

CYBERLAW

by CIJIC

Cyberlaw by CIJIC, *Direito: a pensar tecnologicamente.*

CYBERLAW

by **CIJIC**

EDIÇÃO N.º X – SETEMBRO DE 2020

**REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE
INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA
FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA**

CYBERLAW
by **CIJIC**

CYBERLAW

by CIJIC

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

COMISSÃO CIENTÍFICA:

- ALFONSO GALAN MUÑOZ
- ANGELO VIGLIANISI FERRARO
- ANTÓNIO R. MOREIRA
- DANIEL FREIRE E ALMEIDA
- ELLEN WESSELINGH
- FRANCISCO MUÑOZ CONDE
- MANUEL DAVID MASSENO
- MARCO ANTÓNIO MARQUES DA SILVA
- MARCOS WACHOWICZ
- ÓSCAR R. PUCCINELLI
- RAQUEL A. BRÍZIDA CASTRO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW

by CIJIC

NOTAS DO EDITOR:

Os últimos tempos, assim e porque não os vindouros, sobressaltam-nos com três complexidades *esdrúxulas*: acesso universal e aberto à Rede e democratização desta; capacitação humana numa era de dilúvio informacional; a relação da tecnologia, do digital, ao serviço das organizações e/ou Estado com a pessoa humana.

É inegável que o acesso à Rede é um direito fundamental da pessoa humana. Da mesma forma que a liberdade, a inclusão e democratização do espaço físico possibilitou uma dinamização de valor acrescentado ao elevador social, é já hoje mais do que óbvio, que a inclusão digital trará idênticos efeitos. Quantas mais pessoas acederem à Rede, melhor. E tudo gira em torno de uma característica universal da pessoa humana: o ser social que somos. É, pois, essencial determinarmos, enquanto ente coletivo, a necessidade da prossecução, por via da pólis, de um acesso universal e aberto à Rede. É tema de agenda política.

Preocupam-nos, com efeito, as questões supranacionais que envolvem, desde logo o 5G. O tabuleiro político mundial, neste momento, está partido ao meio. E tal como Harari referiu – ainda que a propósito do combate à pandemia -, é imperioso que saibamos “*criar princípios éticos globais e restaurar a cooperação internacional (...)*”. Obviamente, tudo se resume às escolhas que fizermos, *Ie*, “*(...) Depende das escolhas que fazemos no presente. Os países podem optar por competir por recursos escassos e prosseguir uma política egoísta e*

isolacionista, ou podem escolher ajudarem-se mutuamente através de um espírito de solidariedade global."¹.

Assim, nem a *great firewall* chinesa, uma agenda económica protecionista e isolacionista, ou a pressão e separatismo estaduais servem a humanidade. Não será sobre esta toada *belicista* que a humanidade produzirá ganhos conjuntos. Se é que os almeja produzir. O espírito de solidariedade internacional tem-se perdido na espuma dos dias.

Curiosamente, na era de dilúvio informacional, parece-nos comprometida a capacitação humana. Severa, a incompreensão de que a pessoa humana não pode ser um objeto. Sendo-o, emerge do *trade-off* entre o acesso a um serviço “*free*” e a quantidade de dados pessoais que liberta, não só para lhe aceder como depois no usufruir desse serviço.

Zuboff² alerta-nos para o *direct and personal targeting*, um assombro de *direct emotional manipulation*, em que sobressai o modelo de negócio das *big tech trendy* de sempre: o parcelamento informacional da pessoa, vendido a outras corporações como ponto de dados; métricas, perfis, com o intuito de retornar (ao titular dos dados) sob a forma de bem ou comodidade (que julga querer adquirir). Qual rato de laboratório. Uma pirâmide financeira suportada à conta da pessoa titular dos dados pessoais, por esta e para esta.

O resultado concreto, analítico, sob a forma de capitalização bolsista, demonstra-nos que a era da informação, na verdade, não está a funcionar para as massas. Pelo contrário. Erige-se num paradoxo: empobrece as suas (nossas) vidas, quer pelos dados pessoais que *capta* quer pelos bens/comodidades que impinge, e enriquece o pecúlio dos (*famosos*) 1%. A robustez financeira acumulada por tais 1%, por sua vez, demonstra uma capacidade, por si só, de manipulação de pilares fundamentais dos estados de direito democrático: a capacidade para atingir diretamente o núcleo legislativo internacional. Com acesso a leis-fato (à medida), só o Direito poderá colocar travão a esta distopia.

