CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 01 janeiro 2016 | Grátis

# DIREITO:

## A PENSAR TECNOLOGICAMENTE

**cyber espaço**
novas fronteiras

**cyber ataques**
algumas estratégias de mitigação

**cyber segurança**
preocupação global

**outros**
- direito constitucional do Inimigo
- obscurantismo
- DOTMLPI-I
- ENISA


**EDIÇÃO N.º I – JANEIRO DE 2016**

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


CYBERLAW
by CIJIC

**EDITOR:** NUNO TEIXEIRA CASTRO

**SUPORTE EDITORIAL:** EUGÉNIO ALVES DA SILVA e GONÇALO BAPTISTA DE SOUSA

**DESIGN & GRAFISMO:** ISABEL BAPTISTA e ANTÓNIO OLIVEIRA

**DIRECTOR DO CIJIC:** EDUARDO VERA-CRUZ PINTO



**CIJIC:** CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

**ISSN 2183-7295**

## MENSAGEM DO DIRETOR DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERPEAÇO - CIJIC:

***«A Revista científica «Cyberlaw by CIJIC»: um longo, ousado e consolidado caminho de inovação editorial»***

Breves palavras para apresentar o primeiro número da Revista sobre o Direito no e do Ciberespaço do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, a «Cyberlaw by CIJIC». Breves mas intensas de empenho pessoal e de orgulho institucional por ver concretizado - com competência, qualidade e excelência – um dos objetivos principais do Centro. Tudo começou com uma proposta que fiz, há cerca de cinco anos, enquanto Diretor da Faculdade de Direito de Lisboa, ao Presidente do Instituto Superior Técnico, Prof. Doutor Eng. Arlindo Oliveira e ao Diretor da Escola Naval, Contra Almirante Seabra de Melo, para iniciarmos um projeto conjunto de um Centro de investigação e um conjunto de cursos pós-graduados como embriões de um mestrado multidisciplinar na área da cibersegurança. O caminho fez-se, desde aí, mostrando como organizações centenárias, ancoradas em fortes tradições institucionais, são as que melhor se encontram preparadas para processos de inovação temática e investigativa com efeitos de renovação humana, científica, pedagógica, didática e editorial. Com a colaboração do Gabinete Nacional de Segurança e o apoio do seu Diretor-Geral, o Almirante Torres Sobral, foi possível aos três fundadores do Centro (agora com o Contra Almirante Edgar Bastos Ribeiro como Diretor da Escola Naval) iniciarem um novo

trilho interdisciplinar na investigação, formação e divulgação do Direito no e do Ciberespaço em Portugal.

Esta Revista só foi, no entanto, possível pelo entusiasmo e empenho de uma geração saída maioritariamente do corpo discente do Mestrado em Segurança da Informação e Direito do Ciberespaço (MSIDC). O principal impulsionador e, agora editor, da Revista, o Nuno Teixeira de Castro, é credor de um agradecimento especial por ter concretizado, na forma que agora está, a ideia da «Cyberlaw by CIJIC». Um agradecimento que se estende ao Gonçalo Baptista de Sousa, ao Eugénio Alves Silva, à Professora Raquel Alexandra Brízida Castro, à Professora Sofia de Vasconcelos Casimiro, à Isabel Batista e ao António Oliveira. Aos membros da Comissão Científica, aos autores deste primeiro número, aos colaboradores e amigos anónimos, um agradecimento pela disponibilidade e entusiasmo de todas as horas.

A Direção do CIJIC conta com a equipa da Revista para manter a periodicidade de uma publicação que, além de juntar os especialistas mais reputados nestas áreas como autores, de manter uma informação atualizada e interessante sobre o direito do ciberespaço, de difundir conhecimentos e dar a conhecer personalidades do ciberdireito, servirá como montra da investigação feita no âmbito dos mestrados, doutoramentos e projetos de investigação específicos que se desenvolvem no âmbito do CIJIC. Parabéns à Direção da Revista e ao seu editor, o Nuno Teixeira Castro, com votos de uma longa vida editorial

**Eduardo Vera-Cruz Pinto**

## NOTAS DO EDITOR:

Ano de 2016. O ciberespaço assume-se, de forma quase inquestionável, como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação, de transmissão e de informação ao serviço do Homem. A sociedade, inebriada por esta *revolução tecnológica*, habitua-se, numa *quase-metamorfose híbrida*, a esta tecno-dependência. Mas, será que compreendemos, minimamente, os tempos *revolucionários* em que vivemos?

A «Cyberlaw by CIJIC», integrada ela própria nesta e por esta dinâmica homem-tecnologia, procurará desmistificar certos *topoi*, pertinentes, intrincados, procurando preencher, com uma abordagem multidisciplinar, uma natural preocupação humana refletida na temática da «Cibersegurança».

O Homem é o ponto de partida e ponto de destino da Cibersegurança. Os ciber-instrumentos deverão guiar-se pelo respeito pelos direitos fundamentais, em especial as várias dimensões do direito à autodeterminação informacional, radicado no princípio da dignidade da pessoa humana. Ademais, porque o Homem é um ser livre em toda a sua essência, procuraremos desvelar alguns paradigmas, projetando a construção evolutiva, *simbiótica*, de um pensamento jurídico e tecnológico, capaz de conjugar a essência da «Cibersegurança» com algumas das naturais liberdades humanas. A tarefa é árdua. O caminho, longo. A vontade, imensa. Façamo-nos ao trilho…

## AGRADECIMENTOS:

Vivemos tempos exigentes. Exigentes quanto às relações humanas. Por vezes, deparamo-nos ante a tentação de dúvida quanto a esse valor inalienável que é o valor da dignidade humana. Jamais. É o acreditar no valor da dignidade humana que nos demanda.

Pelo valor, inestimável, das relações humanas, torna-se-nos imperioso relevar a imensa vontade, cooperação e amizade de todos os que tornaram a edição da «Cyberlaw by CIJIC» possível.

Neste sentido, sem relevo específico quanto à preferência, devo um distinto agradecimento aos Professores Francisco Muñoz Conde e Alfonso Galan Muñoz.

É igualmente devido, primeiro, ao Professor Néstor Pedro Sagués. Sem olvidar, obviamente, os Professores Óscar R. Puccinelli e Pablo A. Palazzi.

Um cumprimento e um agradecimento especial ao Professor Mark Tushnet.

À ENISA. Primeiro, ao seu Administrador, Paulo Empadinhas e à Sofia Andrioti. Mas também ao seu Diretor-executivo, Professor Udo Helmbrecht. Desde o primeiro contato demonstraram toda a sua vontade generosa em ajudar nesta tarefa.

Genuínamente, nada disto teria sido possível, afinal, sem a Isabel Batista, o António Oliveira, o Eugénio Alves da Silva, o Gonçalo Batista de Sousa, o Raimundo Neto e o Miguel Ferreira e Silva. E, claro, os Professores, Sofia de Vasconcelos Casimiro, Manuel David Masseno, Alexandre Sousa Pinheiro, Carlos Caleiro e Fernando Ribeiro Correia.

Finalmente, um reconhecimento óbvio, mas inteiramente merecido, à Professora Raquel Alexandra Brízida Castro. E ao meu Mestre, o Professor Eduardo Vera-Cruz Pinto, que muito me honra por me aceitar como seu Mestrando.

A todos, gratidão imensa. Impagável.

Nuno Teixeira Castro

CYBERLAW by CIJIC

**ÍNDICE:**

CYBERLAW by CIJIC

# INTERVIEW WITH ENISA'S EXECUTIVE-DIRECTOR PROFESSOR UDO HELMBRECHT

# ENTREVISTA COM O DIRETOR-EXECUTIVO DA ENISA : PROFESSOR UDO HELMBRECHT


**Professor *Udo Helmbrecht***

## ABSTRACT

*ENISA is a well-established agency known by its relevant stakeholders. Via the so called Art. 14 procedure of our regulation, ENISA recommendations are quoted, and it is explicitly mentioned in EU sector directives.*

*Cyber security is a key priority for most EU Member States. However the approach each country takes on the topic is diverse and according to their national requirements. Harmonized implementation of legislation creates a level playing field and makes it easier for asset owners and users to operate across different EU countries. ENISA plays a key role in encouraging the harmonised implementation of security requirements.*

**Keywords:** ENISA; Cybersecurity, ICT; Privacy Enhancing Technologies; Trust;

# Interview Questions

«*Prof. Udo Helmbrecht is the Executive Director of ENISA since the 16th of October 2009. Prior to this, he was the President of the German Federal Office for Information Security, BSI, for six years, between 2003-2009.*[1]»

First of all, let me thank you for the immediate availability shown on helping us with the construction of the Cyber Law Research Centre at the Lisbon Law School.

This interview is intended to give the tone, the right one, for the beginning of our scientific research at the Centre.

Beyond this minor introductory part, I've picked one *résumé* from the ENISA's webpage. Your CV available at https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director, almost *talks* for itself.

Let's start with a *slight* provocation,

1) Who is Udo Helmbrecht?

Looking to your motivation letter - to your visions - prior to your nomination, in 2009 (*also available at ENISA's website*), to last year's full trust vote, when the ENISA Management Board decided to extend your term of office for more five years, do you feel like the right man at the right track?

*Of course am I the right man at the right track; otherwise I would not do this job.*

2) And about ENISA, this laborious task of its implementation, winding its way slowly since 2004, after 10(ten years) of hard work… what's ENISA in the present moment?

*ENISA is a well-established agency known by its relevant stakeholders. Our recommendations are quoted, we are explicitly mentioned in sector directives like in*

1Text available at ENISA: https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director.

*the telecommunication package, eIDAS directive or the just negotiated NIS directive. Commission and Member States ask for our support, e.g. like CERT trainings, via the so called Art. 14 procedure of our regulation.*

3) Regarding Cyber Law, one of the countless challenges facing the security of information and networks still consists in the fact that most of the Member States have their own interpretation of the legal framework that should be established at national and European level for that purpose. Even now, after facing the recent Digital Single Market's initiatives announcement, many of the Member States still insist on maintaining different priorities and taking opposite approaches. Moreover, the fact that the legal landscape in that area is so fragmented, since it touches so many topics (and controversial topics), such as privacy, criminal law, trade secrets and national security, makes it difficult to find a common ground.

Do you think that one major step towards a joint European cybersecurity commitment is a unified vision of the legal framework that should be established at an European level? Shouldn't it be the priority? If you agree that it should, what would be, from your point of view, the best way to keep Member States on the same page, in what concerns cybersecurity?

*Cyber security is a key priority for most EU Member States, 23 countries have already adopted a national cyber security strategy - the key policy document providing the actions to take place to enhance cyber security in a national level. However the approach each country takes on the topic is diverse and according to their national requirements, i.e. some countries have developed specific action plans drawn by legislation, some others have created working groups per critical sector to focus on tackling the cyber security issues, others include cyber security in the mandate of the body responsible of national cyber security, etc.. These approaches depend on the national assets that need to be protected and on the culture of the country.*

*Harmonized implementation of legislation creates a level playing field and makes it easier for asset owners and users to operate across different EU countries. ENISA plays a key role in encouraging the harmonised implementation of security*

*requirements by stimulating the dialogue amongst various stakeholders across Europe and maintaining a number of technical experts' communities. The article 13a (security and integrity in electronic communication networks, Directive 2002/21/EC) and NCSS (National Cyber Security Strategies) working groups are typical examples of such communities maintained by ENISA.*

4) Last March, at «*Technologist*», again, you've noticed that «*We're missing a vertical approach to escalating decision-making – taking the problem from a technical level up to a politic level*». You emphasized the problem of not having one «*well-established escalation procedure*[2]». Do you see ENISA filling that gap, setting out an escalation procedure and becoming, in the near future, the Network and Information Security European Regulator?

*It is the approach of ENISA to situate its work in between the high level policy initiatives and the low level technical work supporting the Member States in implementing the provisions of EU policy initiatives. Having said this, the decision on whether an EU European Regulator on Information Security is required is entirely up to the National Authorities.*

5) The nature of the Internet and other computer networks gets in the way of dealing with cybersecurity matters. As you noticed before, «*When you talk today about the Internet, it is the "Wild West*[3]». Does that anarchy, that still characterises the Internet and other computer networks – and that is one of its key attractive features – should be limited or even put to an end by an appropriate control?

*As you rightly note this 'anarchy' that characterises the Internet is one of its key attractive features.*

*Perhaps the best answer to this question is that the 'anarchy' should be limited where necessary in order to protect citizens and provide an environment from which*

2 See text available at http://www.technologist.eu/europes-cyberdefence/ .
3 Text available at http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431.

*all communities can benefit. The challenge for the policy maker and an Agency like ENISA is to come up with the best balance in terms of appropriate controls. I do admit that this is not an easy task. For example, you may recall the recent discussion at Members States as well as the European Parliament on allowing or not the use of encryption technologies for public communications.*

6) It's no overstatement to say that much of the growth and richness of the *Internet* itself and other computer networks and information technologies thrived through that singular human feature: «Confidence»(*Trust*).

Latterly, with all those ablaze «*mass surveillance*» cases *affecting* European citizens; with all those cyberatacks that have been reported in major European organisations, with the disclosure of sensitive personal data of millions of customers; and recently, with the CJEU *striking down*, on October 6th 2015, the Safe Harbour data transfer agreement (on the grounds of insufficient guarantees that the companies would comply with the European data protection rules), do you believe that we should continue to "trust in and through" *this necessary and additive technology*? And if we do, is there any way to *counteract* attacks on confidence? Are we still able to entice the trust of 500 million consumers for the Digital Single Market (DSM)?

*In my view the pervasiveness and richness of the content of Internet contributed to its amazing growth. Having said this I agree with you that especially due to recent developments, issues such as Confidence and Trust are becoming of great importance. ENISA is convinced that the area of 'online trust and confidence' is an opportunity for European ICT industry!!! Moreover, the pervasive nature of the Internet and its services forces both industry and policy and policy makers to do their outmost in order to ensure that confidence on the network and its services is set at high levels.*

7) Again, «*Trust*». Is there any way we could establish a based trust-system, from private to public partners, if the temptation of one «mandatory reporting duty» is on the edge of the planned European cybersecurity legislation?

Assuming «Trust» as the kernel of the business relationship (let's think, for instance, Finance, Bank, Stock-exchange, Health, along with many other sectors), isn't a «mandatory report duty» a kind of *assault* to that kernel (private or even public)? As we know, many of the organizations don't disclose the fact that they have been attacked, serving to lessen the overall perception of risk, so, isn't that «mandatory report» seen as a kind of disincentive to the higher level of resilience intended to create?

