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

CYBERLAW by CIJIC

EDIÇÃO N.º IX – MARÇO DE 2020

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

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Globalização. Tecnologia e Inteligência artificial. Mobilidade organizacional e individual. Manipulação. A pandemia de Coronavírus. Hoje. O futuro.

Vivemos tempos "*estranhos*". Acutilantes. Irresolutos. Contingentes. Exigentes. O "tema" que nos capta, quase em exclusivo, a atenção, desde o início do ano de 2020, é a pandemia de coronavírus. Aquela dinâmica, rotineira, até agora tida como "garantida" atravessa momentos de grande indeterminação. Hora a hora somos como que bombardeados com números esmagadores: de taxas mundiais galopantes de infectados, doentes em cuidados intensivos, de mortos. No passar deste tempo, diariamente, deambulámos entre um imoderado e célere na disseminação da infecção *versus* um vagaroso e fleumático passo na demonstração de resultados animadores no seu combate. O racional económico de «custo-benefício» geralmente revelaria a perigosidade associada à extrema cautela. Porém na questão, truncada, do coronavírus é diferente[1]. "*Achatar as curvas*", "*Proteger os mais idosos e os mais vulneráveis*", "*Suster a vaga de procura do SNS por forma a dar-lhe tempo para acudir às solicitações*", mesmo que o custo seja o parar da Economia. Global. Entretanto o tempo continua o seu passo. Assim como a epidemia há-de passar.

1 Cass Sunstein @ https://www.bloomberg.com/opinion/articles/2020-03-26/coronavirus-lockdowns-look-smart-under-cost-benefit-scrutiny

E, quando aí chegados, a questão resolutiva a colocar não deverá andar muito longe de um: "*Que mundo esperar do pós-covid19*"?

O avanço da tecnologia, combinando melhores recursos de *hardware* com inteligência artificial, aos quais o Homem socorre, permitiram sequenciar o genoma do COVID-19 em menos de um mês. A inteligência artificial, por exemplo, num contexto, global, de recursos exíguos tem sido testada para suprir lacunas críticas nos recursos de saúde, ajudando à racionalidade da decisão política, alavancando centros de inovação em inteligência artificial, robótica e automação em saúde. Na Ásia[2]. Por agora.

O mesmo avanço tecnológico, por sua vez, no actual cenário de "*guerra*" ao vírus, colocou a ponderação das liberdades fundamentais num estádio de confronto titânico. Recuperando o "*achatar a curva*", um pouco por todo o mundo, os governos, democráticos, colocaram os respectivos países em *lockdown*. Sem cautelas. Entre confinamentos e quarentenas obrigatórias, um recurso parece permitir - em face da falta de meios humanos para controlo efectivo de milhões de cidadãos - fiscalizar o cumprimento das directrizes estatais. A tentação executiva por esse controlo, universal, dos cidadãos preclude a fruição de múltiplas liberdades constitucionalmente consagradas. O racional da discussão que vinha sendo tido até agora[3], deslocou-se, por via do perigo abstracto que a pandemia comporta, da questão securitária *versus* liberdades fundamentais para "*saúde pública*" *versus* liberdades fundamentais.

Um pouco por todo o ocidente democrático, a tónica recursiva tem passado pelo uso da "*vigilância digital* estadual[4]". Tal como um pouco por todo o mundo, direitos humanos fundamentais[5] são colocados em teste face à imposição destas regras "excepcionais". O Estado de emergência tende a permitir, justificando múltiplas

2 Eficiência, especialidade, racionalidade, sistemas capacitativos e colaborativos público-privados. O trabalho dos dados ao serviço dos povos. https://www.technologyreview.com/s/614555/ai-in-health-care-capacity-capability-and-a-future-of-active-health-in-asia/

3 « Tribunal Constitucional chumba acesso das secretas a registos de comunicações», @ https://rr.sapo.pt/2019/09/19/politica/tribunal-constitucional-chumba-acesso-das-secretas-a-registos-de-comunicacoes/noticia/165164/

4 Por exemplo: https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

5 Por exemplo, no contexto da América do Sul, «Sociedade civil pede que tecnologias usadas devido à pandemia respeitem os Direitos Humanos», @ https://idec.org.br/noticia/sociedade-civil-pede-governos-da-america-latina-e-caribe-que-tecnologias-digitais-aplicadas

intrusões como *adequadas*[6], *necessárias e proporcionais*[7]. A questão, sendo excepcional e de carácter limitada no tempo, deveria ser pacificamente tolerada pelos cidadãos. Afinal, sob o manto de um fundamento como o "*interesse público*" [8] e salvaguarda da "*saúde pública*" até a limitação do escopo de protecção, desde logo, da privacidade de dados pessoais sensíveis claudica[9].

---

6 No parecer 32/2020, a CNPD, delimitando geograficamente a aplicação de videovigilância por drones ao concelho de Ovar, dada a excepcionalidade da cerca sanitária entretanto imposta, reitera que "(…)as restrições aos direitos fundamentais devem limitar-se ao estritamente necessário às finalidades visadas com este sistema de videovigilância ", recomendando, adicionalmente, "que se garanta que a captação de imagens assim realizada salvaguarde a privacidade daqueles que se encontrem nas respectivas habitações", e, "que se garanta o direito de acesso às imagens gravadas , nos termos legalmente previstos", bem como que se adoptem "medidas adequadas a garantir a integridade das imagens gravadas no processo de transferência dos registos(…) para o "contentor de informação encriptado"" . @ https://www.cnpd.pt/home/decisoes/Par/PAR_2020_32.pdf

7 Por exemplo, em Espanha, a AEPD: «(…)*Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.* ***Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia****, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.* ***Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.*** *Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.* ***Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma****, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.****Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.»*** @ https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

8 A limitação ao tratamento de dados sensíveis, por exemplo, de saúde sucumbe ante "*razões de interesse público nos domínios da saúde pública*", desde que «(…)***Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias»*** (Considerando 54 in fine) .