Infelizmente, a erosão, de direitos fundamentais humanos, não fica sustida apenas no aspeto mercantil em que opera a redução da pessoa humana a uma objetificação pronunciada. Intrometida e diligentemente, o próprio Estado passou a focar a pessoa como um “*asset*”, como um meio, rasgando os pilares fundacionais de toda a doutrina kantiana.

1 Harari @ <https://en.unesco.org/courier/2020-3/yuval-noah-harari-every-crisis-also-opportunity> (ultimo acesso setembro 2020).

2 *The age of surveillance capitalism: the fight for a human future at the new Frontier of power.*

A observação da realidade presente, ainda comprometida pela atualidade da pandemia, não olvida que, à semelhança do *surveillance capitalism*, aqui converge a dualidade relacional humano/tecnologia (digital). Se o Estado se comporta como um ente egoísta, usando as pessoas como mero valor, ponto de dados, métrica ou perfil, miríade informacional para prosseguir determinadas agendas (quais?), o que o distinguirá das organizações privadas que procuram o lucro por todos e quaisquer meios?

Note-se, por exemplo, no caso de Portugal – sendo que é uma prática participada por uma maioria de países democráticos deveras preocupante –, o “estado de vigilância” começa, geralmente, como demonstrando ter um propósito justificado por um “*objetivo*” publicamente aceitável. Daqui deriva para uma moção rotineira, *ie*, uma vez implementado – mesmo que “*a título experimental*” –, passa a fazer parte da rotina diária de todos os cidadãos, planeado e executado de acordo com um cronograma racional, não aleatório, seguindo diretrizes perfeitamente concretas, focado em detalhes, como agregação e armazenamento de *dados*³.

A justificação, para esta aceitação passiva e obediente, por parte do cidadão, reduz-se a uma vacuidade: “*eu não tenho nada a esconder...*”. Contudo, o *estado de vigilância* (à semelhança do homónimo capitalismo) serve quem? O quê? Para quê?

Aquiesçamos, um *estado de vigilância* é um que contempla a vigilância como a solução para a esmagadora maioria das questões sociais complexas. Um *estado de vigilância* é respaldo da incompetência, manifestação de uma viciação por tecnologias (criadas por quem?) e dados (para quê? para quem?), com as limitações aí inerentes.

Tal como na problemática do *surveillance capitalism*, o *estado de vigilância* aparece-nos pressuposto no equilíbrio entre as suas necessidades (quais, porque não são coletivamente sufragadas) e desejos/ansias individuais egoístas. Neste jogo de soma zero para o cidadão - ainda que negociado como uma troca de soma não nula -, a propósito de segurança (ou saúde) prometidos pelo estado, este cede, no todo ou em partes, a sua individualidade. Uma vez tal cedência concretizada, a superioridade informacional granjeada, detida pelo *estado de vigilância*, tende a exaurir os mecanismos democráticos de supervisão do próprio estado, na

3 Podemos trazer à colação, para melhor percebermos, desde logo, os sistemas de videovigilância municipal já implementados. De igual forma, podemos pensar sobre a *vigilância*, embora míope quando o cidadão contribuinte tem uma riqueza pessoal assinalável – e tal miopia poderá explicar a constância de acesso de tais cidadãos a regime excecionais de regularização tributária - exercida pela Autoridade tributária. Recentemente, uma *novidade*, a *app* stayawaycovid.

Entre reconhecimento facial, pelas cameras de videovigilância; rastreamento através do cartão Mb – incentivado o seu uso massivo também a propósito da pandemia, sendo o *contactless* qual “sabão azul” nas medidas de mitigação da propagação da doença – não só através da localização como também do perfil de consumo, entre outros; à coleta de dados de saúde que a *app* permite, bem como o rastreio geolocalizado; de tudo temos experimentado. Os propósitos são “*claros*”: segurança, combate ao crime e saúde. Aliciantes...

medida em que o monopólio do conhecimento lhe permite controlar tudo o que pode ser divulgado. Bem coordenado com uma assinalável retórica de medo, tal *estado* passa a dispor da faculdade de usar os seus poderes para propósitos indiferentes à origem e finalidades registadas aos *baby-step* da sua implementação. Distopia? Sim. E já representada nas nossas vidas.