*An example for trust building that works well and also scales for larger groups is set by operational communities, especially the CSIRTs. This mechanism makes use of a "trusted introducer" process, where capabilities and other issues are checked by other teams. In more sensitive environments, where sensitive information needs to be shared, there are vouching mechanisms in place, where for example at least two other already introduced teams need to vouch for a newcomer. This kind of trust building works quite well in everyday business, and could be adopted in other environments as well.*

8) Lets take the singular case of Portugal. Most of its business structure depends on SME's (small and medium enterprises) which operate with very strict budgets. Most of the times, these organizations, eventually yield its cyberprotection to those off-the-shelf programs. Moreover, we see that *Security, [it] is being added on carelessly, and, worse, afterthought rather than a design priority*, as William Saito[4] unerringly noticed. This is normally due to budget constraints.

We need to think broad, and start looking for ways of incentive. The cybersecurity task is immense. Why not start by discussing tax incentives to those SME's organizations when implementing cybersecurity measures?

*The fact that higher security comes at an increasing cost is becoming more and more obvious to many decision-makers; therefore tolerance of some level of insecurity is necessary for economic reasons. From an economic perspective, the key*

4 See text available at http://www.huffingtonpost.com/william-saito/why-internet-security-mat_b_6527104.html.

*question is whether the costs and benefits perceived by market players are aligned with the social costs and benefits of an activity.*

*As the Internet itself can be seen as a public good, it is likely that ICT security shows public good characteristics as well. The consumption of public goods is not affected by rivalries in the domain or by excluding interested parties from involvement. Total security is neither achievable nor desirable. Hence, each actor will carefully make a trade-off between costs and benefits associated with ICT security investments. Some level of ICT security is, however, a prerequisite for the globally interconnected economy to work. This is also true for the Internet's services to function. Basically a secure ICT infrastructure resembles a functioning banking sector, which is essential for doing business. Malevolent or careless users can cause harm to other users. Further incentives to invest in security are often misaligned as parties do not have to bear the costs of their behaviour entirely, if at all.*

*Due to these effects, ICT security can be regarded as a public good. If the existence of a public good is desired by society, its provision has to be safeguarded by means of regulatory intervention from some superseding level of governance. To these means pertain, e.g. legislation (such as liability laws), taxes, requirements, bans and rules and quotas, often designed to fight external effects.*

9) Much of ENISA's software resources are based upon open source products. In a different way, critical infrastructures and Industrial Control Systems (ICS) products are mostly based on standard embedded systems platforms which often use commercial *off-the-shelf* software. The reduction of costs and improved ease of use can be taking place at the cost of cybersecurity and this might open the door to computer network-based attacks. Is it possible to create a capability that allows us to test and evaluate our software? Are we able to rate the security of our software? And what should be the form of control when we deal with the continuous and *gushing* migration to cloud computing, transferring to third parties the decision on the software to use?

*Although the industry is moving in the direction of developing security through the use of standards, recommendations and guidelines established by certification*

*bodies and/or public–private initiatives, there are still several areas where there is room for improvement: poor software development practices, fast testing and objective measuring, official security certifications, current status of new security standards development, etc. All these needs could be addressed by a common test bed framework, which allows for testing ICT, processes and components against specific security requirements.*

*Security testing certification needs a holistic and human-centric approach and as a result security cannot be rated with absolute numbers. Security-certified ICT systems and components need to be operated by competent organisations and personnel. Security testing and certifications of components and organisations and key personnel set the minimum accepted level and can be further elaborated with a "Competence Bonus" to motivate incident reporting and problem solving.*

10) Looking at the cybersecurity chain, we recognize that its weakest link is the «human factor». From social engineering, to lack of skills or knowledge, to unsafe behaviours, all of us concede that it is far difficult to modify existing routine actions. And all the cyberattackers know it also.

Peter Warren Singer have one interesting proposal on «*how to save the Internet*[5]». He compares the effect of CDC (Control Disease Centre) in 1940/50's for the human physical health with a similar approach to the informational and cyberhealth in the present time. Do you believe that we might have one chance to build our cybersecurity centres' based on that Singers' singular proposal[6]?

*Your example has similarities to the approach followed by ENISA namely to situate its work in between the high level policy initiatives and the low level technical work supporting the Member States in implementing the provisions of EU policy*

5 See article available at http://www.wired.com/2014/08/save-the-net-peter-singer/

6 Lets, for instance, assume that the CDC, serves as a *fusion centre*, where the public and private poles can merge their interests: on the one hand, the State accepts its *natural* obligation of (cyber)scientific research (since the cost associated with scientific research is of high provision) and its further dissemination of knowledge; and, on the other hand, the private sector, noting the independence and impartiality of the centre itself, walks toward it in a voluntary basis in a lightly way, devoid of that burden of the mandatory report. Could this help on creating and promoting the much-vaunted and needed cyberawareness?

*initiatives. Having said this, such decisions on the exact role of National and/or a European cyber security centre rests entirely up to the EU Member States.*

11) In the past, in 2013[7], at *Deutsche Welle*, when asked about all the possibilities, technical or legal, linked to the «*right to be forgotten*», you've noticed that «*Ultimately, it comes down to the realization that the Internet never forgets!*».

Viktor Mayer-Schonberger, for instance, seems to have one, even *hypothechnical*, solution to this particular subject. Why not the use of «*Expiry dates*[8]» (maybe, digital time stamps) attached to our digital footprint? Would you subscribe that solution?

*The idea of 'ephemeral messaging' or simpler 'disappearing messages' has been investigated by researchers as a possible solution towards establishing trust online. At this moment in time we are still at a phase in Europe where we recognise the need to deploy Privacy Enhancing Technologies (PETS) in order to safeguard EU citizen privacy as well as the position of EU industry. This is also reflected in the General Data Protection Review.*

*The next challenge for Europe for the coming years would be to translate this into a set of technologies that when combined could enhance online trust. Which are these technologies is still not clear. A number of candidates exist like the one you describe. It is clear however that one technology will not suffice and a combination of techniques would be required. ENISA has been working for a number of year in assessing the maturity and potential of privacy enhancing technologies especially in view of the upcoming General Data Protection Review. In this respect, I believe that we are very well positioned in providing support to Member States in implementing the provisions General Data Protection Review.*

7 See article available at http://www.dw.com/en/the-internet-never-forgets/a-16996942.
8 At the *NJ.com*, in 2009, *Mayer-Schonberger* pointed out the following: «*Expiry dates is just a piece of meta information that we would enter when we store a file or a document in our computer and we would be prompted by our computer not just to enter the file name and the location where we want to store it, but also a expiry date. When that date is reached our computer would automatically purge that file or that image from our system. Of course, we would be perfectly free to change the expiry date anytime we want if we change our mind if we think we want to preserve an image for longer or delete it much faster*» (available at http://blog.nj.com/njv_kelly_heyboer/2009/11/will_the_internet_let_us_forge.html).

12) Finally, how do you envision the development of research centres for cyber and related matters? What role do you think they could play in the near future and, possibly, in connection with ENISA?

We consider research in the cyber security area as very important, where we can we offer our support for institutions and researchers, but sadly we can do this only on a best effort basis, due to our small size and lack of resources. So as much as we consider this important, we cannot engage in research ourselves. But we are open for formal and informal agreements, or maybe staff exchange in limited, well-chosen cases.

13) Do you have some final words to our Cyber Law Research Centre[9], Professor Udo?

*I would like to welcome your initiative and your Cyber Law Research Centre that are the kind of initiatives that we can bring an important added value for our society. The cyber space is growing and developing so fast and changing the way people and society interact. The impact is not only in business but also in the private life of all of us and the legal challenges are increasing to keep the balance between technology and supported development and fundamental rights. All this in line with the vision that is expressed in the Lisbon Treaty for all Europeans. ENISA will continue to work towards the citizens' through the Member States via Industry, Academia and all other related stakeholders that play a crucial part in the development as your Cyber Law Research Centre. Congratulations for the initiative and for the help on Building a Secure Cyber Space in Europe.*

[9] This interview, conducted by Nuno Teixeira Castro - on behalf of CIJIC - was only possible due to the unsurpassed support of ENISA's staff, namely, Sofia Andrioti and Paulo Empadinhas.

CYBERLAW by CIJIC

# LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS TRATAMIENTOS DESTINADOS A LA PREVENCIÓN, INVESTIGACIÓN Y REPRESIÓN DE DELITOS: HACIA UNA NUEVA ORIENTACIÓN DE LA POLÍTICA CRIMINAL DE LA UNIÓN EUROPEA

# THE PROTECTION OF PERSONAL DATA IN PROCESSINGS INTENDED TO THE PREVENTION, INVESTIGATION AND PUNISHMENT OF CRIMES: IN DIRECTION TO A NEW DIRECTION OF THE EUROPEAN UNION'S CRIMINAL POLICY

**ALFONSO GALAN MUÑOZ** [1]

[1] Profesor Titular de Derecho Penal Universidad Pablo de Olavide de Sevilla/España. Correo electrónico: agalmun@upo.es

Este trabajo se ha realizado en el marco del Proyecto del Ministerio de Ciencia e Innovación I+D+I, titulados "La transmisión de datos personales en la copelación policial y judicial penal en la Unión Europea: el Principio de Disponibilidad" (DER 2011/28282) y del Proyecto Investigación I+D del Ministerio de Economía y Competitividad sobre "Cesión de datos personales entre procesos penales y procedimientos administrativos o tributarios en España y la Unión Europea" (DER2014-56401-P).

**SUMÁRIO: 1. EL LARGO CAMINO DEL DERECHO PENAL EUROPEO Y SU INCIDENCIA EN LA REGULACIÓN DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL; 2. EL PRINCIPIO DE DISPONIBILIDAD COMO REFERENTE INICIAL DE LA POLÍTICA CRIMINAL EUROPEA RELATIVA A LA COOPERACIÓN JUDICIAL Y POLICIAL EN MATERIA INFORMATIVA; 3. UN NUEVO E IMPORTANTE REFERENTE NORMATIVO: EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA CDFUE TRAS LA ENTRADA EN VIGOR DEL TRATADO DE LISBOA; 4. LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA DE 8 DE ABRIL DE 2014 Y SU POSIBLE REPERCUSIÓN EN LA POLÍTICA EUROPEA DE PROTECCIÓN DE DATOS PERSONALES EN MATERIA PENAL; 5. LA UNIÓN EUROPEA ANTE LA ENCRUCIJADA. ¿HACIA UNA NUEVA POLÍTICA CRIMINAL REFERIDA A LOS TRATAMIENTOS DESTINADOS A LA PREVENCIÓN, INVESTIGACIÓN Y PERSECUCIÓN DE DELITOS?; 6. BIBLIOGRAFÍA**

---


**RESUMO**

Este artigo procura analisar as diferentes etapas temporais da política penal estabelecida pela União Europeia relativas ao processamento de dados pessoais usados na prevenção, investigação e punição de crimes, até chegarmos à situação presente. Uma situação em que a União deverá repensar a sua política procurando adoptar uma muito mais incisiva na protecção dos direitos fundamentais das pessoas, em especial no tocante ao direito fundamental à protecção de dados pessoais, isto se pretender responder adequadamente às exigências do novo quadro normativo criado pela adopção e entrada em vigor do Tratado de Lisboa e à interpretação do Tratado que o Tribunal de Justiça Europeu tem vindo a seguir em algumas das suas últimas sentenças.



**Palavras-Chave**: Direitos fundamentais; Dados pessoais; Dados de tráfego; Direito penal europeu; Cooperação policial e judiciária.

## ABSTRACT

This paper analyses the different stages of criminal policy established by the European Union in relation with personal data processing that is used to prevent, investigate and punish crimes, until come to the current situation. The situation in which the Organisation must rethink its policy in order to take one policy much more pointed to protect the fundamental rights of people and, especially, the fundamental right of personal data protection, if it wants answer adequately to the demands of the new normative frame created by the adoption and entry into force of the Treaty of Lisbon and the interpretation of this Treaty that the European Court of Justice has done in some of its last sentences.

**Keywords:** Fundamental rights, personal data, traffic data, European Criminal law, police and judicial cooperation.

## RESUMEN

El presente trabajo analiza las diferentes etapas que ha atravesado la política criminal seguida por la Unión europea en relación con los tratamientos de datos personales utilizados para prevenir, investigar o sancionar delitos, hasta llegar a la situación actual. Una situación en la que dicha institución tendrá que replantearse la mencionada política, adoptando una mucho más orientada a la protección de los derechos fundamentales de las personas y, especialmente, del derecho fundamental a la protección de datos personales, que la ha seguido hasta este momento, si realmente pretende responder, de forma adecuada, a las exigencias que se derivan del nuevo marco normativo que la aprobación y entrada en vigor del Tratado de Lisboa ha venido a establecer y a la interpretación que del mismo ha efectuado el Tribunal Europeo de Justicia en alguna de sus últimas sentencias.

**Palabras claves:** Derechos fundamentales, datos personales, datos de tráfico, Derecho penal europeo, cooperación policial y judicial.

# 1.EL LARGO CAMINO DEL DERECHO PENAL EUROPEO Y SU INCIDENCIA EN LA REGULACIÓN DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Uno de los fenómenos más interesantes y relevantes que se han producido en el Derecho penal de estos últimos años se ha derivado del lento, pero imparable nacimiento de lo que ya podemos considerar como un verdadero Derecho penal europeo.

Parecen ya lejanos los días en los que la doctrina discutía sobre el concreto origen del *ius puniendi* positivo de la Unión europea, cuestionando, por ejemplo, si fue el reconocimiento el principio de asimilación en algunas Sentencias Comunitarias, como la referida al asunto del Maíz Griego, el que supuso la aparición de dicha capacidad normativa[1]; o si fueron, en realidad, las posteriores Sentencias del mismo Tribunal que reconocieron la legitimidad de las instituciones comunitarias, y especialmente las de la Comisión, a la hora de emitir normativa sobre las cuestiones penales en las que dicha regulación resultase necesaria para hacer un uso efectivo y adecuado de las competencias que les correspondían en materia de integración, las que realmente dieron lugar a su nacimiento[2].