Considerando *(54) « O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.o 1338/2008 do Parlamento Europeu e do Conselho (11), ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade(…)****».***

9 Confirmando o Considerando (54), ainda, da leitura conjunta **das alíneas g) e i) do Art.o 9, n.º2, RGPD**: «**G)** *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;*», e**, i)** « *Se o tratamento for* ***necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde*** *ou para assegurar um elevado nível de qualidade e de*

Mas há um "*senão*". O receio de que a excepcionalidade vire regra é real[10]. Com efeito, é inegável que, neste momento, os receios de Yuval Harari [11], criador de *Homo Deus*, sejam partilhados por muitos de nós. Tal como as considerações de Joel P. Trachtman, quanto aos benefícios de um mundo global[12]: benéfico se mais cooperativo, com capacidades regulatórias internacionais reforçadas ao nível da saúde, cibersegurança, proteção ambiental e crises financeiras.

Ambos convergem na necessidade de compromisso, de partilha, cooperação e solidariedade global. O que se conclui espontaneamente dos apontamentos citados, através de um silogismo categórico: ameaça sobre todos os países, ameaça global, logo, resposta de todos os países, global. Não obstante, será que hoje temos líderes políticos mundiais à altura dos desafios[13] pungentes que se nos colocam nestes termos?

E no futuro?

---

segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;». @ https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

10 Yuval Harari:«(…) *Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.", @* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

11 Harari: «(…) *In this moment of crisis, the crucial struggle takes place within humanity itself. If this epidemic results in greater disunity and mistrust among humans, it will be the virus's greatest victory. When humans squabble – viruses double. In contrast, if the epidemic results in closer global cooperation, it will be a victory not only against the coronavirus, but against all future pathogens*.», @ https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

12 Joel P. Trachtman, «(…) *Not all global problems result from globalization. For those that do, globalization itself can ameliorate them to some extent. Furthermore, we can establish international laws and institutions to minimize those problems that do arise from globalization: globalized governance to respond to globalization-induced problems. This is smart globalization, and once we do it this way, it is likely that globalization should be retained because, on net, it will make us better off*.", @ https://www.bostonglobe.com/2020/03/30/opinion/not-all-global-problems-result-globalization/

13 Ainda Harari: «(…)*Today humanity faces an acute crisis not only due to the coronavirus, but also due to the lack of trust between humans. To defeat an epidemic, people need to trust scientific experts, citizens need to trust public authorities, and countries need to trust each other. Over the last few years, irresponsible politicians have deliberately undermined trust in science, in public authorities and in international cooperation. As a result, we are now facing this crisis bereft of global leaders that can inspire, organize and finance a coordinated global response*.», *idem*.

Gerd Leonhard, num exercício curioso reproduzido no Diário de Notícias, destaca dois aspectos cruciais. Circunscrevendo-nos à tecnologia, esta *"tornou-se a nova religião"*. "*Estamos a entrar num novo Renascimento*". *O próximo passo será regulamentá-la de forma mais apertada com o objetivo de que humanos e o próprio planeta beneficiem do progresso tecnológico.* Não obstante, esta relação acabará seduzir-se ante uma *vigilância estatal por meios tecnológicos* (que) *irá tornar-se o novo normal após as medidas extraordinárias que foram tomadas para controlar esta pandemia*[14].

E como já vai longo, para concluir, convocamos, novamente, a questão fundamental: "*Que mundo esperar do pós-covid19*"?

A provocação desconcertante e acutilante que se impõe, inclusive politicamente, não poderia ser outra: «*Of course, even if we disappear, it will not be the end of the world. Something will survive us. Perhaps the rats will eventually take over and rebuild civilization. Perhaps, then, the rats will learn from our mistakes. But I very much hope we can rely on the leaders assembled here, and not on the rats.*» [15]

Nesta nova edição da «Cyberlaw by CIJIC», procuramos sustentar o crescimento paralelo que o Mestrado de Segurança da Informação e Direito do Ciberespaço[16] vai granjeando. É pois, com orgulho, que passaremos a destacar produção deste, com maior regularidade. Afinal, este é um desígnio da própria criação da revista. Provavelmente, num futuro não muito distante, estará na calha a edição em papel de futuras edições. Se há questão que se nos colocou com o teletrabalho foi: qual a redundância digital? *Ie*, sem acesso à internet, ou sem eletricidade/bateria, como é que seria possível aceder

14 «Não haverá normal: futuristas preveem mudanças permanentes pós-coronavírus», @ https://www.dn.pt/dinheiro/nao-havera-normal-futuristas-preveem-mudancas-permanentes-pos-coronavirus-11987179.html

15 Yuval Harari: «Yuval Harari's blistering warning to Davos», @ https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/

16 Mais informações @ : https://fenix.tecnico.ulisboa.pt/cursos/msidc

a conteúdos para efeitos de estudo? Como ler(aceder) nestas circunstâncias? Como mitigar a "info-exclusão" quando o sistema não é propriamente redundante na acessibilidade[17]?

Reavendo, nesta edição, incorporando conteúdo em inglês escrito, por força de deveres de participação, cooperação e colaboração internacional[18] que muito nos orgulha, procuramos revisitar temas como cibersegurança em contexto marítimo, dados pessoais e dados não pessoais, monitorização de trabalhadores em contexto laboral, a regulação jurídica do ciberespaço - mutação do paradigma à luz do acórdão James Elliot, *Phishing*, redes sociais e manipulação da opinião pública, o problema da mobilidade em contexto organizacional, e, os desafios da cibersegurança forense de *smartphones* no continente africano. Os temas são oportunos. São, igualmente, desafiantes. São, finalmente, abertos a colaboração múltipla, participada.

Resta-me agradecer a todos quantos contribuíram para mais uma 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 justíssimo: - Muito Obrigado.

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

Boas leituras.