Urge, pois, contrariar as pulsões totalitaristas de *estados de vigilância*, promotores de exclusão e discriminação, sob pena de o nosso futuro, enquanto ente coletivo, ser irreparavelmente composto por cidadãos desprovidos da sua individualidade intrínseca.

Tal distopia estadual não serve à pessoa humana. A luta convoca-nos a todos.

O núcleo não pode, em momento algum, ser desfocado da sua essência: Estado ao serviço da pessoa. Tecnologia ao serviço da pessoa. É pela pessoa que o Estado se materializa. É para a pessoa que o Estado se organiza numa comunhão de direito democrático. É por um Estado que promove e prossegue o cardápio de direitos, liberdades e garantias fundamentais da pessoa que cumpre lutar. De igual forma, o recurso à ferramenta de auxílio – a tecnologia (digital) – pode e deve ser feito sempre que a finalidade seja construir um ente coletivo em que a pessoa é e sempre, também pela sua individualidade intrínseca, um fim em si mesmo. É por tal *futuro por design*, na disponibilidade da pessoa e pela pessoa humana que devemos concentrar o nosso esforço coletivo.

Nesta nova edição da Cyberlaw by CIJIC, perseguidos por tais inquietações, tivemos o ensejo de provocar os autores participantes à procura de juízos sobre a realidade desafiante que convoca a sociedade atual. E futura. Entre a inteligência artificial e a *algocracia* e os desafios que estas convocam ao Direito (e aos juristas); passando pelo crime de violência doméstica num contexto de abuso (mais uma forma de abuso) através das redes sociais e a proteção jurídico-penal que a vida privada exigem; à utilização de *benware* como meio de neutralização das técnicas e medidas antifoforeses que os criminosos usam; à engenharia do “direito penal sobre rodas” e ao agente inteligente automóvel num contexto de um certo desarranjo terminológico - todos escritos em língua portuguesa - e ante as responsabilidades – que já demos conta oportunamente – impondo-se-nos a difusão de conteúdo em inglês escrito, juntamos três temas desafiantes: *State surveillance; fake news & social networks; open banking*.

Como era expectável, *ab initio*, os temas são desafiantes. Para todos. São, como sempre, abertos a colaboração múltipla e, de preferência, participada. A prova foi, quer-nos parecer, superada com mestria.

Entretanto abre-se a janela da próxima edição, para Março de 2021. Não sem antes sublinhar que, nos próximos tempos, ante os critérios definidos pelo corpo diretivo e pelo editor, em parceria com a Associação académica da faculdade de direito de lisboa, passaremos a dispor de um número da revista, anualmente, em formato de papel.

Resta-me, por fim, agradecer a todos quantos contribuíram para mais esta nova edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um merecidíssimo: - Muito Obrigado.



Cyberlaw by CIJIC, *Direito: a pensar tecnologicamente.*

Boas leituras.

Lisboa, FDUL, 29 de Setembro de 2020

Nuno Teixeira Castro

CYBERLAW

by CIJIC

FAKE NEWS AND THE LIABILITY OF SOCIAL NETWORKS

DANIEL FREIRE E ALMEIDA *

* Postdoctoral researcher at Georgetown University (Washington-DC- USA) (2015-2017).
-Ph.D. in International Law, Faculty of Law, Coimbra University (Portugal- EU).
-Professor at Catholic University of Santos (Brazil) - Ph.D. and Master's Program.
-Professor and International Lawyer. -E-mails: lawyer@adv.oabsp.org.br, da616@georgetown.edu.

ABSTRACT

The main objective of this Article is to analyze the liability of digital social networks in relation to the contents known as fake news, when disseminated from their digital platforms. To this end, the Article is divided into two parts.

In the first session, it raises some of the main aspects of the digital environment, especially social networks. In the second session, on a purposeful basis, and in view of the challenges presented by fake news, address the responsibility of social networks on fake news.

