

Katarzyna Chałubińska-Jentkiewicz\*

# Marketing techniques as a threat to cybersecurity

## Summary

The Internet is a suitable place to display a product or service, however, the ways in which an advertising message exerts influence on its audience differ from the ones the advertisers relied on in traditional media. The speed of communication, the availability of information sources and e-administration are significant social benefits that come with the growth of technology. However, there are justified concerns about the consequences of the operation of the Internet. Today, the Internet is not a new phenomenon, but the use of it leads to a growing number of new consequences. The continuous development of the medium has resulted in the significant commercialisation of the web. The active expansion of mass media, visible especially in continually expanding advertising and marketing offers, including mobile devices, requires a fresh look at regulations in the area of advertising.

**Key words:** online marketing, online advertising, cybersecurity, act of unfair competition

\* Katarzyna Chałubińska-Jentkiewicz, Associate Professor at the War Studies University in Warsaw, Head of the Academic Centre for Cybersecurity Policy, e-mail: [kasiachalubinska@gmail.com](mailto:kasiachalubinska@gmail.com).

## Introduction

The Internet can accommodate, to a large extent, newer and newer kinds of communication. Internet radio stations and TV services have become popular. The medium has also influenced the development of telecommunications, opening up new possibilities of communication using video and audio means. Examples of online advertising include banner ads and so-called Internet sponsorship. Websites, blogs and social media sites are also forms of advertising that allow one to display a product or service. Other means of advertising online are advertisements placed on instant messaging apps (chats) and electronic mail (Internet marketing or an electronic newsletter). The ways of influencing the potential audience of advertising today are subject to redefinition. It should be stressed that the issues of online marketing activities should be looked into in the context of Art. 76 of the Constitution of the Republic of Poland, in which the legislators guaranteed that public authorities are obligated to protect consumers from threats to their security, privacy and health as well as unfair market practices.

The rapid development of new technologies and the digitisation and growth of innovation in this field continuously exert influence on the form and impact of present-day online advertising. Advertising plays a significant role in consumer choices as it has an influence on consumers' opinions, choices and behaviour. It also has a considerable impact on the social functioning, political, and economic situations. The primary sphere in which advertising influences consumers the most are the mass media, especially the so-called new media. However, the Internet cannot remain a sphere that is free of regulation and in which every activity, including the one that serves to evade legal bans<sup>1</sup>, constitutes an expression of market freedom. The issue is addressed by Jacek Sobczak, according to whom „since it is unacceptable to place advertisements in the printed press as well as on the radio and television, one must not publish and distribute them via the Internet as well”. The subject of this article is not, however, the regulations of the advertising market in the sphere of the Internet. The existing bans on advertising certain products and professions resulting from EU law and regulations on unfair competition also apply to the transmission of banned, illegal advertising content on the Internet. In addition,

1 Cf. R. Stefanicki, *Prawo reklamy w świetle przepisów ustawy o zwalczaniu nieuczciwej konkurencji na tle prawnoporównawczym*, Poznań 2003, p. 81–214; E. Nowińska, *Zwalczanie nieuczciwej reklamy. Zagadnienia cywilnoprawne*, Kraków 2002, p. 44–155.

the Internet is a place where one can observe new kinds of threats that require analysis and definition of the objectives of public interest and appropriate regulations.

The law, judicial decisions and literature that deals with the analysis of activities connected with advertising in new technologies allow one to state that the norms of protection against unfair activities are still not sufficiently flexible in relation to an ever-changing reality, despite the fact that the purposes and functions of advertising are the same and do not differ from traditional forms. The regulatory policy that refers to advertising activities finds special threats in the sphere of the right to privacy.

Advertising in new technologies allows one to use methods that were not known before. The Internet has contributed to the rise of spamming, viral marketing and search engine optimisation, which, especially in the case of the latter two, is a novelty and touches upon very difficult issues connected with profiling, automatic data processing, target advertising and data monetisation. New technologies engage the consumer to take an active part in the process by, for example, sending data which are later used for marketing purposes. However, the process takes place without the user's conscious participation since eavesdropping and the analysis of consumer behaviour are today standard practices in internet marketing.