Lo cierto es que la UE ha ido creando, a lo largo de los últimos años, una ingente normativa en materia penal, cuya aparición ha dado lugar a que se pongan en tela de

[1] Sentencia del TJCE 28/88, de 2 de septiembre de 1989.

[2] Véase, en especial, lo establecido en la sentencias del TJCE de 13 de septiembre de 2005 y en la de 23 de octubre de 2007. Sobre todo el proceso jurisprudencial que llevó hasta el reconocimiento de dicha capacidad normativa, véase, por ejemplo, lo comentado por FERNÁNDEZ OGALLAR, B. en *El Derecho penal armonizado de la Unión europea.* Ed. Dykinson. Madrid, 2014. p. 183 y ss. Hay que destacar, por otra parte, que mientras algunos autores, como TIEDEMANN, K., hablaban de la existencia de un mero Derecho penal nacional europeizado, precisamente, por entender que, al fin y al cabo, por más que la Unión europea pudiese emitir normativa con contenido penal, la misma no sería vinculante hasta que no fuese transpuesta a cada uno de los ordenamientos jurídicos nacionales de sus Estados miembros por cada uno de sus respectivos paramentos. «EG und EU als Rechtquellen des Strafrechts» en *Festschrift für Claus Roxin.* V Walter Gruyter. Berlín. Nueva York, 2001. p. 1430; otros, como VOGEL, J. señalan, más acertadamente, a nuestro modo de ver, que, dado el carácter vinculante de la normativa comunitaria para los Estados y sus parlamentos y la cada vez más detallada regulación de los contenidos penales sobre la que la misma recaía, la intervención de los parlamentos nacionales terminaba convirtiéndose, en realidad, en una mera salvaguarda formal del principio de legalidad, ya que dichos parlamentos se veían de hecho obligados a acatar y ejecutar las decisiones de política criminal adoptadas desde Bruselas. En «Política criminal y dogmática penal europea», en RP núm. 11, 2003, pp. 143 y 144. En este mismo sentido, SCHÜNEMANN, B. llegó incluso a afirmar que los parlamentos nacionales habían terminado por convertirse en meros «lacayos de Bruselas», en «Fortschritte und Fehltritte in der Strafrechtspflege der EU», en *GA*, 2004. pp. 194 y ss.

juicio, tanto la base competencial sobre la que se ha regulado tal materia, como la más que discutible legitimación democrática que ampararía su emisión; críticas que muy posiblemente hayan sido las que han llevado a que el, por el momento, último gran paso dado en el proceso de construcción de la Unión Europea, el Tratado de Lisboa, suscrito el 13 de diciembre de 2007, haya tratado de afrontar ambos problemas realizando dos grandes aportaciones con respecto a los mismos.

La primera consistió en reconocer, de forma expresa, que la Unión tenía competencias tanto en materia de Derecho penal sustantivo, —materia en la que podrá crear normas mínimas que definan las infracciones penales y sanciones que resulte necesario establecer para desarrollar de forma efectiva las políticas de armonización propias de la Unión (artículo 83.2 TFUE) o las que se refieran a ámbitos criminales dotados de especial gravedad y dimensión transfronteriza, como el terrorismo, la criminalidad organizada, el tráfico de drogas, el blanqueo o la criminalidad informática, entre otros (artículo 83.1 TFUE)—, como en relación a cuestiones de naturaleza procesal penal (artículo 82 TFUE) o incluso en las de pura prevención de delitos (artículo 84 TFUE)[3]. La segunda, por su parte, se derivó del hecho de que el citado Tratado estableciese que todo este proceso de armonización legislativa en materia penal se habría de realizar utilizando el procedimiento normativo ordinario, lo que llevará a que todas las disposiciones que lo desarrollen se tengan que adoptar a través de un proceso de codecisión en el que el Parlamento europeo, único órgano europeo dotado de legitimidad democrática directa, asumirá un papel, tal vez no suficiente, pero sí mucho más relevante que el que hasta ese momento había tenido, en el proceso de creación de dicha normativa[4].

No parece, pese a todo, que éste vaya a ser el último gran paso que se dé en este constante y aparentemente imparable camino hacia el desarrollo de un verdadero y

[3] Precisamente, y a juicio de VOGEL, J. esta última es una de las más evidentes ampliaciones de competencias que la entrada en vigor del Tratado de Lisboa ha traído con consigo a la UE, junto al hecho de que prevea la colaboración entre administraciones no específicamente referidas a la justicia y a las decisiones que se emitan desde estas últimas, por más que no estén referidas a materia penal. En «EU-Arbeitsweisevertrag Artikel 82 Gegenseitige Anerkennung; Angleichung», en *Das Recht der Europäischen Union.* 51 Ergänzungslieferung, V. Becks, München, 2013, Rnd. 66. sobre la cuestionada posibilidad de la existencia de otras bases competenciales de la UE en materia penal, véase, por ejemplo, lo comentado por MAPELLI MARCHENA, C., *El modelo penal de la Unión europea*. Ed. Aranzadi, Cizur Menor, 2014, pp. 160 y ss.

[4] FERNÁNDEZ OGALLAR, B., op. cit. ant., pp. 74, 133 y ss. y 349 y ss.

esperemos que, en un futuro cercano, plenamente legítimo Derecho penal europeo[5], y hacia la paralela implantación una auténtica política criminal europea, que permita, entre otras cosas, que tanto los organismos nacionales, como los europeos responsables de la prevención, persecución y sanción de delitos cuenten con los medios que realmente necesitan para poder ejercer sus competencias, de forma efectiva, en el mundo globalizado y carente de fronteras en el que vivimos[6].

Precisamente, una de las principales herramientas y medios de los que todos estos organismos deben disponer para cumplir con sus funciones, es, sin lugar a dudas, la información. Cuanto más información y de mayor de calidad tengan los agentes responsables de la prevención, la investigación o la represión de delitos, más eficazmente desempeñarán su labor, lo que debería llevar a la UE a crear y establecer los instrumentos materiales y normativos necesarios para permitir que dichos agentes puedan obtener e intercambiar entre sí los datos que necesiten, de la forma más rápida y fiable posible.

Ahora bien, no todo puede reducirse a conseguir la mayor eficacia preventiva y represiva. Si la Unión Europea realmente pretende ser ese espacio único, no solo de Seguridad, sino también de Libertad y Justicia del que habla el artículo 67 su Tratado de Funcionamiento (TFUE), tendrá que tener presente que, junto a la búsqueda de las

[5] Sobre los problemas de legitimidad que enfrenta este Derecho, véase, de forma general, lo comentado por ejemplo, por FERNÁNDEZ OGALLAR, B. en op. cit. ant., pp. 349 y ss. Resulta destacable en este aspecto, que mientras algunos autores como. NIETO MARTÍN, A. se mostraban favorables a considerar que el proceso de codecisión podría cumplir con las exigencias derivadas del principio de legalidad, si garantiza la intervención del Parlamento europeo y dejar margen a los nacionales para determinar la concreta transposición de la normativa europea, en «Posibilidades y límites de la armonización del Derecho penal nacional tras Comisión v. Consejo. (Comentario a la STJCE, asunto C-176/03, de 13-9-2005)». *REDE* núm. 17, 2006. p. 119, mientras que GÓMEZ-JARA DÍEZ, C. afirmaba incluso que el camino emprendido con el establecimiento de dicho proceso, podría tender a crear un Derecho penal europeo de corte federalista, en «Constitución europea y Derecho penal: ¿Hacia un Derecho penal Federal europeo?», en *Derecho penal y política transnacional*, Ed. Alitier, Barcelona, 2005. pp. 168 y ss. Otros, como SILVA SÁNCHEZ, J. M., por su parte, se han mostrado tremendamente críticos con la legitimidad democrática que aporta el proceso de codecisión implantado, en «Los principios inspiradores de las propuestas de un Derecho penal europeo. Una aproximación Crítica», *RP* núm. 13, 2004, pp. 145 y ss. o han considerado, como hace VOGEL, J. que dicho proceso debería ser mejorado ya que entre otras cosas y por ejemplo, debería permitir que el Parlamento goce de iniciativa legislativa, en «Política criminal y dogmática penal europea», en *RP* núm. 11, 2003, p. 144.

[6] Así, señalaba VOGEL, J. que la cooperación moderna no puede quedar reducida a la faceta de represión de delitos, sino que tiene que tener en cuenta aspectos de investigación proactiva y de prevención del crimen, lo que ha de ser muy tenido en cuenta a la hora de regular la cooperación policial, pero también al hacerlo con la judicial, ya que de no hacerse, dará lugar a importantes problemas de coordinación a la hora de, por ejemplo, transferir y utilizar las pruebas obtenidas durante la realización de la labor policial al correspondiente procedimiento judicial. En «Cooperación penal: cinco tendencias. Cinco propuestas para una acción futura», en *El Derecho penal de la Unión europea. Situación actual y perspectivas de futuro.* Ed. UCLM. Cuenca, 2007, pp. 161 y 162.

comentadas finalidades preventivas y represivas y, en la otra parte de la balanza, siempre habrá de encontrarse el respeto y la garantía de los derechos fundamentales de los ciudadanos, lo que, en el concreto caso que nos ocupa, obliga a que toda captación, transferencia o tratamiento de información que se efectúe en aras a prevenir o reprimir delitos, tenga que partir del más estricto respeto a ese derecho fundamental de nuevo cuño que se ha venido a denominar como derecho fundamental a la protección de datos de carácter personal[7].

La normativa creada por la UE para regular esta compleja cuestión ha sido profusa y variada y su paulatina y sucesiva aprobación ha dado lugar a una confusa y aparentemente no del todo coordinada regulación, cuyo concreto contenido ha respondido, como no podía ser de otra forma, a las diferentes fases que la política criminal europea ha ido viviendo hasta llegar al momento actual.

Veamos ahora, aunque sea de forma somera, cuáles han sido los principales hitos que han ido jalonando este largo y complejo proceso normativo.

[7] El nacimiento y la progresiva autonomización de este derecho fundamental con respecto al de la intimidad están íntimamente ligados con el proceso de delimitación que de ambos derechos ha ido realizando nuestro Tribunal constitucional. Así, fue este tribunal el que señaló, inicialmente, en su STC 254/1993, de 20 de julio, que, pese a que el artículo 18.4 CE protege expresamente derechos como la intimidad o el honor, con lo que actúa como instituto de garantía de los mismos, realiza dicha labor otorgando a la persona un haz de facultades positivas de control sobre todos sus datos que trascienden a los que tradicionalmente definen a dichos derechos fundamentales, lo que demostraría, a su juicio, que tal precepto constitucional establecía un nuevo derecho o libertad fundamental autónomo, aunque conectado con aquellos, que podría quedar encuadrado bajo el nuevo y más amplio concepto de la privacidad. Sin embargo, y unos años más tarde, fue el mismo tribunal el que desarrollando dichos argumentos, afirmó, en su decisiva STC 292/2000, de 30 de noviembre, que, en realidad, el derecho contemplado en el artículo 18.4 CE otorgaba a las personas un poder de control sobre sus datos de carácter personal, tanto privados como públicos, que le convertía en titular de unas facultades positivas que imponían a terceros deberes jurídicos, (como los de informar, pedir el consentimiento, permitir el acceso, rectificar o cancelar los datos, etc.), y que no solo trataban de proteger su intimidad, sino que también tutelaban a todos los bienes de la personalidad que pertenecían a su vida privada y estaban unidos a su dignidad personal, lo que convertiría a la protección de dichos datos en un derecho fundamental independiente y diferente de la intimidad y también de la privacidad, ya que, de hecho, le otorgaba a su titular unas facultades y unos poderes que trascendían con mucho a los que definían a estos dos últimos derechos. Se independizaba así este derecho del derecho a la intimidad, incluso entendido en su más moderna y amplia concepción que abarcaría al denominado derecho a la autodeterminación informativa, lo que nos ha llevado a considerar al derecho a la protección de datos de carácter personal como un verdadero derecho fundamental diferente y completamente autónomo de la intimidad, pese a lo aún hoy mantiene una parte de nuestra doctrina. Véase a este respecto lo sostenido, por ejemplo, por GUICHOT, E., *Datos personales y administración pública*, Ed. Aranzadi, Cizur Menor (Navarra) 2005, 108 y ss. y los argumentos que, frente a la postura finalmente sostenida por este autor, mantuve en GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», en *Revista General de Derecho penal*, núm. 19, 2013, pp. 4 y ss., en <http://www.iustel.com/> (últ. vis. 20-4-2014).

## 2.EL PRINCIPIO DE DISPONIBILIDAD COMO REFERENTE INICIAL DE LA POLÍTICA CRIMINAL EUROPEA RELATIVA A LA COOPERACIÓN JUDICIAL Y POLICIAL EN MATERIA INFORMATIVA.

La Unión europea tomó pronto conciencia de la importancia que los tratamientos de datos iban a tener para el tráfico económico del mercado único. Por ello, ya en el año 1995 emitió la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, (más conocida como Directiva General de Protección de datos personales)[8], cuya aprobación dio lugar, entre otras cosas, a la reforma que, sobre la legislación española referida a esta materia, realizó la todavía vigente Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[9].

Pese a la amplitud que caracterizó a la referida norma comunitaria, pronto se hizo evidente que la misma no iba a poder responder a todos los retos y particularidades que planteaba la aparición y rápida expansión de las nuevas tecnologías de la información y la comunicación y, en especial, a los que generaba Internet.

Por ello, tan solo dos años después de la aprobación de dicha Directiva, el regulador comunitario se vio obligado a aprobar otra, la Directiva 97/55/CE, de 15 de diciembre, precisamente referida al tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones; normativa que, pese a todo, solo 5 años más tarde tuvo que volver que ser actualizada, mediante su sustitución por la aún vigente Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de datos

[8] Así, señala PARIENTE DE PRADA, I. que dicha Directiva se aprobó en un contexto caracterizado, precisamente, por el denodado esfuerzo de la Comisión europea por acabar con las trabas que limitaban el mercado único comunitario, lo que llevó a que dicha norma se desarrollase al amparo del artículo 100 del Tratado de la Comunidad Económica Europea en aquel momento vigente. En «La reforma de la protección de datos en el ámbito europeo», en *El Espacio de libertad, Seguridad y justicia: Schengen y protección de datos.* Ed. Azanzadi. Cizur Menor, 2013, pp. 127 y ss.