Lisboa, FDUL, 29 de Março de 2020

Nuno Teixeira Castro

17 Por exemplo, «Ministro Siza Vieira admite aulas por canais "estilo youtube" ou TV por cabo.», @ https://observador.pt/2020/03/29/ministro-siza-vieira-admite-aulas-por-canais-estilo-youtube-ou-tv-por-cabo/
Mas, sem acesso internet, ou sem cabo – até porque a cobertura não é de 100%, há, pelo menos, cerca de 20% de famílias sem acesso ao Cabo – como é que as crianças e adolescentes que se encontrem nesta situação se integram? Como é que se combate esta exclusão digital?
18 Um trabalho colaborativo ímpar. @ https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic

DOUTRINA

SOCIAL NETWORKS AND PUBLIC OPINION MANIPULATION IN DEMOCRATIC REGIMES

NATHÁLIA CARVALHO SCHMIDT DE DEUS [1]

1 Lawyer and Master student at Faculty of Law in the University of Lisbon, in Public International Law, 2018/2020; Master student in Information Security and Cyberspace Law in the University of Lisbon; "Instituto Superior Técnico" of Lisbon and Naval School of Portugal, 2019/2021.

ABSTRACT

Based on a multi – dimensional view, this article aims to analyze the acts of public opinion manipulation in democratic regimes. Therefore, a juridical approach has been used in the perspectives of International Law and Domestic Law with bases on technological science to facilitate the understanding of certain means of executions in the control of social media.

Keywords: Social networks, technology, botnets, Law, Democracy, Public Opinion, control, manipulation.

1.INTRODUCTION

The evolution of media enables us through social networks a popular participation once unthinkable in the democratic activity of the present day.

It should be noted that there is no exact definition for democracy, but it would be the only power organization safeguarding individual freedom and all the elements that structure it, such as political pluralism, freedom of expression, freedom of information, freedom of communication.

If the direction of public opinion in a particular sense tends to bind democratic decisions and, if the result materializes in the way of secret scrutiny or through popular participation by referendum, the analysis in the field of the source of formation of these opinions in the media is required. Using the development of this view we can generate concrete and diffuse effects within society.

If the democratic regime is established in the structures provided by the legal certainty of fundamental rights, the decisive political impetus on the part of its citizens cannot be threatened to limit their free expression of will and consequently cause a chilling effect that hinders the free development of society. The present activity of online information exchange is an area still under regulatory development by states, which are far from establishing definitive rules by mutual agreement, even due to the dynamism that is outlining technological developments. Because of this, several political and economic crises are being noted and the issue of democratic regimes is a subject of much discussion today.

In turn, the network comes in opposition to the rigid and centralizing forms of social and political entities, when it presents an idea of decentralization, an aspect that produces social transformations.

The goal of this report is to establish an approach to the existence of what types of domestic and international legal violations are subject to acts that manipulate public opinion and their means of enforcement in social networks. But in order to do so, two aspects need to be distinguished: law from the point of view of the internal politics of a state; and law from a foreign policy point of view.

2. THE MANIPULATION OF PUBLIC OPINION IN STATE POLITICS

There are many ways usually used to manipulate public opinion, from fake news that violates the good name of the agents and political entities, or even through truthful news affecting personality rights, or the use of sensationalist images that touch a particular collective group, or the use of messages of superficial and political content that tend to manipulate recipients without instruction on subjects or without a sense of criticism. These are the manipulative forms that have existed for many years offline and have not been triggered by an incisive influence on the general public tending to direct some sense in state internal politics to a point of destabilizing it. However, the current manipulation methods are generated by machines that have such potential to reach a massive number of people and much more effectively than a mere influence by television.

We should be able to distinguish between: publications made by responsible journalism under guarantee of press rights corollary of freedom of expression in the pursuit of publication of information in the public interest and publications published by anonymous or sponsored individuals, used with political interests, which aim to use manipulative technological tools of public opinion. The first one has an investigative role within democracies and interference by public authorities must be restricted so that it does not cause an inhibitory effect on their performance or "chilling effect"; the second one refers to the ways of using the media for the behavior of certain illicit acts or of personal interests, often anonymous and not intended to inform. The first is protected by freedom of expression, by international law of the human person, should not have the intention of helping those in power or in groups of political parties; but the second, the interest in helping the policies of entities and the use of instruments of "information operations" that is the use of information technology to achieve government objectives[1].

1Torsten Stein; Thilo Marauhn, *International Law Aspects of Information Operations*, ZaöRV 2000, p.1. Available in: https://beck-online.beck.de/Bcid/Y-300-Z-ZAOERV-B-2000-S-1-N-1, (last access in 03/28/2019).

The right to freedom of propagation rooted in the freedom of expression is understood to be a defense mechanism against the state "prohibiting all direct and indirect state interference, public or subtle, official or non-official, in the conformation and selection of schedule content or a particular program"[2]. Considering the democratic and constitutional relevance in the non-interference of public authorities in the areas of communication (art. 34º, item 4, "Constituição da República Portuguesa", hereinafter designated "CRP").

In reinforcement of this constitutional precept, art. 10 of the European Convention on Human Rights (hereinafter "ECHR") states that "everyone has the right to freedom of expression. This right shall include freedom of opinion and the freedom to receive or impart information or ideas without interference by any public authority and without consideration of borders..." In addition to its broad provision in several other international documents: Article 11 of French Declaration of Human and Citizen's Rights; Article 19 of the Universal Declaration of Human Rights (hereafter "UDHR"); Article 13 of the American Convention on Human Rights (ACHR).

All of these individual freedoms depend on the non-interference of any public authorities and may be considered, directly or indirectly, manifest or subtle, official or unofficial. Predictions in international documents play a role in guaranteeing these constitutionally guaranteed freedoms.

2.1. The online misinformation

All forms tending to manipulate public opinion vitiate the free manifestation of the collective will of a society, by which it can be called digital, since it is predominantly linked to digital media. Article 21.3 of the UDHR states that "the will of the people is the foundation of the authority of public authorities; and must be expressed through honest elections to be held periodically by universal and equal suffrage, by secret ballot or by an equivalent process safeguarding freedom of vote".

2 Raquel Alexandra de Jesus Gil Martins Brízida Castro, Constitution, *Law and Regulation of the Media: Contribution to the Study of the Portuguese Constitution of Communication*, PhD in Law, Legal-Political Sciences, University of Lisbon, Faculty of Law, 2014, p. 426.