The emphasis on respecting the provisions concerning the protection of personal interests and counteracting unfair competition in marketing activities takes on a new meaning in the context of cyber advertising. Advertising instruments enter private space like never before. And although ads should attract a potential customer's attention, as that is their purpose, they also often infringe on the sphere of privacy. Present-day advertising activities are strictly connected with the right to privacy, which is guaranteed by the Constitution, for example, through the protection of the private sphere, the safety of correspondence and personal data. The character of both private and public monitoring systems, the influence of which is hard to identify, makes them present in all varieties offered by the development of new technologies and contribute, in a similar way, to the incidence of certain threats.

The problem of new types of internet marketing is primarily the fact that they have no territorial or time limits, so far used as indicators of the scope of impact of an advertising message. Depending on the type of media, as well as the position and status of the content provider, different rigors of the law concerning responsibility for the advertising content will apply. Such

a situation refers to almost every sphere of human activity, more and more often dependent on the processes taking place in virtual reality.

An advertising message in the days of technological progress differs significantly from a traditional advertising message created on the basis of socio-demographic factors such as gender, age, education or place of living. In addition, it is difficult to establish common rules for very different advertising techniques. Yet Directive 2010/13/EU<sup>2</sup> replaces the rule of separation with the rule of distinction and admits distinction by optical, acoustic or spatial means, without prejudice to the use of new advertising techniques. In the amended Broadcasting Act, Art. 16 (2) was adapted to Art. 19 (1) of Directive 2010/13/UE and it provides that: „Television advertising and telesales shall be kept distinct from the editorial content. Television advertising and telesales shall be kept distinct from other parts of the programme by optical, acoustic and/or spatial means”; however, that rule will not apply to all marketing activities.

Internet marketing puts pressure on advertising agencies to broaden audience classification criteria by individualising the advertising messages targeted at a specific person. Today, marketing agencies cooperate closely with database brokers in order to achieve the maximum personalisation of their advertising messages. Thus, online advertising has become strictly connected with political marketing. Today, the market of online advertising is the most rapidly growing segment of the advertising industry in the world and has a significant influence on the economy of both European and non-European states. The private sector of the economy, inseparably connected with the development of new technologies, in which decisions are made by individuals and private entities, has a direct impact on the functioning of European states.

European politics is focused on fundamental issues. However, the European forum is also a place for discussion about the right relations: an individual and their right to privacy vs. new technologies. From there questions arise about the character of advertising activities and the purpose of collecting data on the Internet. How far does our „right to anonymity” extend? What does anonymity on the Internet mean? So far, there is no doubt that we are also dealing with the question of systemic nature, namely, to what extent are the respective rights balanced with the justified interests of information? A significant part

2 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance) OJ 2010, L 95, p. 1–24.

of the population seems to be aware of the existence of regulations in the sphere of the Internet. There are, however, still groups of people whose skills of using mass media and whose awareness of the existence of regulations are clearly lower. Competence connected with advertising helps people recognise the products or services that are offered, but the identification of more subtle techniques is complex and essentially out of reach. There is clear tension between freedom of expression, freedom of information, and now also freedom of the Internet, as well as the protection of privacy. The issues concerning personal data protection addressed here initially referred only to the problem of using search engines for looking for people. Today that interference is much more advanced.

## **Profiling and targeting**

In their joint efforts to create the most effective advertisements on the Internet, advertisers employ, among others, the so-called technique of profiling. To put it simply, it means an automated process which leads to identifying certain features in an individual. Profiling is a process of automated data processing which consists in using data to assess certain factors that are characteristic of a given user, especially to analyse and predict their interests and behaviour, including credibility on the Internet, location, movement, outlook and consumer or professional preferences. In a broader context, it means the precise adaptation of advertising content to consumers' interests based on their browsing history. It would seem that the use of this technique will allow the advertisers to reach the consumer directly and thus deliver the highest level of service. The term is accompanied by the issue of the so-called targeting, which is a process consisting in the selection of a target group that is the most interested in given editorial and advertising material.

The advertisements and editorial material shown to the user are targeted and personalised using such information as activity in services, Internet websites and applications. This also applies to the use of editorial materials; activity and interaction with advertising content; location, the size of the locality which the user comes from; information stored in end devices, especially information on the type of end device, type of browser, the user's operating system and the language set in the user's operating system.

