on 10 July 2021. A thorough analysis of those guidelines is provided at [www.cookie-law-info.com/new-cn-il-cookie-guidelines/](http://www.cookie-law-info.com/new-cn-il-cookie-guidelines/) and [www.dataguidance.com/news/italy-garante-releases-new-guidelines-cookies-six-month](http://www.dataguidance.com/news/italy-garante-releases-new-guidelines-cookies-six-month), respectively.

such as at the case C-673/17<sup>72</sup> and case C-210/16, where the Court decided that the consent referred to in the provisions of E-Privacy Directive and GDPR is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox that the user must deselect to refuse consent. Therefore, we can conclude that since administrators of chatbots incorporate cookies their use should obey, with all urgency, the principle of prior clear, distinguishable and unconditioned consent from the data subject.

Another crucial issue at stake when using chatbots is the profiling of the data subject. The GDPR provides sufficient answers to the problem. More specifically, Article 22 of the European regulation prohibits automated individual decision-making, including profiling, unless some specific exceptions occur, such as the need for entering into a contract between the data subject and the data controller.<sup>73</sup> It should also be noticed that, according to the last paragraph of the article, automated decision-making that involves special categories of personal data is allowed only under the following cumulative conditions (Art. 22(4)): there is an applicable Article 22(2) exemption; and point (a) or (g) of Article 9(2) applies.<sup>74</sup> In both these cases, the controller must put in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

Therefore, we could allege that chatbots should never constitute the legal basis for producing a binding agreement between the contracting parties. However, since chatbots are widely used in e-commerce we could accept the exception of Article 22 of GDPR owing to their necessity for pre-contractual processing and, consequently, an automated decision-making falling within that scope. The example provided by Article 29 Data Protection Working Party through the guidelines published on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679<sup>75</sup> is strictly relevant to our previous allegation:

A business advertises an open position. As working for the business in question is popular, the business receives tens of thousands of applications. Due to the exceptionally high volume of applications, the business may find that it is not practically possible to identify fitting candidates without first using fully automated means to sift out irrelevant applications. In this case, automated decision-making may be necessary in order to make a short list of possible candidates, with the intention of entering into a contract with a data subject.

72 Case C-673/17, Judgment of the Court (Grand Chamber) of 1 October 2019 (request for a preliminary ruling from the Bundesgerichtshof – Germany) – Bundesverband der Verbraucherzentralen und Verbraucherverbände – *Verbraucherzentrale Bundesverband eV v. Planet49 GmbH and case C-210/16*, Judgement of the Court (Grand Chamber), *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*.

73 See paras. 1 and 2 of Art. 22 of GDPR.

74 9(2) (a) - the explicit consent of the data subject; or 9(2) (g) - processing necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

75 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017, as last revised and adopted on 6 February 2018.

Konstantinos Kouroupis, Dimitrios Vagianos & Aikaterini Totka

The ideal tool for producing that goal (meaning the short list of possible candidates) would be the chatbots.

## C Conclusion

The thorough foregoing analysis demonstrated the dynamic presence of chatbots in the European digital strategy. Being a typical example of AI, they are strictly connected with high goals such as promoting digital economy and technology and empowering business and infrastructure in a secure and sustainable digital environment. Certainly, since the processing of data is inevitable, serious social, ethical and legal concerns arise. Human privacy is at risk and must be protected. The existing European regulatory framework, mainly the General Data Protection Regulation and E-Privacy Directive, offers safe guarantees and may be considered as the 'traditional' legal background for the protection of our privacy. But it is the draft AI Regulation, the main legal text, that could lead (after being adopted) to binding effects and harmoniously regulate all the controversial issues being raised in the new digital era. The provision of all necessary information from the administrators and the respect of prior consent from the data subject, as have been thoroughly described by the provisions of the foregoing legal texts, represent the key principles of the lawful use of chatbots. Transparency reflects all the demanded requirements and seems to be of primary value. It is consequently urgent that any business that uses chatbots must form a concrete privacy policy, easily accessible and with respect to all rights of the data subject. Under those circumstances we could strike a successful balance between the empowerment of digital economy, productivity and economy and the safeguarding of online privacy.