However, any result achieved in the political context of online misinformation is due to a contaminated will to the detriment of its free expression due to the intention of misleading the electorate also contracting online social networking services, and the techniques used for the manipulation of public opinion in the private sphere are tools that endanger individual freedoms by their high incisive power. The violation of individual fundamental rights serves as a means of satisfying the objectives of persons exercising or about to exercise public power. These are people who use the vulnerability still existing in democratic regimes and their predisposed tools in the media to violate the regime or system itself.

Another context is the social networking services used by users made available by online platforms in the consent and acceptability of their security terms, which are legal relationships subject to contractual liability and must obey the laws in force, whether or not provided for in the contract.

Contractual liability arises from a "non-fulfillment or defective fulfillment of a pre-existing obligation resulting from a contractual wrongdoing". While non-contractual liability is a "breach of the general duty to abstain"[3].

As soon as there is a contract between the user and the online platform providing social networking services, we can conclude that the conflicts resulting from this agreement is resolved within the contractual liability area itself.

On the other hand, with regard to tortious liability, Article 485 (1) of the Civil Code provides advice, recommendations or information by stating that "simple advice, recommendations or information shall not hold anyone liable, even if there is negligence on their part". But there are three exceptions to Article 485 (2): a) "when the information

3 Francisco dos Santos Amaral Neto, "Civil Liability", in João Bigotte Chorão (Dir), *Polis Encyclopedia Verb Society and State, Anthropology, Law, Economics, Political Science*, vol.5, Lisbon / São Paulo, Verb, pp. 466-474 (pp. 468-469).

provider has assumed responsibility for the damage that the information could cause; b) when there was a legal duty to give advice, recommendation or information and was done with negligence or intent to prejudice; c) when the agent's procedure constitutes a punishable fact".

We know that within social networking platforms, political people join the service, with or without the acronym of the agency it represents. The duty to inform is done by official public act outside the context of social networks. Since the official means of publication exist, the use of social networks becomes merely optional and not substitute of the official means of publication. The use of social networks by public agents only serves to reinforce the disclosure of a particular subject, as it comprises a right submerged by the freedom of expression characteristic of the democratic regime. However, online communication networks may be used with the intent of harming users by misunderstanding the information provided.

If the public agent had a duty to disclose any information he should do so through appropriate administrative acts and not merely through social networks. If it only proceeded with the publication on social networks, it acted negligently, as it is not considered an official public act when using that legal faculty. When disclosing information online with the intent to harm on must likewise be subject to the obligation to indemnify. Finally, compensation will depend on what is considered to be a punishable fact in the context of communication via social networks.

The doctrine of tortious liability establishes as one of the presuppositions of violation the practice of an act that constitutes an abuse of law, embodied in articles 334, 484, 485, 486, 491, 492 and 493 of the Civil Code; Among them, Articles 334 and 485 deserve to be highlighted in the matter.

Even if he holds a public authority and he formally respects his powers that are conferred on him, exercising a right that is questionable to the fundamental values of the legal system[4], illegitimate acts are configured.

According to Article 334 of the Civil Code, it is found that abuse of the right is nothing more than the proprietor's manifestly exceeding the limits imposed by good faith, good morals or the economic and social purpose of that right. This is a violation of the legal prohibition that reveals an Aquilian liability situation.

It should be noted that this article is normally compared with the German BGB's §826 clause on good manners, but unlike that doctrine, Portuguese Civil Law does not require the presence of deceit, even in its eventual form of deceit, to damage is compensated[5]. If the information is provided in a manner that is distorted and contrary to good morals or the economic and social purpose, by the agent, there should be reimbursement even if the intent was not present.

The presence of the damage, which in the context of social networks, is linked to misuse of information, tending to violate personality rights and private rights, related to good name, reputation, the image of a collective person or group or even messages of violence and hatred, compensation should be provided when the prosecution of the agent is punishable.

Much has been mentioned about hate speech on social networks. Therefore, it is important to quote about the decision of the Strasbourg Court in the case of *Delfi AS v. Estonia*, where "hate speech" does not have a well-defined and universally accepted definition. The theme covers a wide range of hate messages, ranging from offensive to derogatory remarks and comments, stereotypes, abusive and negative, intimidating, inflammatory speeches that incite violence against specific individuals and groups. It also

4 Manuel A. Carneiro da Frada, *A "Third Way" in Civil Liability Law? The problem of attributing damages caused to third parties by company auditors*, Coimbra, Almedina, 1997, p. 49.
5 *Ibid*., p. 51.

reiterates that only the most notorious forms of hate speech, ie those that constitute incitement to discrimination, hostility and violence, are considered illegal[6].

2.2. Competition and Pluralism

Concerning competition and pluralism, acts aimed at promoting online misinformation through computer tools ultimately trigger the concentration of ownership. Competition rules must take into account media pluralism concerns[7], but techniques of manipulating public opinion are threats that put them at risk. Abuse of the above mentioned right, in the context of the media, can be referred to as "abuse of public opinion"[8].

The current Portuguese legal-constitutional order provides for freedom of expression and information, freedom of the press and media in Articles 37 and 38 of the CRP. The Constitution does not prohibit any sector of private or even non-economic /economic activity in the performance of these fundamental guarantees[9].

The monopolization of information is very dangerous especially in democratic regimes that may be susceptible of political manipulation. The use of information, when used as a manipulative computational management tool, other alternative media, plural and free competition in the information market, end up being a refuge that ensures the democratic principle.

The Constitution expressly enshrines as the fundamental principle of economic and social organization the principle of the subordination of economic power to democratic political power[10], and sets out certain priority tasks of the State, in particular, "to ensure the efficient functioning of markets so as to ensure balanced competition between

6 Delphi AS v. Estonia, Appl. No. 64569/09, judgment of 8 June 2015. Available in footnote 9, paragraph. 28, p. 70 at: http://hudoc.echr.coe.int/eng?i=001-155105 (last accessed 09/20/2019).
7 Raquel Castro, *ob.cit*., p.381.
8 *Ibid*., p.383.
9 Evaristo Sousa Mendes, *Annotation to Article 61, in Annotated Portuguese Constitution*, Tome I, 2nd Edition, MIRANDA / MEDEIROS, Coimbra, Coimbra Publisher, 2010, p. 1210.
10 Article 80, item (a) of the CRP ("Constituição da República Portuguesa").

companies ", but to this end," it is necessary to "counter monopolistic forms of organization and to repress abuses of dominant position and other practices harmful to the general interest"[11]. Ways of disseminating, for example, through automated services, online misinformation by private companies, even at the request or under the payment or exchange of favors, by anonymous political agents, endanger these constitutional precepts.