The information collected through profiling can be used to personalise advertising and content in services, websites and applications as well as other

locations on the Internet, which are not the services, websites or applications a user uses or visits. That refers in particular to advertising networks which gather and provide agency services in selling advertisements. Advertising networks collect data about the users of all websites cooperating with them and then use the data to display advertisements which are best suited to the users' interests.

## Present-day acts of dishonest advertising

Nowadays, it can be observed that an alarmingly large number of activities in cyberspace, of non-criminal character, bring a lot of threats to society. One such activity is the use of dishonest techniques in internet advertising. They infringe, directly, upon an individual's right to privacy. The active expansion of transmission techniques, especially visible in the continually expanding marketing offers with mobile devices and instant messaging apps, where information is shared in private, requires a fresh look at advertising regulations. The methods of influencing the potential audience of an advertisement rely more and more often on the instruments of monitoring and surveillance. It should be stressed that the issues should be considered in the context of Art. 76 of the Constitution of the Republic of Poland, in which the legislators guaranteed that public authorities are obligated to protect consumers from threats to their safety, privacy and health, but also from unfair market practices. Such advertising is characterised by a number of unfair practices adopted by advertisers and related entities including: burdensome touting (overlying ads), sending unordered commercial messages (spam) and overusing technical media (information noise, internet of things). In that respect, other practices employed by advertisers that are hard to accept are: misleading, hidden advertising, including surreptitious advertising, and search engine optimisation based on untrue data.

The new techniques of influencing consumer behaviour, the phenomenon of the so-called viral marketing, which consists in the intensive popularisation of information that may be untrue, requires one to identify the dangers that are brought by it<sup>3</sup>. Viral marketing is based on the informal communication

3 P. Michalak, D. Daszkiewicz, A. Musz, *Marketing wirusowy w Internecie*, Warszawa 2012, p. 37.

between Internet users. The use of it by the producer results in its further popularisation among users. The customer takes over the task of disseminating information about a product or company. Viral marketing involves „targeting” a message, which means sending tailored information to individual users who are directly interested in such specific information. Activities of this kind involve some risk. It is both easy to lose control over the message and difficult to assess the effects of using the message as there are more and more anti-spam settings in e-mail boxes that protect users from such advertising activities. Viral marketing often relies on e-mail addresses, which constitute collections of legally protected databases. Customers often pay greater attention to the opinions of other buyers instead of the assertions and persuasion of the advertiser. This can also be an advertising method (the so-called buzz marketing). The law has developed certain restrictions connected with advertising as an act of unfair competition. Such activities are of various character and their consequences may influence public opinion.

The very process of search engine optimisation is based on the optimisation of the code, the aim of which is to create a website that complies with the standards used on the Internet. This can be achieved through content optimisation, which means creating a website that is easy to use and understand for an Internet user. In order to enhance the effectiveness of such activities, one needs to include certain keywords. Yet, search engine optimisation can also take on the form of an act of unfair competition. Such activities include: 1) black hat SEO, which is a set of banned practices that are used to increase a website's rank in search engines – keyword cloaking e.g. by using the same colour for background and text; as a result of such practices a website may be banned from search engines; 2) Google bowling, which is a strategy of pointing a lot of links to a website<sup>4</sup>; 3) tattling, which consists in constant monitoring and reporting on any irregularities to the administrators of a search engine; 4) denial of service – an attack on a server on which a website is hosted. It often consists in sending a lot of messages with a Trojan horse, the aim of which is to overload servers. This method was used for blocking government websites in Poland in 2012, in connection with the attacks by Anonymous (the protest against ACTA); 5) copying the content of websites or reporting on the appropriation of content in the case of the competition's websites. The grounds

4 T. Karwatka, D. Sadulski, *E-commerce: proste odpowiedzi na trudne pytania*, Warszawa 2011, p. 134.

for blocking content may be premises stemming from the Act on Copyright and Related Rights and the provisions of the Unfair Competition and the Personal Data Protection Acts; 6) click fraud – the attack hits a competitor who uses pay-per-click online advertising. If an attack hits a competitor who displays advertisements of search engines within advertising networks, a website is banned; 7) Google insulation – searching for so-called keywords, which results in showing a given trademark in a bad light<sup>5</sup>.