[9] En concreto, fue precisamente la transposición de la comentada Directiva la que obligó a reformar la primera legislación nacional específicamente reguladora de esta materia (la ya citada LOTADP), dando lugar a la aprobación de la todavía vigente Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPDP), que, entre otras muchas cosas, extendió la especial protección jurídica que se otorgaba a tales datos, no solo a aquellos que estaban recogidos en forma informática, como hacía la LOTAD, sino también a todos aquellos que se encontrasen en cualquier clase de soportes o ficheros que resultasen adecuados o idóneos para ser tratados, como exigía el artículo 2 de la Directiva 1995/46/CE.

personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[10].

Ya las propias denominaciones de las citadas normas comunitarias parecían indicar que no se habían creado para regular los tratamientos de datos de los que nos vamos a ocupar en este trabajo, esto es, los realizados para prevenir, investigar y reprimir delitos; impresión que se vio completamente ratificada por el hecho de que tanto el artículo 3.2 de la Directiva General de Protección de Datos Personales (la 95/46/CE), como el artículo 1.3 de la vigente Directiva 2002/58/CE, referida al sector de las telecomunicaciones, excluyesen de sus correspondientes ámbitos de aplicación precisamente a los tratamientos *«… que tengan por objetivo la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y* ***las actividades del Estado en materia penal****»*.

Se optó así, claramente por mantener una doble vía a la hora de proteger los datos de carácter personal. Una general y garantista, en la que se reconocía al titular de dichos datos el control sobre los mismos, que, entre otras cosas y en principio, no podían ser recogidos, procesados, ni transmitidos sin contar con su consentimiento[11] y sobre los cuales conservaba unos derechos positivos de información, acceso, rectificación, cancelación y oposición (derechos ARCO), cuyo respeto debía ser controlado y garantizado por determinados organismos administrativos independientes expresamente dedicados a asegurar su efectividad; y una segunda, especial o excepcional, que quedaba al margen de dicha regulación general y de sus garantías, precisamente por entenderse que los tratamientos a los que estaba referida no podrían cumplir con los fines para los que se realizarían (la prevención, investigación y represión de delitos) si el titular de los datos sobre los que recayesen

[10] Sobre la evolución de esta normativa y los problemas a los que se enfrentaba en la moderna sociedad de la información, véase, por ejemplo, RODRÍGUEZ LAINZ, J. L., «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: Derecho derivado», en *LA LEY* núm. 7373, 2010 en <www.laley.es> (últ. vis. 12-4-2014).

[11] Debe señalarse, sin embargo, que los niveles de exigencia de dicho consentimiento varían, atendiendo, entre otras cosas, a la relevancia o especial sensibilidad de los datos de lo que se trate. Véase, por ejemplo y en relación a esta cuestión, lo señalado por APARICIO SALOM, J., *Estudio sobre la protección de datos*. Ed. Aranzadi, Cizur Menor, 2013, pp. 65 y ss. y 149 y ss. o SANTOS GARCÍA, D., *Nociones generales de la Ley orgánica de protección de datos y su reglamento: adaptado al RD 1.720/2007 de 21 de diciembre*. Ed. Tecnos, 2012, pp. 67 y ss., entre otros.

(p. ej. un sospechoso) conservase sobre los mismos todos los derechos que la normativa general le otorgaba[12].

Podría pensarse entonces, que la Unión europea se había mantenido inicialmente al margen de cualquier planteamiento que tuviese que ver con la articulación o armonización de esta segunda vía, de la estrictamente penal, habiéndose limitado a regular la primera por ser la que más clara y directamente incidiría en la libre circulación de mercancías, servicios y capitales que debía caracterizar el mercado único que dicha organización supranacional trataba de implantar y garantizar.

Nada más lejos, sin embargo, de la realidad.

La verdad es que los organismos comunitarios fueron pronto conscientes de que, desde el mismo momento en que se estableciese un espacio o mercado único de libre circulación de personas, capitales y mercancías, como el que en 1985 generó la ratificación y entrada en vigor del Acuerdo Schengen, se hacía necesario implementar medidas de coordinación y de información entre las distintas policías que iban a encargarse de controlar y asegurar la nueva frontera única y común que iban a tener todos los Estados integrados en tal espacio, lo que llevó a que, ya el 19 de julio de 1990 y dentro del Convenio de aplicación del Acuerdo Schengen, se crease y regulase un complejo sistema de intercambio de datos relativos a la identidad de las personas y la descripción de objetos buscados [el Sistema de Información Schengen (SIS)] que trataba, precisamente, de fomentar y facilitar la colaboración entre las autoridades

[12] La existencia de esta doble vía para la protección de datos personales es algo común en todos los ordenamientos jurídicos de los Estados miembros de la Unión Europea y así, en concreto, la propia LOPD española establece en su artículo 2.2.c) que su régimen de protección no será aplicable *«… a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada»;* mientras que su artículos 22, de forma mucho más general, reconoce expresamente que los cuerpos y fuerzas de Seguridad del Estado pueden recoger y tratar los datos de una persona sin contar con su consentimiento, si ello resulta necesario *«… para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales»* y su 23 otorga al responsable del fichero creado con tales fines, la potestad de denegar los derechos ARCO que corresponderían a los titulares de los datos que hubiese recopilado, si su ejercicio pusiese en peligro la seguridad pública o alguna investigación que se estuviese realizando. Sobre estas prescripciones y su incidencia, véase lo comentado por SOLAR CLAVO, P. «La doble vía europea en protección de datos», en *LA LEY* núm. 2832, 2012, en <www.laley.es> (últ. vis. 10-4-2014). En esta misma línea señala, por ejemplo, RODRÍGUEZ LAINZ J.L. en relación con el sistema de captación de datos referidos a las comunicaciones establecido por la Ley Española (Ley 25/2007) que traspuso a nuestro ordenamiento la Directiva 2006/24/CE, que la exención que contempla dicha ley con respecto al principio de consentimiento y la que permite a los proveedores no cumplir con los deberes generales de acceso y cancelación de datos de carácter personal que generalmente les correspondería a su titular, se han establecido, precisamente, para garantizar que los tratamientos que se realicen sobre dichos datos resultasen eficaces a efectos de la investigación y persecución de delitos. En «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», en LA LEY núm. 6859 y 6860, 2008, en <www.laley.es> (últ. vis. 12-2-2014).

policiales y aduaneras de dichos Estados, entre otras cosas, para luchar contra la criminalidad[13].

No fue éste, sin embargo, el único ni el último instrumento creado desde la Unión Europea con el fin de favorecer los intercambios de información y de datos de carácter personal entre las distintas administraciones que están, directa o indirectamente, llamadas a desarrollar labores de prevención o represión de delitos.

De hecho, no tardaron mucho en aparecer organismos como Europol[14] o sistemas, como el Sistema de Información Aduanero (SID)[15], que intentaban favorecer y facilitar al máximo el intercambio de información entre dichas administraciones de los Estados miembros para convertir al mercado único, también en un mercado seguro.

Ahora bien, si hay un momento decisivo en la creación y desarrollo de todos estos sistemas, éste es, sin duda, el que vino dado por la perpetración de los atentados terroristas producidos el 11 de septiembre de 2001 en Nueva York y, sobre todo, por los acaecidos el 11 de marzo de 2004 en Madrid y el 7 y el 21 de julio de 2005 en Londres[16].

No debe sorprender que, ante la magnitud y peculiares características de los referidos atentados, marcados, entre otras cosas, por la internacionalidad y descentralización de la organización terrorista que los perpetró, la Unión Europea optase por intensificar su programa de cooperación en materia penal fomentando y

[13] Sobre el nacimiento de este sistema, su funcionamiento y posterior transformación en el actual sistema de Información Schengen de segunda generación (SIS II) véase, lo comentado por RECUERO, P., «La protección de datos y Schengen: Una visión desde la experiencia española», en El Espacio de libertad, seguridad y justifica: Schengen y protección de Datos. Ed. Aranzadi. Cizur Menor, 2013, pp. 197 y ss.

[14] Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía, hecho en Bruselas el 26 de julio de 1995.

[15] Reglamento (CE) núm. 515/97 del Consejo de 13 de marzo de 1997 relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y la colaboración entre éstas y la Comisión con objeto de asegurar la correcta aplicación de las legislaciones aduanera y agraria

[16] Sobre la incidencia de estos atentados en el desarrollo de esta normativa, véase lo comentado por FERNÁNDEZ, OGALLAR, B., op. cit. ant., p. 338 o AIXALA, A., quien diferencia, a su vez y dentro de este periodo, dos etapas distintas. Una primera que iría desde el atentando del 11 de septiembre en Nueva York hasta el del 11 de marzo en Madrid, donde, a su modo de ver, se adoptó un impulso primordialmente político a las medidas de cooperación judicial y policial, y otro que comenzaría con este último atentado, en el que se produjo un desarrollo mucho más técnico y, a su modo ver, también eficaz. En «La estrategia de la UE ante el terrorismo internacional y la defensa de los derechos y libertades», p. 51, en <http://www.iuee.eu/pdf-publicacio/1/jpjdqoe8lrscpmve8of8. Pdf> (últ. vis. 16-4-2014).

favoreciendo aún más el intercambio transfronterizo de información[17], llegando incluso el programa de trabajo establecido en la Haya, los días 4 y 5 de noviembre de 2004, a considerar, de forma expresa, como uno de los principales objetivos que la UE debería alcanzar, el de favorecer el intercambio de información entre los diferentes organismos nacionales y supranacionales llamados a desempeñar un papel en la prevención de este tipo de conductas.

Para lograrlo se crearon nuevos organismos, como Eurojust[18], y se multiplicaron los datos o ficheros específicamente destinados a favorecer la consecución de dichas finalidades, como los implantados conforme a lo dispuesto en la controvertida Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones,[19]. Pero además y por otra parte, se desarrolló e implantó un nuevo principio rector de la política criminal europea referida a esta clase de tratamientos de datos, el llamado «*principio de disponibilidad*», que tendería a garantizar que las autoridades de cualquier Estado de la UE tuviesen derecho a acceder y a disponer de las informaciones que necesitasen a efectos de prevenir, perseguir o sancionar delitos, cuando menos, en las mismas condiciones que podrían hacerlo las autoridades de

[17] Sobre este proceso y las sucesivas declaraciones emitidas en relación con esta materia, véase lo comentado por AIXALA, A., op. cit. ant. Entre estas declaraciones merece la pena destacar la emitida en Bruselas, el 25 de marzo de 2004, sobre la lucha contra el terrorismo por el Consejo tras el atentado de Madrid, donde se expresamente se afirmó que *«El Consejo Europeo, con el objeto de seguir desarrollando el marco legislativo mencionado más arriba, encarga al Consejo que estudie medidas en los siguientes sectores:*

- *propuestas destinadas a establecer normas sobre la conservación de datos de tráfico de comunicaciones por parte de los proveedores de servicios;*
- *intercambio de información sobre condenas por delitos de terrorismo;*
- *persecución transfronteriza;*
- *un registro europeo de condenas e inhabilitaciones;*
- *una base de datos sobre material forense, y*
- *simplificación del intercambio de información entre los cuerpos y fuerzas de seguridad de los Estados miembros».*

[18] Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

[19] Sobre el contenido de esta Directiva que modificó la previa Directiva 2002/58/CE y su transposición a nuestro ordenamiento véase, lo comentado, por ejemplo, por RODRÍGUEZ LAINZ, «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», cit. ant o GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas?…», cit. ant., pp. 46 y ss., entre otros.

aquel otro Estado miembro en el que la información en cuestión se encontrase registrada[20].

Este principio tuvo una enorme importancia normativa y quedó reflejado, por ejemplo, en la Decisión del Consejo 2008/633/JAI, de 23 de junio de 2008, que permitió a las autoridades responsables de la investigación y prevención de delitos de terrorismo y graves acceder al Sistema de Información de Visados (VIS), previamente creado por el Reglamento 767/2008, de 9 de julio, y también, en la Decisión Marco 2008/315/JAI , de 26 de febrero, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros, posteriormente desarrollada por la Decisión del Consejo 2009/616/JAI, de 6 de abril, que creó el Sistema Europeo de Antecedentes Penales (ECRIS), obligando a los Estados de los nacionales condenados penalmente en otro país, a recibir y almacenar los datos referidos a sus condenas, para poder ponerlos a la disposición de aquellos Estados miembros que se lo requiriesen[21].

Sin embargo, tal vez fuesen la Decisión 2008/615/JAI, del Consejo, de 23 de junio, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza[22], más conocida como la Decisión Prüm, por su por su estrecha relación con el Tratado firmado con anterioridad en dicha localidad alemana entre varios países miembros de la Unión[23], y la Decisión Marco 2006/960/JAI, del Consejo, de 18 de diciembre, sobre la

[20] VOGEL, J., «EU-Arbeitweisevertrag Artikel 82..»., cit. ant. Rnd. 70, ACED FÉLEZ, E., «Principio de disponibilidad y protección de datos en el ámbito policial» en <http://noticias.juridicas.com> (últ. vis. 11-3-2014).

[21] Sobre el proceso de consolidación del intercambio de antecedentes penales y el concreto funcionamiento del sistema ECRIS, véase, por ejemplo, lo comentado por BLANCO QUINTANA, M. J. en «La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales», en *BMJ*, 2013, pp. 3 y ss.

[22] Desarrollada por la Decisión 2008/616/JAI del Consejo, de 23 de junio, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

[23] En concreto, el referido tratado internacional se firmó el 27 de mayo de 2005, en la Abadía benedictina de Prüm, entre el Reino de Bélgica, la Republica Federal de Alemania, España, Francia, Luxemburgo, Países Bajos y Austria, siendo posteriormente suscrito por Italia, Finlandia, Portugal y Eslovenia. De hecho, la aprobación de este tratado por parte de España es la que motivo la aprobación de la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir de ADN, cuya entrada en vigor, como señala HOYOS SANCHO, M. ha llevado a que el sistema de transmisión de datos establecido por la comentada Decisión Marco se haya podido utilizar desde el inicio en España, sin necesidad de que el Consejo haya tenido que comprobar que nuestro ordenamiento había incorporado las disposiciones del capítulo 6 de dicha Decisión. En «Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos», en *Espacio europeo de libertad, seguridad y justicia: Últimos avances en cooperación judicial penal*. Ed. Lex Nova. Valladolid, 2010, p 164.

simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea[24], las normas europeas que dieron el mayor impulso a la implantación de dicho principio, al garantizar la disponibilidad de un amplio y variado número de informaciones a todos los organismos nacionales y europeos dedicados a la investigación y prevención de delitos.