Even if there is a Regulatory body such as the ERC, the eminent Professor MIRANDA warns of the existence of an unconstitutional omission, considering that the assignment of his function is insufficient to all titles[12].

The concern to ensure the pluralism brought by the ERC, Media Regulator, is restricted to the functioning of the press market, in order to enable its transparency, the confrontation of information and the various currents of opinion, the quality of publications allowing a wide choice by consumers[13], which turns out to be an alternative when systems linked to social networks suffer manipulative threats of information by automated technological methods, to the detriment of the right to be informed. It should be noted that the right to information is a fundamental right and has a very significant link with the democratic principle. The development of public opinion depends on the guarantee of this right.

2.3. Violation of electoral rights

Techniques used to trigger mass online misinformation by political interests undermine the principle of equal opportunities and the treatment of various candidatures in election campaigns, as provided for in Article 113 (3) (a) of the CRP. These are techniques that give priority to the dissemination of mass publications that favor one

11 Article 81, item (f) of the CRP ("Constituição da República Portuguesa").
12 "The unconstitutional legislative omission has to do with the lack of enforceability to constitutional command. This omission is compounded by a constant phenomenon of concentration according to purely economic motives". Jorge Miranda, "Freedom of Social Communication and Public Service of Radio and Television", in Carlos Blanco de Morais and others (coord), *Media, Law and Democracy*, Coimbra, Almedina, 2014, p.28.
13 Raquel Castro, *ob.cit.*, pp. 397-398.

political party or political agent over the others, to the detriment of the equal opportunities sought in an electoral campaign. The equality sought is that which allows for parity of rights between candidates.

The freedoms guaranteed by the Constitution, such as freedom of propaganda and freedom of expression, cannot be confused with these techniques. The act of provoking disinformation affronts and disturbs the Democratic Rule of Law, while the principle of freedom of expression and freedom of propaganda is the corollary of the regime itself and its purpose is to protect it against any threats. The right to freedom of expression cannot be exercised as a tool that threatens the democratic regime itself, when its role is precisely to protect it.

The fairness of the electoral process and universal and equal suffrage by secret ballot depends on the internal legal and political security that ensures the free expression of the will of voters in accordance with Article 25 (b) of the International Covenant on Civil and Political Rights, at the disposal of : "Every citizen shall have the right and the possibility, without any of the forms of discrimination mentioned in Article 2 and without unfounded restrictions: (b) to vote and to be elected in periodic, authentic elections by universal and equal suffrage and by secret ballot, that guarantee the manifestation of the will of the voters ".

There are several techniques that tend to lead to online misinformation in order to manipulate public opinion. In addition to being user-made, they can be based on algorithms; advertising oriented; facilitated by technology[14].

To highlight, according to the practical code of misinformation of the European Union "the notion of "Disinformation" does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary,

14 See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Online Misinformation: A European Strategy, Brussels, 26.4.2018 COM (2018) 236 final, p. 6. Available in:https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-236-F1-PT-MAIN-PART-1.PDF, (last time accessed 12/27/2019).

and is without prejudice to binding legal obligations, self-regulatory advertising codes, and standards regarding misleading advertising"[15].

2.4. Perpetrated by users

When dealing with the activity of users, they are those characterized as end consumers of the services provided by social networks. Users share fake news and play that role in spreading misinformation by adopting a habitual practice of not checking its accuracy.

False news tends to spread in manner viral. In France, a fake news platform has been found to generate over 11 million interactions per month - five times more than reputable news brands. However, "in most cases, in France and Italy, fake news agencies do not generate as much interaction as established news brands"[16].

2.5. Based on Algorithm

Algorithms used for the purpose of generating online misinformation are prioritization-based tools when displaying business-driven information from the online platform and by adopting ways that focus on personalized, sensational, attention-grabbing content that will be shared by related users. Consequently, algorithms increase polarization and strengthen the effects of misinformation[17].

However, it is important to note how networks work and how these generated links may or may not have propagation potential.

15 EU Code of Practice on Disinformation, Preamble, available in: https://ec.europa.eu/digital-single-market/en/news/code- practice-disinformation (last time accessed 12/17/2019).
16 Measuring the reach of 'false news' and online misinformation in Europe, Reuters Institute https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-onlinedisinformation- Europe (last time accessed 12/17/2019).
17 See Communication from the Commission to the European Parliament, Tackling Online Misinformation: A European Strategy, *ob.cit.*, p.6.

The notion of network itself reflects a characteristic of complexity. Regarding the latter, it should be noted that "Most systems do not work in a simple linear fashion"[18], that is, they work with nonlinear mathematical models. Thus, even identifiable behaviors of individual entities are insufficient to predict the evolution of the whole, and these systems are usually described in terms of probability. This complexity that assumes a mathematical modeling is known as "Network Science"[19].

For this, it is necessary to understand the dynamics of a complex network in the occurrence of an evolution, because the links are not distributed equally (randomly, in terms of mathematics), and are not organized in an orderly manner, presenting three main characteristics: 1) *small world networks*; 2) *scale-free networks* and; 3) *promote viral spread*[20]:

1) *Small world networks*: According to the "Watts-Strogatz Model" (WATTS & STROGATZ, 1998), what happens is that these networks are grouped into small densely connected subnets (clusters). It's necessary only a reduced number of connections to connect two links within the network. Reference is made to the idea of psychologist Stanley Milgram who, in the 1960s, demonstrated that any two individuals were just a few degrees apart (on average, six people would already be sufficient to establish a link between the two randomly chosen persons);

2) *Scale-free networks*: Their topology does not follow a linear scale and the number of links follows a power law distribution, unlike a normal distribution (Gaussian or "Bell curve"). The "Barabási – Albert Model" consists of connecting two links detected by chance through a path of "big links" or hubs, which concentrate a large number of links. Barabási makes a comparison of the US highway network (as a random network) where major cities are linked by the same number of highways (would be correlated to a Bell curve); to the air transport network that has hubs, which corresponds