It needs to be stressed that the said activities are observed both in the realms of commerce and politics, leading to violations of safety, which should be viewed as a threat to the security of a state. Both in the classical dimension (political and military) based on international, state, internal and local affairs, and in the individual dimension that pertains to the safety of an individual (the so-called human security), based on consumer relations and the protection of human dignity, which the right to privacy stems from. There is no doubt that the specificity of new technologies and their role in the state and society requires an assessment from the perspective of a superior good, which is in the public interest especially in the period of transformation connected with the digital revolution. At the same time, the national and European attitudes towards the protection of public interest may differ due to the character of the subject matter. The changes connected with the development of new technologies are accompanied by certain social processes on both a global and local scale. The development of new technologies as a technical process not only has an influence on the changes in attitude towards online media, but also plays a significant role in the spheres connected with culture and national identity. Since this revolution sneaks in the domain of an individual, their sense of national belonging undergoes re-evaluation.

## **Marketing instruments and safety**

Having one's own controlled information space, large-scale socio-technical instrumentation and specialist or journalist potential are the foundations in the area of national security. An individual's safety and privacy in cyberspace are horizontal issues and they pertain to all areas of using new media. Financial security, the secrecy of correspondence and medical confidentiality depend on

5 Ibidem.

that competence and skill. That is why it is important that Internet users can take care of their own safety and privacy on the Internet in a conscious way and know the laws that apply in that area. However, providing comfort to the users of new technologies, who make use of technological progress in many spheres of their lives, is not the ultimate objective for advertising agencies.

What is more, the technique of profiling makes it easier for them to segment data within a given target group and send other more customised messages. Advertising agencies solicit consumer data – data about Internet users – who, by installing applications on their smartphones, unconsciously agree that their data can be accessed and processed. A single move of the mouse pointer, a click or logging into a website can be followed without a user's knowledge or consent. Profiling the potential audience of an advertising message also applies to the voice, sound and location data of the users of mobile devices. One should remember that profiling, in many cases, requires the user's consent to the processing of their private information in that manner. Especially in situations when the process involves special categories of personal data (e.g., medical information) or when, as a result of the process, the problems of an individual that have been discovered are taken advantage of (e.g., showing ads of payday loans to people who are in debt). Users of new technologies most often do not have any influence on the profiling criteria or the content they finally see on the screens of their devices. In addition, they do not have any actual influence on the scope of data that are collected or generated in relation to them. It is worth mentioning the fact that the controlled activity of the users of new technologies comes down to trapping them in a so-called information bubble. It is a seemingly safe sphere of media reality from which it is difficult to resign and thus be able to have a good grasp on the actual state of affairs without exposing oneself to misinformation.

Now we need to refer to Art. 47 of the Constitution of the Republic of Poland, which constitutes the normative basis for distinguishing personal good defined as „privacy”. Under this provision, „everyone has the right to legal protection of their private and family lives, dignity and good name and to decide on their personal lives”. Therefore, the legislators forbid unjustified interference in the private sphere. In addition, the right to privacy, laid down in Art. 47 of the Constitution of the Republic of Poland, is guaranteed, e.g., through the protection of the secrecy of communication (Art. 49 of the Constitution of the Republic of Poland) and the protection of private life (Art. 51 of the Constitution of the Republic of Poland). Therefore, it should be noted that the protection of private life provided for in Art. 47 of the

Constitution of the Republic of Poland includes information autonomy, which is the right to decide on one's own about sharing information about oneself to other people as well as the right to control that information if it is in the possession of other entities.

The right to privacy is applicable in a great many spheres of human activity, extending its protection over a multi-level network of personal goods, thereby remaining in direct relation to the detailed regulation included in Art. 30, Art. 48–51, Art. 53 (1) and (7), and Art. 76 of the Constitution of the Republic of Poland. At the same time, Art. 51 of the Constitution of the Republic of Poland introduces the principle of personal autonomy, which means that no one can be obligated, unless under a statute, to disclose information that pertains to them. The right to privacy has its roots in the right to dignity and provides that „dignity is the ultimate value, which other values protected under law stem from, such as the protection of personal goods”. According to a lot of experts, dignity should be treated as the source of all human rights guaranteed in the Constitution (which includes the constitutional right to the protection of privacy). It is significant to point out the meaning of dignity in all those cases where the respective defined rights do not provide enough protection. That applies especially to situations caused by the rapid development of technology. Then, it is dignity in the normative sense that will determine the limits of behaviour that will not be an interference in human dignity.