Como se puede comprobar, el predominio de las políticas securitarias y represivas europeas durante este periodo fue, como era previsible, absoluto, quedando la garantía de los derechos a la intimidad y a la protección de datos personales de los ciudadanos en un muy segundo plano.

Así, mientras todas las normas comentadas tendían a facilitar al máximo la captación, el intercambio y el uso de información por parte de las autoridades implicadas en la investigación y represión de delitos, estableciendo, entre otras cosas, la obligación de los Estados miembros de tener disponibles los datos en cuestión y de entregarlos, incluso en plazos perentorios, a los organismos y autoridades competentes en dicha materia del resto de países de la UE[25], y reconociendo, incluso, la posibilidad de que la simple autorización del Estado cedente de los datos pudiese habilitar al cesionario para utilizarlos con fines diversos de aquellos para los que inicialmente los había solicitado[26]; sus textos dedicaron una prácticamente nula atención a la protección de los derechos y garantías que habrían de corresponder al titular de los datos personales tratados y transmitidos por tales sistemas, limitándose alguno a realizar alguna alusión general a la necesidad de que tales sistemas

[24] ACED FÉLEZ, E., op. cit. ant.

[25] Así, por ejemplo, y como señala ACED FÉLEZ, E. la Decisión Marco 2006/960/JAI, establece un plazo máximo de entrega de tan solo 8 horas en caso de urgencia, en op. cit. ant.; mientras que BLANCO QUINTANA, M. J. señala que las solicitudes de antecedentes penales realizadas por los Estados en relación a un procedimiento penal, utilizando el sistema ECRIS creado por la Decisión Marco 2009/315/JAI y la Decisión 2009/316/ JAI, deben ser atendidas en un periodo máximo de 10 días desde la recepción de la solicitud. En op. cit. ant., p. 22.

[26] Así lo hace, por ejemplo, el artículo 35 de la conocida como Decisión Prüm (la Decisión Marco 2008/615/JAI) que, como señala SAINZ HERMIDA, A., permite que los datos transmitidos puedan ser utilizados para otros fines, previa autorización de la Parte titular del fichero, siempre que tales fines estén previstos en el Derecho interno y la transmisión se realice de conformidad con el Derecho de la parte receptora, en «Protección de Datos…» cit. ant., p. 8. Algo más restrictiva es, pese a todo, la Decisión Marco 2009/315/JAI, cuyo artículo 9 establece que los antecedentes trasmitidos para su uso en un procedimiento penal solo podrán ser usados en aquel procedimiento para el que se solicitaron según consta en el impreso de solicitud, aunque su apartado tercero establece la excepción de que se podrán utilizar también *«…para evitar una amenaza inminente y grave para la seguridad pública».* Sobre este particular, véase lo comentado también por BLANCO QUINTANA, M. J., op. cit. ant., p. 23.

respetasen los derechos fundamentales reconocidos por el artículo 8 de la Convención Europea de Derechos Humanos (CEDH)[27], mientras que otros tan solo declaraban, en su parte expositiva y sin mayor precisión, que su articulado era, de hecho, conforme a lo establecido en la Carta de Derechos Fundamentales de la UE (CDFUE) y en especial, a los derechos a la intimidad y a la protección de datos de carácter personal que allí se contenían[28].

Puede que fuese esta situación la que llevó a que, más recientemente, el regulador europeo decidiese aprobar la Decisión Marco 2008/977/JAI, de 27 de noviembre, de protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, cuya creación, como indicaba su artículo 1, tenía por objetivo *«… garantizar* ***un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas*** *y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal, contemplada en el título VI del Tratado de la Unión Europea, garantizando al mismo tiempo un alto nivel de seguridad pública»*[29].

Pese a lo contundente de esta declaración, la verdad es que lo concretamente establecido en esta norma se presentó, ya desde un primer momento, como claramente insuficiente para conseguir tal fin.

No es sólo que, al haberse optado por establecer esta nueva normativa mediante la aprobación de una Decisión Marco, que, por definición, carecería de efecto directo sobre las normativas nacionales, se incrementase significativamente el riesgo de que se pudiesen dar importantes divergencias entre dichas regulaciones a la hora de transponer sus disposiciones, impidiéndose así que su aprobación pudiese servir para

[27] Así lo destaca RODRÍGUEZ LAINZ, J. L. con respecto a las Directivas 2002/58/CE y 2006/24/ CE viniendo el artículo 4 de la última Directiva citada, como señala el mismo autor, a determinar que el sistema de acceso a los datos que los proveedores tienen que almacenar para cumplir con lo en ella impuesto, debe atender a lo establecido en la CEDH. En «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas…», cit. ant.

[28] Así lo hace, por ejemplo, la conocida como Decisión Prüm (Decisión 2008/615/JAI del Consejo), cuyo considerando 18 del preámbulo parte precisamente parte del principio general de que la Decisión respeta dichos derechos.

[29] Precisamente, y con respecto a este precepto, destaca OERMANN, M. que mientras el artículo 8 de la CDFUE no aludía a ninguna finalidad a la hora de tutelar el derecho fundamental a la protección de datos, en el comentado precepto de la DM 2008/977/JAI se deja claro que su protección se pone en relación con de la seguridad pública, sin que el regulador haga establecido una prelación entre ambos fines. En OERMANN, M. *Individualdatenschutz im europäischen Danteschutzrecht*. V Centauros, Freiburg, 2012 p. 81.

alcanzar el deseable y necesario nivel de armonización en la materia que nos ocupa[30]; o que, al limitar paralelamente su ámbito de actuación a los intercambios transnacionales de datos realizados entre los Estados miembros, se dejasen al margen de su regulación y garantías a todos aquellos intercambios o tratamientos que se produjesen dentro de un único Estado, lo que podría dar lugar a la paradójica situación de que los titulares de datos que se incorporasen a los registros españoles mediante transferencias de otro Estado miembro pudiesen disfrutar de unos derechos y unas garantías de los que podrían carecer aquellos que vieron como sus datos se incluyeron en tales registros sin mediar dicha transferencia[31]; o incluso que, al no limitar su articulado suficientemente la finalidad con la que los Estados receptores podrían utilizar los datos que se les hubiesen transmitido, continuase dejando las puertas abiertas a que éstos puedan usarlos para fines completamente diferentes de los que fundamentaron su absolutamente excepcional captación y transmisión, esto es, para fines distintos de la mera persecución, investigación y represión de conductas penalmente relevantes[32].

Es que además y lo que es más importante, al no derogar ni modificar su articulado, lo que la multitud de normas comunitarias reguladoras de los diferentes sistemas de intercambio y facilitación de datos de carácter personal con fines penales establecen con respecto al funcionamiento y utilización de dichos sistemas, se convirtió a esta Decisión Marco en un instrumento que en nada afectó al verdadero «*patchwork*» normativo que existía ya en la UE con respecto a tales de tratamientos, con lo que se le dotó de una escasísima trascendencia práctica, quedándose muy lejos, por tanto, de alcanzar el objetivo para el que supuestamente se había creado, el de

[30] Así se deduce de lo establecido por el artículo 1 de la comentada Decisión Marco, como lo señala RODRÍGUEZ LAINZ, J. L., «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas…», cit. ant.

[31] ACED FÉLEZ, J., op. cit. ant. En este mismo sentido, SANZ HERMIDA, A. señala que se podrían dar divergencias en la protección otorgada a los datos que se transmiten, los internos y también con los que se podrían transmitir a terceros países a los que no les sea aplicable la normativa europea. «Protección de datos en la transmisión», cit. ant. p. 13.

[32] En este sentido, señala ALCAIDE FERNÁNDEZ, J. que los artículos 3 y 11 de esta Decisión Marco, también permiten que los datos inicialmente transmitidos para la realización de una investigación criminal puedan ser posteriormente utilizados para fines diferentes pero compatibles de los que justificaron dicha transmisión, afirmando, el referido autor que ello obligará a que tengan que ser los Estados los que deban determinar, en el ámbito nacional, de forma más precisa qué concretos fines posteriores se tendrán que considerar como incompatibles con el inicial, en op. cit. ant., p. 6.

establecer un alto nivel de protección para los derechos y libertades de las personas que se pudiesen ver afectadas por tales tratamientos[33].

El panorama, por tanto y como se puede comprobar, continuaría siendo, tras la aprobación de esta Decisión Marco, desalentador en lo que se refería a la protección de los derechos fundamentales de los ciudadanos. Sin embargo, tras este inicial y hasta cierto punto esperable comienzo, parecía que la aprobación y entrada en vigor del Tratado de Lisboa, suscrito por los Estados miembros de la Unión el 13 de diciembre de 2007, podría obligar a la UE a cambiarlo de forma radical.

## 3.UN NUEVO E IMPORTANTE REFERENTE NORMATIVO: EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA CDFUE TRAS LA ENTRADA EN VIGOR DEL TRATADO DE LISBOA

La aprobación y entrada en vigor del Tratado de Lisboa ha supuesto, entre otras cosas, que el nuevo artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) haya pasado a reconocer de forma expresa que toda persona tiene derecho a la protección de sus datos de carácter personal y que el Parlamento europeo tiene la obligación de establecer una normativa que garantice tal derecho[34].

Pero, además y lo que es incluso más importante para el tema que nos ocupa, también ha llevado a que el nuevo artículo 6 del propio Tratado de la Unión Europea (TUE) haya convertido, de una vez por todas, a la Carta de Derecho Fundamentales de la Unión Europea (CDFUE) en un instrumento de valor equivalente a los propios

[33] PEYROU, S., «Algunas reflexiones sobre la protección de datos en el ELSA o la crónica de una esperanza frustrada», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013, p. 148, GONZÁLEZ MURUA, A. R., «El supervisor Europeo de protección de datos ante la revisión del marco jurídico de la protección de datos. Especial referencia a las reformas en el seno del espacio de libertad, seguridad y justicia», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013, p. 246.

[34] En concreto, este precepto establece que: *«1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.* (…)», lo que llevó a TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. a afirmar que dicho precepto deberá llevar a la unificación de la protección jurídica de datos en el nivel del Derecho derivado, atendiendo, eso sí, a los principios de subsidiaridad y proporcionalidad. En *Einführung in das Datenschutzsrecht.* V. Oldenburg, München, 2012. p. 136.

tratados constitutivos, lo que llevará a que sus prescripciones y derechos resulten directamente vinculantes para toda la Unión y para toda la normativa derivada que de ella proceda, dejando ya de actuar como un mero referente de esa serie de principios generales comunes a todos los Estado miembros que, según sostenía el Tribunal Europeo de Justicia, el Derecho de la UE debería tener en cuenta y tratar de respetar, para pasar a convertirse, por fin, en derechos plenamente vinculantes para dicha institución supranacional y su Derecho, con lo que su respeto se podrá exigir directamente ante el citado Tribunal[35].

Con ello, se reconoció expresamente la competencia de la UE para regular en materia de protección de datos personales y se introdujo, al mismo tiempo, la obligación jurídica de que todo el Derecho europeo derivado hubiese de respetar el derecho a la protección de dichos datos que se contiene en el artículo 8 de la CDFUE; precepto que, entre otras cosas y como señala OERMANN, a diferencia de lo que sucede, por ejemplo, con el artículo 3 de la todavía vigente Directiva General de Protección de Datos personales (la 95/46/CE), no contempla ninguna limitación expresa del ámbito de aplicación de este derecho en relación a las materias de policía, justicia o defensa de los Estados vinculados por tal tratado[36].

Parecía entonces, que el comentado Tratado tendía a adoptar un enfoque mucho más transversal y orientado hacia la protección de los datos de carácter personal que el que hasta aquel momento había mantenido la UE y, consecuentemente, obligaría a

[35] En concreto, el artículo 6 de TUE establece que *«La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.*
*Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados.*
*Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones. (…)*». Sobre la trascendencia de dicha declaración normativa, véase lo comentado por FERNÁNDEZ, OGALLAR, B., op. cit. ant., pp. 53 y ss. y 72, mientras que sobre la situación previa a la entrada en vigor de este Tratado y el tratamiento que el Tribunal Europeo de Justicia dio a lo establecido tanto en el CDFUE o en el CEDH, resulta interesante la lectura de lo comentado por RODRÍGUEZ LAINZ, J. L en «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: Derecho primario», en *LA LEY*, núm. 7373, 2010, <www.laley.es> (últ. vis. 12-4-2014).

[36] OERMANN, M., op. cit. ant., p. 77. Ha de señalarse, en esta misma línea, que, como mantiene PEYROU, S., pese a que en un principio el nuevo artículo 16 del TFUE tampoco establezca excepción alguna en materia de policía o derecho penal a la necesidad de regular y garantizar dicho derecho, excepcionando del mismo tan solo las materias de extranjería y seguridad común, la Declaración núm. 21 aneja al Tratado de Lisboa sí que prevé expresamente la adopción de reglas específicas o excepciones en materia de cooperación judicial o policial en materia penal. Op. cit. ant., pp. 152 y 153.

dicha institución a revisar la regulación que hasta entonces había creado sobre la materia[37].

Así de hecho, se indicó en el Programa de Estocolmo (COM (2010) 171), que definió las orientaciones de la UE en el marco del Espacio de Libertad, Seguridad y Justicia para el periodo 2010-2014, y en la Agenda Digital para Europa (COM (2010) 245), en cuyo desarrollo, la Comisión europea elaboró e hizo público, el 25 de enero de 2012, un importante paquete normativo, tendente a establecer un nuevo marco normativo en materia de protección de datos de carácter personal, que estaría compuesto por dos normas fundamentales[38]: Una propuesta de Reglamento que vendría sustituir a la ya citada Directiva General de protección de datos personales[39] y una de Directiva llamada a reemplazar a la ya comentada y criticada Decisión Marco 2008/977/JAI, para establecer, como su propio título indica, un sistema de *«… protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos»*[40].

Con ello, y como fácilmente se puede deducir, se continuaba manteniendo la doble vía que había caracterizado a la regulación europea referida a la protección de datos personales hasta ese momento, diferenciando, una general, regulada en el proyectado Reglamento y una específica o excepcional, contenida en la propuesta de Directiva, que trataría de establecer un régimen especial que respondiese adecuadamente a las particulares necesidades que planteaba la cooperación informativa, policial y judicial, en materia penal[41].

Esta última regulación presentaría significativas y destacables diferencias con respecto a aquella que vendría a sustituir, la contenida en la anteriormente criticada Decisión Marco 2008/977/JAI.