18 David Byrne, *Complexity Theory and Social Sciences, An Introduction*, London, New York, Routledge, 1998, p.19.
19 Benjamim Loveluck, *Networks, Freedoms, and Control: A Political Genealogy of the Internet*, Petrópolis, RJ, Vozes, 2018, p. 198.
20 *Ibid*., p. 199.

to dense traffic (correlated to a power law distribution). These complex networks are those formed by the physical internet network, web hyperlinks, scientific literature citation networks, and some social networks;

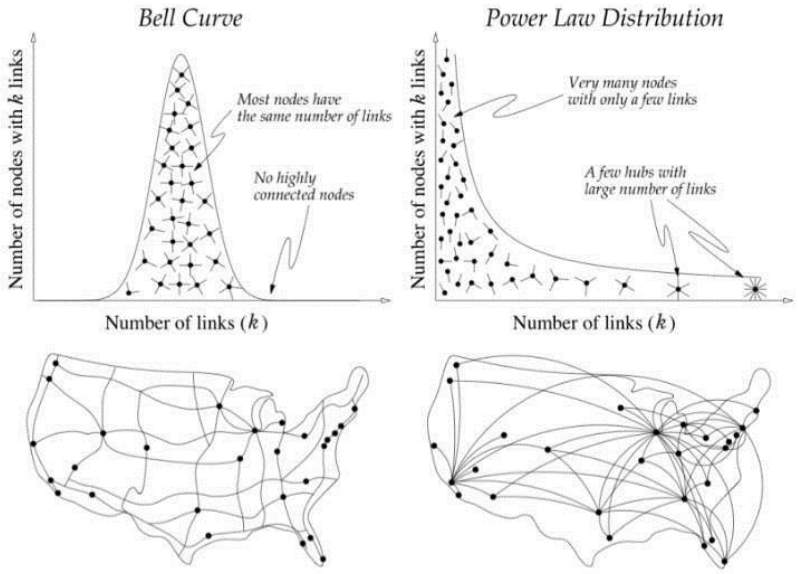

Figure 1: Random network and non-scaled network[21]

3) *Promote viral spread*: What happens is that within non-scaled networks, hubs promote infections in a sufficient number of people for the spread and circulation of the "epidemic". The form of the network that works in a distribution of a power law is enough to guarantee the spread and persistence of infections, which facilitates the diffusion process, that is, it depends on its architecture and not on the nature of the content in circulation.

This whole structure facilitates the phenomenon of social contagion in complex networks, which has the power to potentially bring about political and social changes

21 Albert-László, Linked, *The New Science of Networks*, Cambridge, MA, Perseus, 2002, p. 71.

and consequences in a given society or even in a global society by promoting viral spread.

We can also conclude that if viral spread depends on the infection of a sufficient number of people to promote the spread and circulation of the epidemic, this can be added to the tactic offered by the botnet tool, which exponentially increases the potentiality of the attack.

The centrality of hubs is a facilitator of the spread of infection and a generator of "epidemics", and its finding in complex networks allows to associate with the phenomena of social contagion on a large scale and may even raise adherence movements in political campaigns[22].

2.6. Advertisement oriented

This is a model based on digital advertising based on sensational and viral content. Through algorithmic decision making, agency-operated networks ensure real-time ad serving, facilitating the manipulation of the emotional part of users who are subject to misinformation.

The content may be sensational, but its viral spread is much more due to the network architecture when used in a distribution of a power law.

2.7. Facilitated by technology

Through automated services (referred to as "bots") they artificially extend the spread of misinformation. These mechanics can be facilitated by mock profiles (fake accounts) where no real user profiles are present, and which can be orchestrated on a large scale (referred to as "troll factory").

22 Benjamim Loveluck, *ob.cit.*, p. 203.

The new technology used by botnet attackers is an infected computers function in an automatic way to trigger performance without attackers immediate involvement. This kind of attack uses a control at a distance through the infected computer and botnet malware for the attackers[23].

It is important to know that botnet has a life cycle of five steps: initial infection, secondary infection, connection, malicious command and control, update and maintenance (Feily et al., 2009). The creation of a botnet starts from already known vulnerabilities on a victim system[24].