## **The future of regulations**

The e-commerce industry, in other words, electronic trade, is nowadays one of the most popular channels of distribution, called the foundation of modern economy. It is used by online stores, Internet auctions, group-buying platforms, partnership programmes etc. In addition, it is assumed that the 21<sup>st</sup> century is characterised by a very clear use of new technologies, instruments and innovative solutions not only in commerce, but also in politics (political marketing, political advertising), e.g., during political campaigns. Together with technological progress, the art of effective political communication and persuasion, and the skill of managing internal political structures have started moving, in a natural way, to the Internet. As a result, political marketing has started to bring to politics some Internet tools thanks to which political communication has become gradually easier and the effectiveness of activities aimed at gaining voter support has increased.

Similarly to e-commerce, the techniques of profiling and the phenomenon of the information bubble discussed above can be found in political marketing, where they function on the same rules. Therefore, one should pay attention to the existing correlation between political marketing and the e-commerce industry and thus the multi-dimensionality of the phenomena brought about by the development of new technologies connected with the advertising market. Hence the use of unfair practices in advertising in information warfare is such an important issue. Let us take the example of the phenomenon of fake news (deliberate and aggressively distributed misinformation), considered one of the main instruments of this type of warfare. State actors taking part in this type of war strive to achieve their aims in the following spheres: military, political, social, religious, economic, etc. An unprecedented example is the intervention of other states in electoral campaigns, e.g., through dishonest advertising messages distributed on social media such as the promotion of content that divides public opinion, which took place during presidential elections in France and the United States.

In consideration of the above, in order to protect state interests and thereby ensure that a state maintains a stable position on the international arena, a series of legislative activities in the sphere of information security are undertaken. One can observe very clearly the activeness of European states, including Poland, in implementing and updating legal regulations such as the strategy of information security and the doctrines and concepts concerning cybersecurity, the so-called cyber strategies. The main document that programmes the EU policy in the area of the development of new technologies is the Digital Single Market Strategy. In addition, in order to increase the protection of privacy in view of the mass processing of metadata and mass monitoring, the EU introduces new regulations, namely, e-Privacy, which is a legal act much more detailed than the current personal data protection regime (GDPR). The world of digital services will be, in turn, regulated by the Digital Services Act (DSA)<sup>6</sup> and the Digital Market Act.

In the DSA, in recital No. 63, the EU legislators stressed that „advertising systems used by very large Internet platforms create a special risk and require further public and regulatory supervision in the light of their scale and the capacity to target services towards an audience and to reach that audience

6 Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM(2020).

based on their behaviour on the platforms' interfaces and outside of them. Very large Internet platforms should ensure public access to repositories of advertisements shown in their Internet interfaces in order to facilitate supervision and research on the dangers resulting from advertising on the Internet, for example, with reference to illegal advertisements or manipulative techniques and misinformation which, in a real and predictable way, negatively affects public health, security, citizen discourse, participation in political life and equality. The repositories should contain the content of advertisements and related data concerning the advertiser and the distribution of advertisements, especially in the case of targeted advertising". At the same time, in accordance with the definition adopted therein, an „advertisement” means information intended for propagating a legal or natural person's message, no matter if for commercial or non-commercial purposes, shown by an Internet platform in its interface for remuneration for propagating that information, which means that the way of thinking about marketing techniques in the Internet is changing and that there is a need for regulating the sphere in view of threats to individuals. As proposed, Art. 30 of the DSA introduces the obligation to create data repositories containing: a) the content of an advertisement, b) an indication of the natural or legal person in the name of which an advertisement is shown; c) the period in which an advertisement is shown; d) information concerning the intention to show an advertisement to at least one target group and, in the case of such intention, the main parameters applied for this purpose; e) the total number of service recipients to whom an advertisement was shown and, if applicable, the aggregate number in the case of a group or groups of recipients at whom the advertisement was targeted. The obligation applies to very large Internet platforms which show advertisements on their interfaces, create and share, by means of the interfaces of application programmes, a repository containing information, for the period of one year following the last presentation of an advertisement on their Internet interfaces. The platforms see to it that the repositories do not contain any personal data of service recipients to whom advertisements were or could have been shown.