Keywords: Fake News. Social Networks. Facebook. Twitter. Liability.

INTRODUCTION

The global configuration of social networks, which stand out on the Internet today, presents a digital environment that strongly represents the different segments of society.

In this context, the use of formidable programming tools (software) can attract, integrate and make enjoyable the digital life of billions of people around the world.

On the other hand, it also uses the whirlwind of information conveyed by users, duly registered in the domains of social networks, to sell highly profitable marketing services, based on the purposeful treatment of data available by users.

To achieve these goals, networks such as Facebook, Instagram, or Twitter, *in exemplis*, collect data ranging from publications, photos, videos, likes, comments, friends, events, profile information, among many others. From there, it promotes this content to other users with the initial intention of increasing even more their contacts and, consequently, their digital activities.

In this sequence, after collecting and processing the data resulting from the countless digital interactions, the management companies of the referred social networks provide this data to third parties, at high remuneration. We must mention, right now, that due to the advanced treatment of the information collected, it is possible to achieve high levels of return, making digital data a valuable asset.

It happens that, to further boost the interactions and enable the increase of data to be handled, is that social networks eventually edit content primarily served by the users, making them even more attractive. Then, they spread the information to thousands of other users, also disseminating posts, news, publications, comments, photos, likes, reactions, and videos, which fall, also, under the fake news.

Therefore, this article seeks to analyze the responsibility of social networks for the referred content called fake news.

1. THE DIGITAL ENVIRONMENT OF SOCIAL NETWORKS

The social transformations experienced today are strongly promoted by the diverse uses of the Internet and the digitization of content.

Indeed, people can opt for new forms of relationship and identification with digital, *detrterritorialized* networks, of a cultural, social, professional, and political nature.

In fact, the possibilities leveraged by the Internet, of which the multiple uses of digital social networks are a recent example, are automatically connecting people and the world.

In this line, in addition to the potential and great opportunities that we find in these networks, there are implications for society, due to the profound changes in individual and collective behavior, arising from fake news, for example.

We are currently in the midst of a time of change. In this perspective, one of the most impactful and revolutionary transformations is constituted by the activities of society on the Internet.

In this sense, information technologies have been used by society to obtain, manipulate, organize, store, and transmit information in digital form.

Indeed, innovations leveraged by different uses of the Internet have brought changes in the way people relate. In fact, we are experiencing the assumptions, as well as the first impacts, of this inexhaustible source of innovation that has transformed technological development into social transformation.

In short, the Internet and digital communications are opening new paths to transform the way we live, work, learn and relate. The Internet has been a virtual space of convergence and concentration, unprecedented, of the most varied forms of information, communication, commercialization of products, services, and entertainment.

We can risk saying that if everything is not on the Internet, at some stage the subject, the product, or whatever it is, goes through the Internet. Therefore, the data transmitted by digital networks reveal habits and preferences that can, and are, used to influence users' next clicks.

The Internet revolution has changed, and continues to change, the ways in which we organize the world, how we give it meaning, how we interact, and how we look at ourselves and others.

In this context, a factor that contributes to the dissemination of information, content and contacts has been the digitization of data. The possibility of digitizing messages, information, documents, music, videos, software, has facilitated the communication between users.

Accordingly, GIDDENS argues that the traditional communication system has been replaced by integrated systems, where large amounts of information are compressed and transferred in digital format¹. In pertinent conclusion, and as noted, the various conditions of connection increase the number of users and relationships that result from it.

We should also note that the dissemination and spreading of content transmitted over the Internet reaches levels never confronted by law, potentiating the harmful effects of false content, or fake news.

Continuing, in this line, the influence that the Internet causes in the social environment is unprecedented, when compared to any other previous means of communication.

Having said all that, it is worth emphasizing the countless possibilities of using the Internet, such as e-mail, www., texts, e-commerce, and digital social networks. Therefore, the generation of data and relationships arising from this frantic interaction contextualize a new environment, the digital environment.

Such conditions, in fact, make the contexts of interaction and communication over the Internet universal, immediate, simultaneous, and incredibly fast.