La primera y más evidente, se deriva del hecho de que, al tener forma de Directiva y no de Decisión Marco como su predecesora, conseguirá que su articulado

[37] PEYROU, S., op. cit. ant., pp. 150 y ss.
[38] TINNEFELD, M. T./ BUCHNER, B. /PETRI, T., op. cit. ant., p. 124; PEYROU, S., op. cit. ant. p. 152, SOLAR CALVO, P., op. cit., ant., entre otros.
[39] COM (2012) 0011.
[40] COM (2012) 0010.
[41] PEYROU, S., op. cit. ant., p. 153.

tenga un efecto directo sobre las normativas nacionales, lo que sin duda incrementará su eficacia de armonizadora[42], por más que continúe permitiendo que existan ciertas divergencias entre tales ordenamientos, al otorgar a sus respectivos legisladores cierto margen de maniobra a la hora de decidir el modo en que cumplir con lo que la misma les exigiría que consiguiesen[43]; efecto que, además, y por otra parte, se verá notablemente intensificado como consecuencia de que la proyectada regulación no limite ya su ámbito de aplicación, tal y como hace la todavía vigente Decisión Marco, a los intercambios transfronterizos de datos, sino que también prevea su aplicación con respecto a los tratamientos puramente nacionales[44].

Sin embargo, y frente a todos estos importantes avances, hay que reconocer, como señala el Supervisor Europeo de Protección de Datos (SEPD) en su dictamen de 7 de marzo de 2012, referido al comentado paquete legislativo, que la Directiva propuesta también presenta notables deficiencias.

Así, por ejemplo, resulta altamente criticable que, a pesar de que sus artículos 5 y 6 obliguen a los Estados miembros a distinguir los datos personales que traten con fines penales, dependiendo de a quien estuviesen referidos (sospechosos, condenados, víctimas, testigos, etc..), de su grado de fiabilidad y exactitud o de si estaban referidos a personas o a hechos, no prevea, sin embargo, ninguna consecuencia ni efecto práctico para dicha clasificación; o que continúe dejando completamente en manos de las normativas estatales la determinación de cuestiones tan fundamentales para la protección de los derechos de los ciudadanos, como las de los plazos máximos que las autoridades competentes podrán almacenar sus datos personales, sin contar con el consentimiento o voluntad de su titular.

---

[42] SOLAR CALVO. P., op. cit. ant.

[43] TINNEFELD, M. T./ BUCHNER, B. /PETRI, T., op. cit. ant., p. 125. Esto último ha sido, sin embargo, criticado por PEYROU, S. quien pone de manifiesto el hecho de que resultaría mucho más efectivo, a la hora de reducir la fragmentación jurídica existente, haber establecido dicha normativa mediante un reglamento, como se ha hecho a la hora de regular la protección general de los datos utilizados con otros fines, en op. cit. ant., p.154.

[44] Así lo indica, por ejemplo, PEYROU, S., op. cit. ant., p. 157; TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. quienes, sin embargo, destacan que quedan al margen de su ámbito de aplicación los tratamientos de datos realizados por las instituciones de la UE (que se han de ajustar a lo establecido por el Reglamento (CE) 45/2001, de 18 de diciembre de 2000 y otras normas específicas) y las actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, como las relativas a la seguridad nacional (artículo 2.3 de la Propuesta de Directiva) op. cit. ant., p. 134; excepción ésta que, curiosamente, y como señala SOLAR CALVO, P. podría llevar a que se mantengan al margen de dicha norma europea todos los tratamientos de datos de carácter personal que se realicen con fines de prevención, investigación, prevención, detección o enjuiciamiento de delitos terroristas, en Op. cit. ant.

Tampoco parece aceptable que establezca unos requisitos y garantías realmente débiles a la hora de autorizar que dichos datos se puedan transferir a terceros países diferentes de los integrantes de la UE y que, consecuentemente, no estarían dentro del ámbito de aplicación de las garantías que prevé la propia Directiva o, lo que es incluso peor, que su artículo 59 deje vigentes e inalterados los articulados del numeroso elenco de normas especiales que regulan el complejo «patchwork» normativo actualmente existente en la UE en relación a los tratamientos de los que nos venimos ocupando, lo que, evidentemente, redundará en una significativa merma de las garantías de los derechos de los ciudadanos[45].

Otra crítica que se debe hacer a la comentada norma se deriva del hecho de que parezca contemplar la posibilidad de que el régimen excepcional que establece para los tratamientos realizados con fines penales, se pueda también llegar a utilizar para perseguir fines distintos de los exclusivamente referidos a la prevención, investigación o represión de delitos.

Así se deduce del hecho de que su artículo 7 establezca que los Estados miembros dispondrán que los tratamientos de datos personales a los que dicha norma se refiere serán lícitos, tanto si se realizan, por parte de la autoridad competente, para ejecutar las tareas tendentes a lograr los fines de los que habla su artículo 1.1., esto es para, prevenir, investigar o sancionar alguna infracción penal, como si se utilizan *«b) para cumplir con una obligación jurídica a la que esté sujeto el responsable del tratamiento*», *«c) con el fin de proteger intereses vitales del interesado u otra persona»* o *«d) a fin de prevenir una amenaza inminente y grave para la seguridad pública»*, amenaza que, evidentemente y por pura coherencia, no podrá tener carácter delictivo, ya que ello llevaría a que su expresa previsión resultase redundante y careciese de cualquier sentido.

La pregunta es inmediata, ¿podrían utilizarse entonces, conforme a lo establecido en esta nueva Directiva, unos datos que hubiesen sido recogidos, con limitaciones de los derechos de sus titulares, por ser necesarios para realizar una investigación de un delito, para realizar un posterior tratamiento que persiguiese otro fin diferente, aunque

[45] Sobre este informe GONZÁLEZ MURUA. A. R., op. cit. ant., p. 245. Respecto al mantenimiento de la fragmentariedad normativa existente en esta materia, señala PEYROU, S., que el sistema de evaluación de la aplicación del contenido en de esta Directiva, previsto en el artículo 61 de su proyectado texto y que obliga a la Comisión a evaluar su efectividad armonizadora tras tres años desde su entrada en vigor, no impedirá que dicha profusa y completa normativa siga estando vigente por un periodo que se considera inaceptable por parte del SEPD. En op. cit. ant., p.155.

legítimo, como podría ser la prevención de alguna alteración pública no delictiva o la resolución de un procedimiento administrativo sancionador?

La respuesta atendiendo a lo dispuesto en el referido precepto parece que tiene que ser afirmativa, con lo que no debe extrañar que nos asalten las dudas sobre la compatibilidad de esta nueva normativa con las exigencias derivadas del respeto al derecho fundamental a la protección de datos personales del artículo 8 CDFUE.

Habrá que afirmar, en consecuencia, como de hecho hace el propio SEPD, que el panorama normativo referido a los tratamientos de datos de los que nos venimos ocupando, continuará siendo «extremadamente decepcionante» en lo que se refiere a la garantía y tutela del derecho a la protección de datos de carácter personal, incluso si se llega finalmente a aprobar la proyectada Directiva[46]; panorama que, sin embargo y a nuestro modo de ver, habrá de cambiar de forma radical en un futuro cercano, no como consecuencia de la aprobación de ninguna norma o Tratado nuevo por parte de la UE, sino, precisamente y como en tantas ocasiones anteriores, como resultado de la emisión de una Sentencia del Tribunal de Justicia de la Unión Europea. En concreto de la que dicho Tribunal emitió el pasado 8 de abril de 2014, en relación a la Directiva de conservación de datos relativos a las comunicaciones con fines de investigación criminal, (la ya citada Directiva 2006/24/CE), resolución de la que nos pasamos a ocupar.

## 4.LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA DE 8 DE ABRIL DE 2014 Y SU POSIBLE REPERCUSIÓN EN LA POLÍTICA EUROPEA DE PROTECCIÓN DE DATOS PERSONALES EN MATERIA PENAL MUITO POUCO SE SABE ACERCA DO VERDADEIRO CONHECIMENTO E PODER COMPUTACIONAL E INTELECTUAL DAS AGÊNCIAS DE SEGURANÇA DAS GRANDES POTÊNCIAS MUNDIAIS, COM DESTAQUE PARA A NSA.

Muchas fueron las voces que, desde un principio, se alzaron frente al controvertido sistema de captación y almacenamiento generalizado de datos de

[46] Dictamen del SEPD de 7 de marzo de 2012 (2011/C 181/02).

telecomunicaciones que creó la Directiva 2006/24/CE y que obligaba a todos los proveedores de dicha clase de servicios a retener determinados datos externos, relativos a las comunicaciones que realizasen sus clientes, para garantizar que su realización se puedan posteriormente «trazar» o analizar, en caso de que ello fuese requerido para investigar un delito grave. Críticas que incluso se vieron judicialmente respaldadas por el hecho de que algún Tribunal Constitucional, como el alemán, llegase a declarar que parte de la ley que traspuso dicha normativa europea al ordenamiento jurídico de aquel país era incompatible con los derechos garantizados por su Carta Magna [47].

Precisamente en esta misma línea, pero más recientemente, la Corte Suprema de Irlanda y el Tribunal Constitucional de Austria plantearon sendas peticiones de Decisión prejudicial ante el Tribunal Europeo de Justicia, (asuntos C-293/12 y C-594/12 respectivamente), en las que solicitaban a dicho Tribunal que aclarase si ya el propio texto de la Directiva de conservación de datos era compatible o no con los derechos a la vida privada y a la protección de datos de carácter personal contemplados en los artículos 7 y 8 de la CDFUE, cuyo respeto, como ya vimos, resulta directamente vinculante para la propia Unión y judicialmente exigible ante dicho Tribunal, tras la entrada en vigor del Tratado de Lisboa[48].

Ambas peticiones fueron acumuladas por el Tribunal europeo y se resolvieron finalmente en su muy reciente sentencia de 8 de abril de 2014.

En esta Sentencia, el citado Tribunal afirmó que, dado que las captaciones y almacenamientos de datos que se efectúan conforme a lo establecido en la citada Directiva indudablemente limitan o interfieren en los derechos a la vida privada y a la

[47] Véase a este respecto lo establecido en la Sentencia del BverG, de 2 de marzo de 2010, en la que se declara inconstitucional la normativa alemana que transponía esta Directiva por violar los principio de proporcionalidad y de determinación jurídica o claridad legal, comentada, entre otros, por ORTIZ PRADILLO, J. C. «Tecnología *versus* Proporcionalidad en la investigación Penal: La nulidad de la ley Alemana de conservación de datos de tráfico de las comunicaciones electrónicas», en *La Ley Penal* núm. 75, 2010, en <www.laley.es> (últ. vis. 2-5-2012). No faltaron tampoco las voces en España que desde un primero momento pusieron en tela de juicio la legitimidad del sistema establecido por esta Directiva por considerarlo incompatible con el principio de proporcionalidad. Véase a este respecto, por ejemplo, lo comentado por GONZÁLEZ LÓPEZ. J. J. «La retención de datos de tráfico de las comunicaciones en la Unión europea: Una aproximación Crítica», en *La LEY* núm. 6456, 2006, en <www.laley.es> (últ. vis. 10-5-2012), entre otros.

[48] En concreto, la Corte Suprema Irlandesa presentó su petición el 11 de junio de 2012, como consecuencia de la demanda presentada la Sociedad Digital Rights, dedicada a la promoción y protección de los derechos civiles y ciudadanos contra la normativa de aquel país que transpuso dicha directiva; mientras que Tribunal Constitucional de Austria presentó la suya el 19 de diciembre del mismo año, como consecuencia de los recursos interpuestos contra la normativa de aquel país por el Estado de Kärntner, el Sr. Seitlinger y otros 11.130 demandantes más.

protección de datos personales protegidos por los mencionados preceptos de la CDFUE, se hacía necesario analizar si tal interferencia o limitación podía quedar, sin embargo, justificada atendiendo a lo establecido en el artículo 52 la propia Carta, donde se afirma que *«… cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades»,* para afirmar a continuación que *«… sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».*

Partiendo de esta base, el Tribunal europeo señaló que, si bien era cierto que la cuestionada Directiva afectaba a los citados derechos fundamentales, no llegaba, sin embargo, a lesionar sus respectivos contenidos esenciales, ya que, ni lesionaba el contenido esencial del derecho a la vida privada, al no ser una norma que permitiese conocer el contenido de lo que los ciudadanos comunicasen a través los medios a los que sus prescripciones les eran aplicables, ni afectaba al núcleo del derecho fundamental a la protección de los datos personales, ya que establecía ciertas medidas de protección de los datos captados frente a posibles abusos o actuaciones accidentales precisamente para salvaguardar lo fundamental de dicho derecho.

Tampoco consideró el Alto Tribunal que se pudiese cuestionar que la finalidad perseguida por la Directiva analizada, la de asegurar que los datos estuviesen disponibles a efectos de investigación, detección y persecución de delitos graves, no fuese un fin u objetivo perfectamente legítimo y de interés general, cuya búsqueda podría contraponerse a los citados derechos fundamentales, llegando incluso a legitimar su limitación. De hecho, así parecería indicarlo el hecho de que el propio artículo 6 de la CDFUE reconozca que todas las personas tienen derecho tanto a la libertad, como a la seguridad, contraponiendo, de esa forma, al primer valor, la libertad y sus garantías, con aquel otro que el comentado sistema de captación de datos trataría de alcanzar, el de la seguridad[49].

Es por ello, por lo que el Tribunal europeo entendió que la cuestión fundamental a dilucidar en los asuntos que ante él se habían planteado, sería la relativa a si las

[49] En concreto, el artículo 6 CDFUE establece que *«Toda persona tiene derecho a la libertad y a la seguridad»*.

concretas limitaciones de derechos establecidas por el sistema contenido en la cuestionada Directiva respondían o no a las exigencias derivadas del principio de proporcionalidad en sentido estricto; cuestión que obligaba a analizar, en primer lugar, si su imposición resultaría adecuada o no para conseguir la finalidad supuestamente justificaba su existencia, para después estudiar, si las concretas restricciones de derechos que iba a imponer para alcanzarla habrían quedado realmente limitadas a aquellas que resultaban estrictamente necesario imponer para hacerlo.