The said information obligations are aimed at introducing regulations the purpose of which are to establish responsibility for the activities on the Internet that are connected with marketing techniques. As stressed by the drafters, „the measures concerning advertisements placed on internet platforms are a supplement, not altering the applicable provisions of laws concerning the consent for personal data processing and the right to object to personal data processing. By means of such measures, one imposes obligations

in respect of transparency towards the users of internet platforms who, having obtained such information, will be able to exercise the rights vested in them as individuals to whom the data pertains. What is more, such measures make it possible for authorities and verified researchers to supervise the ways of showing and targeting advertisements”.

## Conclusion

In the days of psychological and information operations used in warfare (vide RF –Ukraine), the main actors base their activities mainly on the psychological character of the information sphere. The attitudes of Russians<sup>7</sup> seem to stand in opposition to the position of European states which, similarly to the United States, rely mainly on the „technicist” vision of cyberspace. While the dissimilarity of the Russian model of impingement in the infosphere and the significance of that impingement in military culture are today the main focus of analysis in science, social studies and political science as a novum in relation to the rules obeyed in Europe. It should be stressed, however, that these techniques are nothing new in the conditions of the functioning of digital market rules. That is why the aspect of using and regulating the use of new marketing technologies known in the commercial and political planes by a state actor in their operations should not be overlooked as far as cybersecurity issues are concerned. Since never before has it been so clearly visible that, on the one hand, technological progress brings convenience and offers a lot of opportunities both for the e-commerce industry and political marketing, whilst on the other hand, this phenomenon intensifies the occurrence of a great number of threats to an individual and a state. An example can be the unfair marketing practices mentioned at the beginning, which are used both on commercial and political levels. In both cases, the practices infringe on an individual’s right to privacy and in consequence, are a threat to state security.

<sup>7</sup> Here it should be added that the RF, for the first time, officially stressed the role of the influence of computerisation on state security and the defence potential in Военной доктрине Российской Федерации (The Military Doctrine of RF).

### Bibliography

- Karwatka T., Sadulski D., *E-commerce: proste odpowiedzi na trudne pytania*, Warszawa 2011.  
Michalak P., Daszkiewicz D., Musz A., *Marketing wirusowy w Internecie*, Warszawa 2012.  
Nowińska E., *Zwalczanie nieuczciwej reklamy. Zagadnienia cywilnoprawne*, Kraków 2002.  
Stefanicki R., *Prawo reklamy w świetle przepisów ustawy o zwalczaniu nieuczciwej konkurencji na tle prawnoporównawczym*, Poznań 2003.

## Techniki marketingowe jako zagrożenie dla cyberbezpieczeństwa

### Streszczenie

Internet jest odpowiednim miejscem na wyeksponowanie produktu czy usługi, ale sposoby oddziaływania przekazu reklamowego na jego odbiorców różnią się od tych, które stosował reklamodawca w tradycyjnych mediach. Szybkość komunikacji, dostępność źródeł informacji czy e-administracja stanowią istotną korzyść społeczną rozwoju technologii. Pojawiają się jednak uzasadnione obawy o skutkami funkcjonowania sieci. Obecnie internet nie stanowi już zjawiska nowego, wciąż jednak pojawiają się nowe konsekwencje działania w sieci. Ciągły rozwój tego medium doprowadził do znaczącej komercjalizacji sieci. Aktywna ekspansja technik przekazu, widoczna zwłaszcza w powiększającej się ofercie reklamowej i marketingowej, także w ramach urządzeń mobilnych, wymaga nowego spojrzenia na regulacje związane z reklamą.

**Słowa kluczowe:** marketing internetowy, reklama online, cyberbezpieczeństwo, czyn nieuczciwej konkurencji