On the other hand, the resource of making information available (publishing) can be more easily performed by people. Unlike the previous restricted possibilities (tv, radio, newspaper - in the hands of a few), now anyone can have their profile, and publicize their subjects of interest, in the most varied areas, all over the world.

Messages, posts, music, videos, and images can establish communications between users across the planet. These resources have never been closer to people and companies, and in such a massive and dispersed way, as they are now. So, once again, we must mention that the search and dissemination of information and knowledge is easier with the Internet.

The biggest highlight in this segment is Google, a well-known global search engine that seeks to shorten Internet users to the task of reaching new Web sites through the world wide web. In fact, in the company's own words, Google's corporate mission is "*to organize the world's information and make it universally accessible and useful.*".

Therefore, from now on, the treatment of data is a basic activity of these companies, as mentioned above.

In continuation, for the first time in history, an ordinary citizen or a robot can, easily and at a very low cost, not only have access to information located in the most distant point of the globe, but also create, manage, post, make available and distribute digital content,

1 Cfr. GIDDENS, Anthony. *Sociologia*. Lisboa: Fundação Calouste Gulbenkian, 2009, p. 53.

worldwide, something that only a large organization could do previously, using conventional means of communication. In fact, technological advances leveraged by the Internet make the world increasingly one, bringing individuals and groups together through supranational relations.

Currently, many of us spend more time using new Internet services, connecting with friends on social networks like WhatsApp, Facebook, Instagram, TikTok, QQ, Snapchat, Twitter, among others.

Issues such as marketing, business, community, privacy, politics, sex, love, campaigns, are also issues that are associated with the concept of popular social media platforms. Indeed, there is a profound relationship between online communication tools and the changes in our social relationships.

All these services and utilities have revolutionized the potential for using digital information and relationships. It should be added that this phenomenon of digital social networks currently involves billions of people on the planet.

Therefore, the consequences for society promise to be profound, due to the way we live, work, learn, communicate, entertain, influence, and think.

However, it is important to emphasize that the consequences of these changes are enormous for the future of our societies, which are increasingly digital. However, it is not an evidence that it will prove to be only for good. In the context of fake news, for example, influences can lead to serious consequences.

Having said all that, we conclude that new technologies are not only tools, they form our ways of communication, and the processes of some of our thoughts, and part of our potential attitudes.

2. FAKE NEWS AND THE LIABILITY OF SOCIAL NETWORKS

Initially, at this point, we can state that the digital society is the result of activities, communications and interactions carried out by people and based on the Internet and new technologies.

So, undoubtedly, the change to the abundance of information when we decide what to read, listen to, buy, or watch on the Internet is much greater than what our parents or grandparents had without it. Before, few influences defined our culture. Now, millions of information (data) can form our culture, in a world of infinite varieties and sources.

However, in the professional selection of such influences are the digital social networks, with computer programs that are able, from the treatment and editing of data, to make content available to users.

Within this context, the transfer of information from one individual to another is crucial in any society. Digitization, in the same way, makes it possible to increase the interactive means of communication, allowing an active participation of users.

In social networks, such occurrences are constant.

In this segment, therefore, the impact, influence, and integration power of social networks are enhanced by its activities such as promoting, publishing, editing, controlling content, using data, organizing, listing, sharing, instigating, and promote users to online and offline activities.

Never in history an entity, such as digital platforms, had the power to influence users to do or stop doing something.

Therefore, the publication of an offensive rumor on a page on the social network, with due editing and control by a social network, its consequent organization, listing, promotion, instigation, and requested reaction, quickly spread through the networks, inducing an action by its users, which can lead to serious consequences.

These networks raise their large funds with the services they offer, among others (according to Facebook's "Terms of Service", *in exemplis*, such as: ²,

- "Facebook builds technologies and services that enable people to connect with each other, build communities, and grow businesses. These Terms govern your use of Facebook, Messenger, and the other products, features, apps, services, technologies, and software we offer."

² Vide FACEBOOK. Terms of service. Available at: <https://www.facebook.com/terms> (09.11.2020).

- "We don't charge you to use Facebook or the other products and services covered by these Terms. Instead, businesses and organizations pay us to show you ads for their products and services. By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you." (control, Editing).

- "We provide advertisers with reports about the performance of their ads that help them understand how people are interacting with their content." (organization, listing).