La primera de las cuestiones fue rápidamente resuelta por el Tribunal, ya que entendió como innegable que la captación de los datos relativos a las comunicaciones resultaba perfectamente adecuada e idónea para facilitar la investigación y persecución de delitos, sobretodo, teniendo en cuenta el papel fundamental que dichas comunicaciones han adquirido en la sociedad de la información en la que vivimos

Mucho más cuestionable resultaba, sin embargo, la segunda. Esto es, que se pueda realmente afirmar que el uso previsto para esta herramienta limitadora de derechos fundamentales hubiese quedado verdaderamente limitado a aquel que resultaba estrictamente necesario efectuar para perseguir tan legítimo fin.

En concreto, el TEJ consideró que la comentada Directiva vulneraría dicho límite con respecto al derecho a la protección de datos establecido en el artículo 8 CDFU, al permitir, por ejemplo, que el nivel de las medidas de seguridad que los proveedores tendrían que imponer, para evitar posibles abusos con respecto a dichos datos, pudiese depender de una valoración de los costes que su implantación podría llegar a generarles a dichos sujetos y también al autorizar que los datos que los mismos captasen y almacenasen pudiesen ser transferidos a terceros países, ajenos a la UE, donde su uso o posible abuso escaparía por completo al control de las autoridades independientes que, conforme a lo establecido en el apartado 3 del citado artículo de la CDFUE, deben garantizar el respeto a dicho derecho.

Tampoco respondía a las exigencias derivadas del principio de proporcionalidad el hecho de que la comentada Directiva implante un sistema de captación y almacenamiento general de los datos externos referidos a todas las comunicaciones, que lleve a que tales datos se puedan e incluso se tengan que recopilar y almacenar, aun cuando no exista indicio alguno, ni siquiera remoto, de que estuviesen

relacionados con la comisión de un delito grave, o cuando se sepa incluso que estaban referidos a comunicaciones efectuadas por personas que estaban amparadas y obligadas a mantener el secreto profesional. Esto resulta, a juicio del Alto Tribunal, absolutamente desmedido y, por tanto, desproporcionado, como también lo será que la citada norma comunitaria ordene que los datos captados se almacenen por un periodo mínimo de 6 meses, olvidando así que no todos los datos captados son igualmente útiles para perseguir e investigar delitos, con lo que la prolongación del almacenamiento de algunos de ellos carecerá de sentido a tales efectos y resultará, por tanto, también manifiestamente innecesaria y desproporcionada.

Pero es que además, tampoco resulta posible mantener que las restricciones de derechos establecidas por esta Directiva hayan quedado realmente limitadas a las que resulta estrictamente necesario imponer para perseguir delitos graves, cuando su articulado ni determina que comportamientos deben considerarse como tales[50], ni establece ninguna limitación o control que garantice que sus restricciones no se puedan emplear para perseguir otro tipo de conductas diferentes de las finalmente se lleguen a tener como verdaderos delitos graves[51].

[50] De hecho, sobre la interpretación y delimitación de este concepto, del de delito grave, existe todavía una viva polémica doctrinal y jurisprudencial, ya que mientras algunos autores y tribunales parten de el mismo debe ser interpretado conforme a la clasificación de los delitos que realiza nuestro Código penal en su artículo 33 CP; otros, como, por ejemplo, RODRÍGUEZ LAINZ, J. L. en «Hacia un nuevo entendimiento de gravedad del delito en la Ley de conservación de Datos relativos a las Comunicaciones Electrónicas», *LA LEY* núm. 7789, 2012 <www.laley.es> (últ. vis. 4-2-2014) o en «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», cit. ant., propugnan una interpretación mucho más flexible y que no atienda tan solo a la concreta pena con la que el legislador sancione las conductas en cuestión, sino también otros factores, como la «relevancia social del hecho» o su repercusión; conceptos todos ellos altamente indeterminados y difusos, cuya concreción puede depender de criterios puramente subjetivos o incluso de factores tales como la importancia que los medios de comunicación decidan darle al hecho en cuestión, lo que nos lleva a rechazar su posible aplicación en este contexto, tal y como hace, por ejemplo, CORTÉS BECHIARELLI, E. por entender, como este autor, que el uso de tales conceptos no solo puede llevar a que los jueces se arroguen funciones casi legislativas en esta materia, sino también a que se olvide que cuando el legislador impone una pena de forma abstracta para un delito, es porque ha valorado y determinado la gravedad de su realización en la propia ley que lo castiga. En *El delito de corrupción deportiva.* Ed. Tirant lo Blanch, Valencia 2012 .p. 217.

[51] Ha de señalarse en este sentido, que aún a día de hoy, continúa habiendo una viva polémica doctrinal y jurisprudencial en nuestro país sobre las condiciones y requisitos procesales que han de cumplirse para poder acceder a dichos datos, ya que mientras algunas sentencias, como la STS 236/2008, de 9 de mayo, mantienen que dichos datos están disponibles para cualquiera de las autoridades responsables de la persecución e investigación de delitos de las que habla la Ley 25/2007, de 18 de octubre de 2007, de conservación de datos de comunicaciones electrónicas y redes públicas de comunicación, algunos autores, entre los que me incluyo, consideramos que el artículo 7 de dicha ley obliga expresamente a contar con una autorización judicial para acceder a los mismos, ya que su acceso afecta también al derecho fundamental al secreto de las comunicaciones, tal y como ha afirmado el TEDH en reiterada jurisprudencia, desde su célebre Sentencia de 2 agosto 1984, referida al denominado «caso *Malone vs Reino Unido*». Sobre esta polémica véase lo comentando, por ejemplo, por FRIGOLS I BRINES, E.

Todo ello llevó al TEJ a considerar que la comentada Directiva resultaba completamente incompatible con lo establecido en el CDFUE, por lo que debía considerarse inválida y carente de todo efecto. Pero también y paralelamente, le llevó a establecer una serie de criterios o referentes que habrán de ser tenidos muy en cuenta a la hora de valorar la posible compatibilidad con las prescripciones contenidas en dicha Carta protectora de los derechos fundamentales, de cualquier normativa que se haya creado o se vaya a crear con el fin de regular los sistemas de tratamientos de datos personales a los que hemos dedicado este trabajo.

Veamos por ello, a continuación y aunque sea someramente, en qué medida dichos referentes o pronunciamientos judiciales deberían influir tanto en la normativa europea actualmente vigente en relación a dichos tratamientos, como sobre los proyectos que la UE vienen tramitando, precisamente y según se nos dice, con el fin de crear un nuevo y más garantista marco regulador para los mismos.

## 5.LA UNIÓN EUROPEA ANTE LA ENCRUCIJADA. ¿HACIA UNA NUEVA POLÍTICA CRIMINAL REFERIDA A LOS TRATAMIENTOS DESTINADOS A LA PREVENCIÓN, INVESTIGACIÓN Y PERSECUCIÓN DE DELITOS?

Lo comentado hasta el momento ha puesto de manifiesto que la regulación europea referida a los tratamientos de datos con fines de prevención o represión criminal ha vivido hasta el momento dos fases claramente diferenciadas.

Una inicial, caracterizada primordialmente por la creación de instrumentos tendentes a facilitar y favorecer la cooperación y el intercambio de datos e informaciones entre las diferentes administraciones nacionales y supranacionales competentes en materia penal y que culminó con el desarrollo del principio de disponibilidad, y otra, más cercana en el tiempo, en la que la garantía del respeto a los derechos fundamentales de los ciudadanos y entre ellos, destacadamente, los de intimidad y protección de datos de carácter personal, ha comenzando paulatinamente

---

«La protección constitucional de los datos de comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a intimidad a la luz del uso de las nuevas tecnologías», en *La protección jurídica de la Intimidad*. Ed. Iustel. Madrid, 2010, pp. 45 y ss. o por mí mismo, en GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas?..»., cit. ant., p. 46.

a reclamar el papel que le corresponde y deberían haber tenido, desde un primer momento, en dicha regulación.

Esta segunda fase ha tenido, sin duda, en la aprobación del Tratado de Lisboa un hito fundamental, pero, por el momento y pese a lo declarado, tanto en dicho Tratado como en el Programa de Estocolmo o en la Agenda Digital para Europa, solo ha dado lugar a la elaboración de un proyecto de Directiva que resulta, como hemos visto, «extremadamente decepcionante» en términos de garantías.

Es precisamente, en este momento, cuando la emisión de la anteriormente comentada Sentencia del Tribunal Europeo de Justicia ha venido a aportar un pequeño rayo de esperanza en tan oscuro y decepcionante panorama normativo, ya que no solo ha dejado completamente claro que las limitaciones de los derechos a la intimidad o a la protección de datos de las personas que se creen para prevenir, investigar o reprimir delitos graves, solo resultarán legítimas en la medida en que se establezcan para perseguir tal fin y no otro, y queden limitadas a las que resulten estrictamente necesarias para conseguirlo, sino que, además y al mismo tiempo, también ha señalado que tendrá que ser el regulador europeo que implante tales restricciones, y no el nacional, quien habrá de definir y establecer los criterios o elementos objetivos que tendrán que garantizar que las mismas no sobrepasen las barreras de lo que es estrictamente necesario hacer para alcanzar dicha finalidad.

Los efectos que estas declaraciones judiciales han de tener sobre la materia que nos ocupa son, a nuestro modo de ver, extremadamente relevantes.

Así, por ejemplo resulta evidente que, una vez que el Tribunal Europeo de Justicia ha señalado, de forma tajante, que será precisamente la persecución de los fines penales señalados y no la de otros posibles objetivos o motivos[52], la que podrá

[52] En este sentido resulta interesante destacar que algunos autores, como TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. señalan que lo que impide que el proyecto de Directiva para la protección de datos personales en los tratamientos con fines de prevención y represión penal de la que venimos hablando, contemple al consentimiento como posible causa de autorización del tratamiento de dichos datos, será que la existencia relación de subordinación existente entre el titular de los datos y la administración que se encarga de esta materia, hará inviable que dicho el consentimiento emitido por el ciudadano pueda tener efectos jurídicos, atendiendo a lo que vendrá a establecer el nuevo Reglamento General de Protección de datos que se tramita de forma paralela a dicha Directiva, por no haberse emitido en una situación de verdadero equilibrio, en op. cit. ant., p. 135. No creemos, sin embargo, que ello sea del todo correcto, ya que dicha afirmación se sustenta en la existencia de una relación de sometimiento o subordinación del ciudadano ante la administración que no se ajusta a los parámetros conforme a los que esta última deba actuar en un verdadero Estado democrático y de Derecho. En realidad, en los Estados realmente democráticos el ciudadano no está para servir a la administración, sino la administración para servir al ciudadano, siendo precisamente dicho hecho el que impide que la

legitimar el régimen excepcional y las restricciones de derechos que se permiten en los tratamientos de datos personales de los que nos venimos ocupando, se obliga al regulador europeo a revisar tanto la normativa vigente, como la que pretenda crear en el futuro en relación a los mismos, para garantizar que dichas normativas excluyan cualquier posibilidad de que su absolutamente excepcional regulación pueda ser utilizada para efectuar tratamientos con fines distintos de los estrictamente penales, ya que ello evidentemente llevaría a que tales tratamientos alternativos se efectuasen empleando algunas restricciones de derechos fundamentales que, si bien podrían resultar necesarias y proporcionadas en relación a la persecución de finalidades penales, no tendrían por qué serlo con respecto a estos nuevos y alternativos objetivos.

Habrá pues, que revisar, incluso antes de su aprobación, tanto el proyecto de Directiva relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves[53], como la ya citada propuesta Directiva de protección de datos personales en los tratamientos realizados con fines penales, que en estos momentos se tramitan en el seno de la UE, con el fin de garantizar que sus articulados excluyan cualquier posibilidad de que sus excepcionales prescripciones puedan utilizarse para perseguir fines diversos a los puramente penales; pero también, y por otra parte, habrá que comprobar en profundidad la numerosa normativa europea vigente relativa a los tratamientos de datos personales con finalidades penales y que, no lo olvidemos, se pretende dejar inalterada tras la aprobación de dichas Directivas, para evitar que

---

administración pueda los derechos de las personas, salvo que ello resulte estrictamente necesario para perseguir un fin legítimo y de interés general. En concreto, y en el caso que nos ocupa las restricciones de derechos establecidas en la Directiva se sustentarían en la necesidad de posibilitar las investigaciones de delitos, siendo dicho hecho y no la relación de subordinación existente entre ciudadano y Estado, la que permitirá que la administración pueda obtener y procesar los datos del primero sin contar con su consentimiento, lo que evidentemente en modo alguno supondrá, frente a lo que sostienen TINNEFELD, M. T./ BUCHNER, B. /PETRI, T. que las administraciones no puedan e incluso tengan que contar con dicho consentimiento para tratar los datos de los ciudadanos para fines diferentes de los puramente penales.

[53] Esta propuesta de Directiva [COM (2011) 32 final], de 2 de febrero de 2011, conocida como por la propuesta de Directiva PNR, como consecuencia del acrónimo de la denominación inglesa *Passanger Name records*, y que trata de armonizar las diferentes normativas estatales referidas a los tratamientos de los datos de los pasajeros para luchar contra el terrorismo, ha recibido múltiples críticas tanto doctrinales, como del propio Grupo del artículo 29 o el SEPD, lo que, como señala KAINER, F., ha llevado a que su posible aprobación haya sido parada, por lo menos por el momento, por el Parlamento europeo, en «Strafrecht im Raum der Freiheit, der Sicherheit und des Rechts. Entwicklung und Umsetzungsprobleme des europäisierten Strafrechts in Deutschland» en Eur-Bei, 87, 2013, p. 108. Sobre los problemas de todo tipo que este texto normativo presenta, véase lo comentado, por ejemplo, por PEYROU, S., op. cit. ant., pp. 160 y ss.

ninguna de sus prescripciones pueda permitir, por ejemplo, que las autoridades receptoras de los datos personales enviados desde otro Estado miembro, para facilitar una investigación penal, puedan utilizarlos para fines diferentes de los puramente penales, simplemente porque las autoridades del Estado emisor se lo hubiese autorizado[54].

Lo lógico, a nuestro modo de ver, para acabar con todo este despropósito normativo y para dar, al mismo tiempo, cumplimiento a lo exigido por el Tribunal Europeo de Justicia, será convertir a la nueva Directiva de protección de datos personales en esta clase de tratamientos en una norma general, de aplicación a todos los sistemas destinados a cumplir con fines de prevención o prevención de delitos, que garantice, entre otras cosas, que ninguno de ellos se puedan utilizar para fines diferentes de aquellos que legitimaron su creación, esto es, tal y como expresamente afirma el artículo 1 de la propuesta de Directiva que venimos comentando, para la *«… prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales»*.