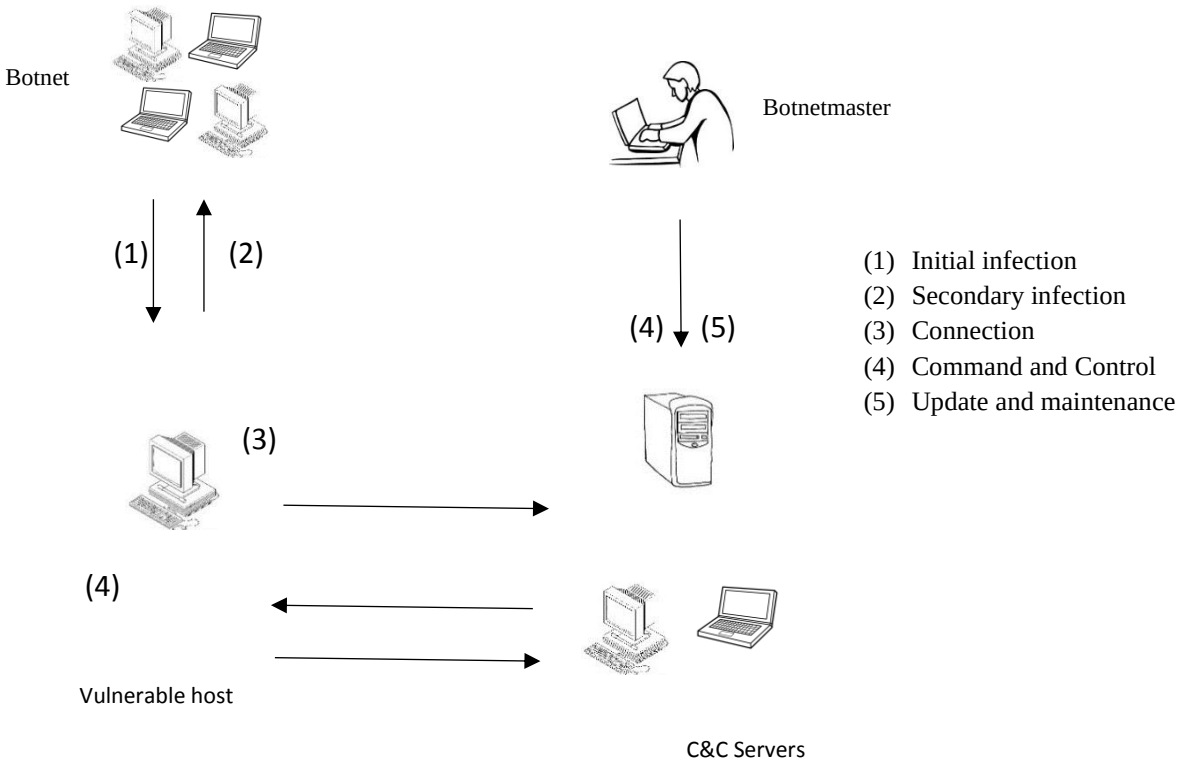

Figure 2: A "Typical Botnet Life-Cycle"[25]

23 Kishor Sarkar, *Cyber Security Botnet Attacks: Procedures and Methods*, Sarkar publication, 2018, p.12.
24 *Ibid.*, p. 16.
25 Maryam Feily; Alireza Shahrestani; Sureswaran Ramadass, *A Survey of Botnet and Botnet Detection, Impact Researsh Team*, Universiti Sains Malaysia (USM), 2009, p.269.

(1) *Initial infection*: This is a critical phase, when the Botmaster tries to exploit a known computer operating system's vulnerability to infect the user's machine[26]. During this phase, the attacker uses the scanning techniques for any known vulnerabilities, and infects victim machines through different exploitation methods. The spreading mechanism includes several infection strategies already used in worms, viruses and social engineering[27].

(2) *Secondary injection*: This phase starts by executing the dropper script code in the infected machine, by downloading the Bot binary from a specific Internet server using a File Transfer Protocol (FTP), HTTP, or Peer-to-Peer (P2P), and then setting up a newer Bot code on the victim's machine. The infected hosts execute a script known as shell-code. "The shell-code fetches the image of the actual bot binary from the specific location via FTP, HTTP, or P2P". The infected machine turns into a zombie (Bot)[28]. The bot application starts automatically each time when the zombie is rebooted[29].

(3) *Connection:* A new bot establishes a command and control (C&C) channel to communicate with the control server. "Upon the establishment of C&C channel, the zombie becomes a part of attacker's botnet army"[30]. Bots, remotely, controlled by a bot master, can conduct various malicious activities such as exploiting other machines, commencing DDoS attacks, and so on[31].

(4) *Command and Control:* The C&C channel is a kind of network protocol to communicate between a bot and a server controlled by an attacker. Moreover, the commands received through C&C channel can be

26 *Ibid.*
27 Kishor Sarkar, *ob.cit.*, p. 16.
28 Feily et al., *ob.cit.*, p. 269.
29 Kishor Sarkar, *ob.cit.*, p.16.
30 Feily et al., *ob.cit.*, p. 269.
31 Kishor Sarkar, *ob.cit.*, p.16

executed autonomously and automatically without the end-user's consent[32]. "The botmaster uses the C&C channel to disseminate commands to his bot army. Bot programs receive and execute commands sent by botmaster. The C&C channel enables the botmaster to remotely control the action of large number of bots to conduct various illicit activities"[33].

(5) *Update and maintenance*: The Botmaster may to add a new function to enhance the Botnets future attacks or to improve the evasion methods. The IP address of a new C&C server can be updated to keep it working and thus then prevent it from being blocked due to the evolution of Botnet detection techniques. "This process is called server migration and it is very useful for botmasters to keep their botnet alive"[34].

32 *Ibid.*, p.13.
33 Feily et al., *ob.cit.*, p. 269.
34 *Ibid.*

3. THE MANIPULATION OF PUBLIC OPINION IN THE CONTEXT OF FOREIGN POLICY

The use of social networks as a means of manipulating the formation of public opinion in the context of a foreign state must be viewed from the perspective of public international law.

Acts of espionage or cyber exploitation are usual forms of interference in the domestic politics of a foreign state. They are recognized as cyber actions that fall below the level of force use or non-kinetic activities. The purpose of cyber exploitation is to unauthorized access to information without affecting system functionality in order to gain clandestine advantage, so that the user does not notice any changes to the system or network. Unauthorized access to computers is made by tools called trapdoors or sniffers that are particularly useful for conducting such operations[35].

Cyber espionage, recognized as a form of cyber exploitation, presupposes the confidentiality of the IT system or the control of foreign intelligence services, and is aimed at gaining some advantage in accordance with secret interests. The interest of controlling the public opinion of a foreign state through the use of cyber exploitation tools can be considered as IO (information operations), which is the use of information technology to achieve government goals[36].

According to the Tallinn Manual I, State liability arising from an act of cyber espionage is not a matter of international law, exceptionally in the case of violation of specific international prohibitions as in the case of diplomatic communications[37]. These international bans are urged to understand acts that tend to provoke domestic state intervention, as it is not in the sole interest of collecting information from an adversary.

35 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, United Kingdom, Oxford University Press, 2014, p. 17.
36 Torsten Stein;Thilo Marauhn, *Völkerrechtliche Aspekte von Informationsoperationen*, Zaö RV 2000, 1, p. 1. Available at: https://beck-online.beck.de/Bcid/Y-300-Z-ZAOERV-B-2000-S-1-N-1 (last time accessed 03/28/2019).
37 Tallinn Manual I, Rule 6 (a).

It should be remembered, however, that traditional espionage alone can be prosecuted under the national law of the adversary state affected, but under due process of law and under the protection of the International Law of the Human Person[38].

3.1. "Hybrid Threats"

"Hybrid threats" consist of activities designed to undermine a country's democratic values and fundamental freedoms by exploiting its vulnerabilities. To this end, disinformation campaigns use the media in order to control political narratives[39] for the manipulation of public opinion.