- "Our Data Policy explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described below." (promotion, instigation, and requested reaction).

- "Provide a personalized experience for you"

- "Connect you with people and organizations you care about".

- "Empower you to express yourself and communicate about what matters to you".

- "Help you discover content, products, and services that may interest you".

- "Combat harmful conduct and protect and support our community".

- "Use and develop advanced technologies to provide safe and functional services for everyone".

- "Research ways to make our services better".

- "Provide consistent and seamless experiences across the Facebook Company Products".

- "Enable global access to our services."

It does not take much effort to denote that the referred platforms have the capacity to edit the data, controlling, editing, organizing, promoting, instigating, encouraging, asking for reactions, sharing, spreading through the network, inducing user's actions and reactions, among others.

Therefore, the responsibility advocated in this Article is explicitly described in Facebook's terms of service, for example, by providing that:

"We use the data we have to make suggestions for you and others - for example, groups to join, events to attend, Pages to follow or send a message to, shows to watch, and people you may want to become friends with. Stronger ties make for better communities, and we believe our services are most useful when people are connected to people, groups, and organizations they care about."

“Your experience on Facebook is unlike anyone else’s: from the posts, stories, events, ads, and other content you see in News Feed or our video platform to the Pages you follow and other features you might use, such as Trending, Marketplace, and search. We use the data we have - for example, about the connections you make, the choices and settings you select, and what you share and do on and off our Products - to personalize your experience.”

In other words, the company promotes, instigates, and requests reactions based on the treatment of data.

In fact, it makes no mention of whether what it promotes is good or bad. But even so, it promotes, taking responsibility for what it does.

In continuation, we can still mention, the **“sharing status updates, photos, videos, and stories across the Facebook Products you use, sending messages to a friend or several people, creating events or groups, or adding content to your profile”**.

In the same sense, sending messages instigating users to reactions, such as: “reply”, “react”, “share”, “comment”, “click”. In other words: "do something" about it.

Obviously, many users actually do...

In brief summary, what seems clear is that the activities normally developed by social networks, when it comes to fake news, end up increasing the problem, causing effects for everyone, amplifying the consequences for the promotion that they do. Therefore, they must answer for that, too.

In addition to direct and objective liability, for the actions they promote in their tools, social networks, in many cases, also fail to act.

In effect, offensive publications and fake news that generate actions by its users, have not deserved, usually, activity, control, censorship, or removal by those social networks.

Therefore, they violate the “Terms of Service” of these networks by not “Combat harmful conduct and protect and support our community”³.

It is necessary to emphasize that the control of content editing is ensured in Facebook's “Terms of Service”, for example, in these words:

“Combat harmful conduct and protect and support our community:

People will only build community on Facebook if they feel safe. We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help

3 Vide FACEBOOK. Terms of service. Available at: <https://www.facebook.com/terms> (09.11.2020).

support or protect our community. If we learn of content or conduct like this, we will take appropriate action - for example, offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement. We share data with other Facebook Companies when we detect misuse or harmful conduct by someone using one of our Products.”

Regarding social networks, in general, claim that they have not been “judicially notified” of fake news and offensive content, to do something, and in other cases that only protect the “freedom of expression”, reality shows the opposite: in many cases the networks act on their own and remove famous content when they are “interested” in it, forgetting freedom of expression or any previous judicial manifestation about it.

In other words, social networks have decided what they want to remove, what they want to promote, edit, boost, list, organize, regardless of a court order. In short, they have control over the edition of the contents. They use the need for a judicial decision and freedom of expression only in what they "judge" convenient.

On this subject, the Facebook CEO, below, demonstrates the power to direct its 2 billion users to real news, and to ward off the so-called fake news.



Mark Zuckerberg ✓
16. April · 🌐

I want to share an update on the work we're doing to connect people with March, we displayed warnings on about 40 million posts related to Covid-19 based on 4,000 articles reviewed by independent fact-checkers. When people saw those warning labels, 95% of the time they did not go on to view the original content.

We're also launching a new feature called Get The Facts, a section of our Covid-19 Information Center featuring articles written by independent fact-checking partners debunking misinformation about the coronavirus. We will also soon begin showing messages in News Feed to people who previously engaged with harmful misinformation related to Covid-19 that we've since removed, connecting them with accurate information.

Through this crisis, one of my top priorities is making sure that you see accurate and authoritative information across all of our apps. I hope all of you are staying safe, healthy and informed.

👍❤️😬 140.864 13.573 Kommentare 8.173 Mal geteilt

➦ Teilen

4

4 Available at: <https://www.facebook.com/zuck/posts/10111806366438811> .

The illustration above demonstrates the company's editorial power, demonstrating its ability, when it wishes, to remove content called fake news. Therefore, the social network's liability is assumed.

Now, for all the titles, companies, such as Facebook, exercise editorial control over the contents of their digital environments. In this step, must be remembered, that Facebook itself explicitly promotes these qualities of control of the contents and data of users, to the companies that hire its services:

*“We don't charge you to use Facebook or the other products and services covered by these Terms. Instead, businesses and organizations pay us to show you ads for their products and services. **By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you.**”*

In the sense of the aforementioned, and corroborating what we have alluded to in the introductory section of this Chapter, is that social networks such as Facebook, Instagram or Twitter, collect data ranging from publications, photos, videos, likes, comments, friends, events, profile information, and more. From there, the networks promote this content to other users to increase their contacts and, consequently, their digital activities. Then, after collecting and processing the data resulting from the countless digital interactions, the referred social networks provide this data to third parties, at high remuneration. Therefore, to further boost interactions and enable the increase of data to be processed, it is that social networks end up editing content, first broadcast by users, making them even more attractive. Then, social networks spread the information to thousands of other users, disseminating posts, news, publications, comments, photos, likes, reactions, and videos, including fake news.

In this table below, considering what happens inside Facebook, for example, it is evident that the Company has strict liability when it transmits fake news:



Timely and necessary, the appreciation in this plan, that international jurisprudence has been gradually accepting, and insofar as they understand what networks do, the thesis that social networks are responsible for offensive content and fake news that cause damage to others.

In a direct approach, media companies have the responsibility to moderate the content when they assume in their "Terms of Service", or in fact carry out activities, in which they edit, control, organize and disseminate the content initially generated by their users, through “password” to enter the website, inside the digital environment of the companies.

What is beginning to be recognized is that social networks are responsible for entering and editing information in the first place. That is really the main difference. The current situation is that media companies are responsible not only for canceling comments or posts when they notice them, but for preventing them from uploading in the first place, or from continuing online, or even from the social networks themselves continuing to disseminate the content. This places a significantly greater burden, of responsibility, on what social networks profit, than was previously in force and understood.

In our understanding, as social networks use the pages from the perspective of their own commercial interests, they effectively assume the risks of defamatory comments, and

fake news that cause harm, made initially by their users, but controlled, promoted and edited by these networks.

FINAL CONSIDERATIONS

For everything analyzed, we found the liability of social networks on the content called fake news, when broadcast in their digital environments, duly controlled by them, through passwords.

In an identical angle to what we defend in this Article, there are the judicial positions taken, increasingly, in Australia, India, United Kingdom, United States, Germany, and France when it comes to the strict responsibility to Content Editors and controllers, such as digital social networks.

Indeed, leading Internet companies, such as Facebook, Twitter, and Instagram, are operators of social media platforms, publishers of editorial content.

If not, in fact, the platforms then offer open access and “free” of any legal and judicial limitations.

In the digital environments of networks, platforms must follow the rules and, yes, insofar as they gain the financial benefits of data processing, they must restrain criminal practices carried out within the networks themselves, managed by passwords granted by the networks (environment controlled by the networks).

If the social network controls the digital environment, then it is responsible for the same space.

No environment, however “cool”, can serve to cover up, or even “leave”, criminal practices to thrive, like many fake news.

Social networks have the power to transmit and process data. With that power came the responsibilities.

However, networks want to reap the financial benefits of being Content Editors and Controllers, **without being responsible**.

So, if it is true that networks have editorial power, as they decide which specific news, research results, reactions and posts will show us in our timelines (and that of all other users), among the billions of people and possibilities, then we should treat them legally as such. In other words, as responsible.

In fact, the liability must be recognized.