It is the obligation of a state not to intervene directly or indirectly in domestic matters of a foreign state. According to the Declaration on Enhancing the Effectiveness of the Principle of Abstention of Threat or Use of Force in International Relations, "States are required not to intervene directly or indirectly, for any reason, in the internal or external affairs of any other State"; as well as, it is the duty of states "to abstain from their relations of armed, political, economic or any other form of coercion against the political independence or territorial integrity of any state"; and "the inalienable right of every state to choose its political, economic, social and cultural system without interference from any other state" and the "inalienable right of every state to choose its economic, social and cultural political system without interference from any other state"[40].

Regardless of the active subject who uses these forms of online manipulation, these are acts that hinder the free expression of the will of a collective of people. Any result that occurs in this political context is due to a vice of will to the detriment of its free expression given the intention of misleading an entire national electorate. These

38 John F. Murphy, *Cyber War and International Law: Does the International Legal Process Threat to U.S. Vital Interests?* International Law Studies, 89 Int'l L. Stud. 309, 2013, p. 17. Available at: www.westlaw.com (last time accessed 10/16/2018).
39 Ana Maria Guerra Martins, *The Contemporary Challenges to European Union External Action*, Coimbra, Almedina, 2018, p. 407.
40 UN General Assembly, 42 Session Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Force in International Relations, 18 November 1987 (A /42/766), ANNEX, p. 288. Available at: https://undocs.org/sp/A/RES/42/22 (last time accessed 09/15/2019).

techniques have an incisive power to manipulate public opinion and if external influence is proven, they also violate the principle of nonintervention, political independence and the right to internal self-determination.

The right to internal self-determination referred to is the right to the political, social, economic and cultural development of the people within their own existing state[41].

Cyber operations aimed at achieving the objectives of internal affairs of another state, such as the manipulation of political elections, are acts that violate national sovereignty, subject to the principle of non-state intervention. Even if such an act is considered below the level of 'use of force' provided for in the UN Convention, according to the International Court of Justice, intervention is considered as a 'manifestation of a policy of force' which in the past, "Gave rise to the most serious abuses" and emphasizes that it has no place in international law[42].

Thus, it should be emphasized that a state cannot use technological vulnerabilities to generate internal crises and hinder its free political, economic and administrative development. Given this framework of destabilization of national security and defense, as well as to ensure the maintenance of the law and order, the responsibility of the States is due[43].

Moreover, according to the Universal Declaration on Information and Democracy, which establishes democratic guarantees in the global space of communication and information, with regard to the right to information, "having reliable information is

41 See Vienna Declaration and Program of Action, World Conference on Human Rights, Vienna, 14-25 June 1993, p. 3: "All peoples have the right to self-determination. By virtue of this right, they freely choose their political status and freely pursue their economic, social and cultural development". Available:https://www.oas.org/dil/port/1993%20Declaration%20and%20Program%20of%20Action%20adopted%20by%20Conference% 20World% 20of% 20Vienne% 20About% 20Human% 20in% 20June% 20of% 201 993.pdf (last time accessed 5/17/2019).
42 ICJ, International Court of Justice, Corfu Channel (United Kingdom v. Albania), Merits, Judgment, 9 April 1949, ICJ Reports 1949, p. 35. Available at: https://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-BI.pdf, (last time accessed 7/20/2019).
43 Ana Maria Guerra, *ob. cit.*, p. 407.

essential for exercise freedom of opinion, so that other human rights and all democratic practices are respected, including deliberation, elections, decision-making and accountability. The integrity of the democratic process is compromised when the information that may influence it is manipulated. (...) A commitment to the free pursuit of truth, the accuracy of the facts and the principle of "doing no harm" is necessary to preserve the integrity of the information. Disseminating misleading or incorrect information or covering up information that should be disclosed may impair people's ability to understand what is happening in their environment and the development of their skills"[44].

44 Universal Declaration on Information and Democracy promoted by Reporters Without Borders (RSF). Available at: https://rsf.org/es/el-espacio-global-de-la-comunicacion-y-la-informacion-un-bien-comun-de-humanidad (last time accessed 12/27/2019).

4. FINAL CONSIDERATIONS

Through this multidisciplinary report, it was possible to understand the techniques used in the use of social networks in order to manipulate public opinion. By understanding the forms of technological control in the use of botnets and the vulnerabilities presented that guarantee this intrusion, it is possible to analyze that there are harmful effects for which justice cannot abstain.

The very complexity characterized in social networks, in which phenomena use nonlinear mathematical models, which cause an evolution without direct correspondence to the behaviors of individual entities but described in terms of probability. A study that requires a specialty focused on "Network Science". The cause of the viral spread linked to the architecture of non-scaled networks, which looks more like the air transport network, mainly because the centrality of hubs, which works in a distribution of a power law, generating “epidemics”, assume a potential large-scale social contagion effect and may even lead to movements of adherence to political campaigns.

All this is taken into account when there is a concern to keep the democratic regime out of external threats. In accordance with the norms and principles of international law, the State has a duty not to intervene in the internal affairs of other States.

The manipulation of public opinion is also a matter of domestic state policy, when various internal interests linked to political parties and social movements are at stake. For this, some legal analyzes and notes were taken that take into account rights and freedoms, the optional use of these rights for personalities of the political public, and the abuse of these rights, among other forms of civil and constitutional provision.

It has been seen that manipulation of public opinion can pervade the internal interests of state political parties for an external threat of the national sovereignty. However, when it comes to information at home, care must be taken with the principles surrounding freedom of expression in order to ensure the Democratic Rule of Law. In contrast to this principle is online misinformation, which undermines the structural system of a society by endangering the protection of trust and the free will of voters in a democratic state.

Both, internally and externally, there is legal support for fundamental rights that ensure the Democratic Rule of Law. To this end, the abuse of law as a cause of civil liability is highlighted, as are the ways of ensuring the maintenance of competition and pluralism of information services, as well as the principle of equal opportunities and the treatment of various candidatures in election campaigns. In the context of state foreign policy, the State must protect itself against hybrid threats, and compliance with the principle of non-state intervention and the right to internal self-determination gain special relevance in this regard.