Freedom of speech is not above crimes. Whoever disseminates fake news and who drives fake news, must be responsible for that.

Indeed, the alleged prohibition on freedom of expression cannot be a subterfuge for the promotion of crimes.

Social networks are “no man's land”, where everyone can carry out criminal activities freely, and only after a court decision, and if there is time, something will be restrained.

For the same reasons explained above, companies can remove content - if they can do it through a court order, they can do it without the same order.

This is because, when editing the content, the networks assume the function of supervising it, under penalty of being co-authors.

Consequently, what are the “Terms of Service” for, if not to enforce them?

On the contrary, instead of controlling what is shown in their digital environments, social networks handle information, edit, control, profit and encourage reactions: “like”, “comment”, “share”. But they do not accept to be held responsible for the consequences.

Therefore, after careful analysis, we conclude that social networks are responsible for fake news, when networks disseminate the content in their own digital environments.

REFERENCES

- BAKARDJIEVA, Maria. *Internet Society: The Internet in Everyday Life*. London: SAGE, 2005.
- BRAZIL. General Data Protection Law. Law number 13.709 (08.14.2018), Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm .
- CARR, Nicholas G. *The Big Switch: Rewiring the World, from Edison to Google*. New York: Norton & Company, 2008.
- CASSESE, Sabino. *Regulation, Adjudication and Dispute Resolution Beyond the State*. Heidelberg: Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, Fall, 2008.
- CASTELLS, Manuel. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press, 2003.
- COUNCIL OF EUROPE. *Convention on Cybercrime*, Budapest, 2001.
- DIXON, Helen. *Regulate to Liberate. Can Europe Save the Internet?* New York: Foreign Affairs. September 19, 2018. Accessed September 19, 2018. Available at <https://www.foreignaffairs.com/articles/europe/2018-08-13/regulate-liberate> .
- DRAETTA, Ugo. *Internet et Commerce Électronique en Droit International des affaires*. Paris: Forum Européen de la Communication, 2003.
- DUTTON, William. *Social Transformation in an Information Society: Rethinking Access to You and the World*. Paris: United Nations Educational, Scientific and Cultural Organization, 2004.
- FACEBOOK. Terms of service. Available at: <https://www.facebook.com/terms> (09.11.2020).
- FREIRE E ALMEIDA, Daniel. A Global Digital Society. *LAWINTER REVIEW*, v. VII, p. 458-498, 2016.
- FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016.
- FREIRE E ALMEIDA, Daniel. *International Law under a New Digital Dimension*. *CIFILE- JOURNAL OF INTERNATIONAL LAW (CANADA)*, v. I, p. 001-008, 2019.
- FREIRE E ALMEIDA, Daniel. *The Taxation of Electronic Commerce in The United States of America And in The European Union*. 1. ed. São Paulo: Almedina, 2016.
- FREIRE E ALMEIDA, Daniel (Org.). *Os Cybercrimes na Perspectiva do Direito Internacional na Internet*. 1. ed. New York: Lawinter Editions, 2020.

GIDDENS, Anthony. Sociologia. Lisboa: Fundação Calouste Gulbenkian, 2009.

GOOGLE SPAIN SL AND GOOGLE INC. V AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ, Available at <http://curia.europa.eu/juris/document/document.jsf?text=&docid=153853&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=380763> .

INTERNATIONAL TELECOMMUNICATION UNION- ITU. Digital.life. Geneva: ITU, 2006.

KHOR, Zoe, MARSH, Peter. Life online: The Web in 2020. Oxford: The Social Issues Research Centre, 2006.

LESSIG, Lawrence. Free Culture. How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity. New York: The Penguin Press, 2004.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons regarding the processing of personal data and on the free movement of such data. Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT> .

SEGAL, Adam. When China Rules the Web. New York: Foreign Affairs. September 19, 2018. Available at <https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web> .

THE FOUNDER TREATY OF AN INTERNATIONAL TRIBUNAL FOR INTERNET, in FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016.

UERPMANN-WITZACK, Robert. Internetvölkerrecht. Archiv des Völkerrechts, Volume 47, Number 3, September 2009.

UERPMANN-WITZACK, Robert. Principles of International Internet Law. German Law Journal, Volume 11, nº 11, 2010.