Para ello, se debería modificar lo establecido en los artículos 7 y 59 de dicha propuesta. Pero también y por otra parte, sería conveniente que se regulase, de forma específica, mediante la creación de normas especiales, adecuadas y completamente autónomas de las referidas a los propiamente penales, los tratamientos de datos realizados con fines no penales que pudiesen necesitar del establecimiento de determinadas excepciones al régimen general de protección de este tipo de datos, para poder cumplir con la finalidad para la que se realizasen (p. ej. los destinados a la

[54] La trascendencia de esta cuestión ha quedado, de hecho, reflejada en algunos casos concretos que ya se han planteado, como el que se presentó cuando el Comité Olímpico Nacional Italiano solicitó que al Juzgado de instrucción núm. 31 de Madrid le hiciese llegar las muestras de sangre que había recogido en uno de los registros domiciliarios que se realizaron en el marco de la denominada «Operación Puerto», o cuando poco después fue la propia Federación española de ciclismo la que solicitó su entrega a efectos de tramitar los correspondientes expedientes administrativos sancionadores contra los sujetos que se vieron envueltos en este conocido caso de dopaje, sin llegar, sin embargo, a tener responsabilidad penal por ello (los propios deportistas que utilizarían las sustancias ilegales). Pese a lo contradictorias que han resultado hasta el momento las resoluciones emitidas por nuestros tribunales con respecto a este tipo de casos, creemos que hay que entender, como de hecho hacen COLOMER HERNÁNDEZ, I. en «La transmisión y cesión de datos personales obtenidos en un proceso penal a un procedimiento sancionador por dopaje», en *RDDE* 2013, pp. 32 y ss. o CORTÉS BECHIARELLI, E., op. cit. ant., pp. 219 y ss., que los indicios o pruebas que se obtienen vulnerando legítimamente derechos fundamentales, como la inviolabilidad domiciliaria, el secreto de las comunicaciones o el propio derecho de protección de datos de carácter personal, por haberse recopilado para realizar una investigación criminal, nunca deberían poder usarse para investigar y, en su caso, sancionar unos hechos que no tuviesen dicha condición, esto es, para investigar y sancionar, por ejemplo, una mera infracción administrativa, por muy grave que ésta fuera.

persecución y sanción de infracciones administrativas, a la recaudación de impuestos o aranceles o a la salvaguarda de algún derecho de los ciudadanos).

Todo ello, plantea, sin duda, un reto reformador enorme para el regulador europeo; reto que, además, se verá incrementado como consecuencia de que dicho regulador también estará obligado, atendiendo a lo establecido en la comentada Sentencia del TEJ, a revisar por completo tanto el proyecto de Directiva del que venimos hablando, como el resto de normas reguladoras de los diferentes sistemas de tratamiento de datos con fines penales que ha creado y pretenda crear en el futuro, para garantizar que sean sus articulados, y no los de las normativas nacionales que los traspongan, los que realmente definan los plazos, límites y condiciones que habrán de garantizar que las restricciones del derecho fundamental a la protección de datos personales que impongan nunca y bajo ninguna circunstancia puedan ir más allá de las que resultaría estrictamente necesario aplicar, para que tales sistemas puedan cumplir con la finalidad para la que se crearon, la de prevenir, investigar, perseguir y sancionar los delitos graves que se puedan llegar a cometer[55].

[55] Entendemos en tal sentido, que lo establecido por la comentada Sentencia del TEJ obligará, entre otras cosas, a replantearse si todas las restricciones de derechos que define y limita la citada propuesta de Directiva, pueden aplicarse con independencia de la gravedad de la infracción penal con respecto a la que se aplique, o debe definirse un mínimo de gravedad, posiblemente atendiendo a la posible pena abstracta prevista para la infracción en cuestión, que garantice que tales limitaciones solo se puedan aplicar con respecto a la persecución o represión de infracciones que resulten realmente graves. Por otra parte, la comentada Sentencia también obligará a revisar el sistema de transmisión a terceros países establecido por los artículos 33 y siguientes de la propuesta y a que haya de replantearse lo establecido en sus artículos 15 y 16, con respecto a las restricciones de los derechos de rectificación y supresión de datos personales de los ciudadanos, ya que tales preceptos deberían fijar de forma clara los criterios objetivos que servirían para garantizar que dichos derechos solo se vean limitados en los casos y en la medida en que resulte estrictamente necesario hacerlo, para alcanzar los fines de investigación y represión penal perseguidos por su tratamiento, no pudiendo quedar la fijación de tales criterios, tal y como pretende el actual proyecto, por lo menos en relación a la segunda de las cuestiones planteadas, exclusivamente en manos de la decisión de los reguladores estatales. En la misma línea, el comentado texto normativo tampoco podrá dejar completamente en manos de la regulación de los países miembros la determinación del distinto régimen que se habrá de otorgar a cada una las categorías de datos que los artículos 5 y 6 de la propuesta diferencian en atención a su exactitud, fiabilidad y el carácter del sujeto al que estén referidos (sospechoso, condenados, víctimas, testigos, etc.), sino que habrá de fijar su correspondiente régimen jurídico y las posibles limitaciones a los derechos que el mismo pueda suponer con respecto a los derechos de tus titulares (p. ej. innecesariedad del consentimiento del titular para su recolección, restricción al derecho a la información, denegación del derecho de cancelación, etc.), atendiendo a la especifica utilidad y relevancia que cada una de dichas clases de datos tendría, según su características y procedencia, en la prevención y persecución de delitos. En este sentido, el regulador europeo debería, a nuestro modo de ver, tener muy presente lo establecido por la Sentencia de 4 diciembre de 2008 del Tribunal Europeo de Derechos Humanos, referida al caso S. y *Marper vs Reino Unido*. En esta Sentencia, el referido Tribunal afirmó que el almacenamiento de las huellas dactilares, de muestras celulares y del perfil genético con fines de investigación criminal de personas que, como los demandantes en dicho procedimiento, ya habían sido absueltos respecto a los casos penales que motivaron la recolección de las pruebas suponía un desproporcionado e innecesario sacrificio de sus derechos fundamentales a la

Será, sin duda, un reto reformador formidable, pero también, y a nuestro modo de ver, uno que el regulador europeo habrá necesariamente de afrontar si realmente pretende crear un «sistema de justicia penal europeo integrado».

Para hacerlo, tal y como en su día señaló VOGEL, resulta imprescindible que todos los Estados integrados en tal sistema puedan colaborar entre sí sobre la base de la confianza y el reconocimiento mutuos, lo que exigirá que todos ellos deban poder estar seguros en que el resto respetarán los derechos humanos de todas las personas, con independencia de su nacionalidad[56]. Esta exigencia convierte, sin duda, al respeto a dichos derechos, y entre ellos, el referido a la protección de datos, no en un obstáculo o una rémora para la posible creación e implantación de una política criminal europea capaz de luchar contra las modernas formas de criminalidad inter- o transnacional, como la delincuencia informática, la económica, la medioambiental o incluso, el temible terrorismo[57], sino, precisamente, en uno de los elementos configuradores básicos de la «cultura penal común» a todos los países de la UE, que se requiere para que todos ellos, pese a las evidentes y profundas diferencias que existen entre sus respectivas tradiciones y sistemas jurídicos, puedan llegar a

intimidad y a la protección de datos de carácter personal, por dar lugar a que el almacenamiento de dichos datos pudiese tener una duración que excedería de lo estrictamente necesario para conseguir las finalidades para los que los datos se habían registrado. Este hecho debería ser tenido muy en cuenta por el regulador europeo a la hora de establecer en la comentada Directiva el concreto tratamiento de los datos personales deberían recibir, atendiendo a su concreta procedencia, del mismo modo que debería hacerlo la todavía vigente normativa española en la materia, la LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir de ADN, que tendría que evitar que los datos de los sospechosos no imputados se puedan retener, como permite hacerlo su artículo 9, hasta que transcurra el periodo de prescripción del delito para cuya investigación se recabaron. Esto último resulta del todo inadmisible, como señalan, por ejemplo, HOYOS SANCHO, M., «Profundización en la cooperación transfronteriza en la Unión Europea:…», cit. ant., p. 179 o por CARUSO FONTÁN, V., «Bases de datos policiales sobre identificadores obtenidos a partir del ADN y derecho a la intimidad genética», en *Foro*, vol. 15, núm. 1 (2012), pp. 163 y ss., quienes, precisamente por ello, consideran que todos estos datos deberían ser eliminados en el mismo momento en que se constate que no se han reunido elementos suficientes para proceder al enjuiciamiento del hecho cuya investigación motivó su captación. No son, por tanto, pocas las cuestiones que el regulador comunitario debe replantearse y resolver tanto a la hora de revisar tanto esta Directiva, como el resto de normas reguladoras de los procesamientos de datos personales con fines penales, lo que, sin duda, incrementa aún más la magnitud del reto reformador que el TEJ le ha exigido que comience a afrontar.

[56] VOGEL, J., «Cooperación penal: cinco tendencias. Cinco propuestas para una acción futura», cit. ant., pp. 158 y ss.

[57] No le falta, por tanto, razón a AIXALA, A. cuando afirma que existe *«… un verdadero European way of fighting terrorism, distinto y mucho más eficaz y eficiente que el estadounidense»*, caracterizado por «*combatir el terrorismo con la ley en la mano y en el marco del Estado de Derecho*. Op. cit. ant., 55, lo que, sin embargo, no nos puede hacer olvidar que también en seno de la Unión se han producido tensiones securitarias ante el fenómeno terrorista que deben ser corregidas lo antes posible, para garantizar el más absoluto respeto a los derechos fundamentales.

implantar y seguir la política criminal europea que se necesita para poder luchar coordinada y eficazmente contra tales fenómenos criminales[58].

El reto para la política criminal europea, por tanto, está ya planteado. El camino para afrontarlo, por lo menos, en lo que se refiere a los tratamientos de datos personales realizados con fines de prevención, investigación y sanción de delitos graves, lo ha trazado el Tribunal Europeo de Justicia. Solo resta entonces que regulador europeo lo entienda y comience, de una vez por todas, a asumir la función que está llamado a desempeñar en ese Espacio Único, no solo de Seguridad, sino también de Libertad y Justicia, que la Unión Europea pretende llegar a ser.

[58] QUINTERO OLIVARES, G. / GONZÁLEZ CUSSAC, J. L., «Sobre una política criminal común europea», en *La adecuación del Derecho penal Español al ordenamiento de la Unión europea. La política criminal europea.* Ed. Tirant lo Blanch, Valencia, 2009, pp. 39 y ss.

## 6.BIBLIOGRAFÍA


ACED FÉLEZ, E., «Principio de disponibilidad y protección de datos en el ámbito policial» en <http://noticias.juridicas.com> (últ. vis. 11-3-2014).

APARICIO SALOM, J., *Estudio sobre la protección de datos*. Ed. Aranzadi, Cizur Menor, 2013.

AIXALA, A., «La estrategia de la UE ante el terrorismo internacional y la defensa de los derechos y libertades», p. 51, en <http://www.iuee.eu/pdf-publicacio/1/jpjdqoe8lrscpmve8of8.pdf> (últ. vis. 16-4-2014).

BLANCO QUINTANA, M. J., «La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales», en *BMJ*, 2013.

CARUSO FONTÁN, V., «Bases de datos policiales sobre identificadores obtenidos a partir del ADN y derecho a la intimidad genética», en *Foro*, vol. 15, núm. 1 (2012).

COLOMER HERNÁNDEZ, I., «La transmisión y cesión de datos personales obtenidos en un proceso penal a un procedimiento sancionador por dopaje», en *RDDE* 2013.

CORTÉS BECHIARELLI, E., *El delito de corrupción deportiva.* Ed. Tirant lo Blanch, Valencia 2012.

FERNÁNDEZ OGALLAR, B., *El Derecho penal armonizado de la Unión europea.* Ed. Dykinson. Madrid, 2014.

FRIGOLS I BRINES, E., «La protección constitucional de los datos de comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a intimidad a la luz del uso de las nuevas tecnologías», en *La protección jurídica de la Intimidad*. Ed. Iustel. Madrid, 2010.

GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», en *Revista General de Derecho penal*, núm. 19, 2013, pp. 4 y ss., en <http://www.iustel.com/> (últ. vis. 20-4-2014).

GÓMEZ-JARA DÍEZ, C., «Constitución europea y Derecho penal: ¿Hacia un Derecho penal Federal europeo?», en *Derecho penal y política transnacional*, Ed. Alitier, Barcelona, 2005.

GONZÁLEZ LÓPEZ. J. J., «La retención de datos de tráfico de las comunicaciones en la Unión europea: Una aproximación Crítica», en *La LEY* núm. 6456, 2006, en <www.laley.es> (últ. vis. 10-5-2012).

GONZÁLEZ MURUA, A. R., «El supervisor Europeo de protección de datos ante la revisión del marco jurídico de la protección de datos. Especial referencia a las reformas en el seno del espacio de libertad, seguridad y justicia», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013.

GUICHOT, E., *Datos personales y administración pública,* Ed. Aranzadi, Cizur Menor (Navarra) 2005.

HOYOS SANCHO, M., «Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos», en *Espacio europeo de libertad, seguridad y justicia: Últimos avances en cooperación judicial penal*. Ed. Lex Nova. Valladolid, 2010.

KAINER, F., «Strafrecht im Raum der Freiheit, der Sicherheit und des Rechts. Entwicklung und Umsetzungsprobleme des europäisierten Strafrechts in Deutschland» en *Eur-Bei*, 87, 2013.

MAPELLI MARCHENA, C., *El modelo penal de la Unión europea*. Ed. Aranzadi, Cizur Menor, 2014.

NIETO MARTÍN, A., «Posibilidades y límites de la armonización del Derecho penal nacional tras Comisión v. Consejo. (Comentario a la STJCE, asunto C-176/03, de 13-9-2005)». *REDE* núm. 17, 2006.

OERMANN, M., *Individualdatenschutz im europäischen Danteschutzrecht*. V Centauros, Freiburg. 2012.

ORTIZ PRADILLO, J. C., «Tecnología *versus* Proporcionalidad en la investigación Penal: La nulidad de la ley Alemana de conservación de datos de tráfico de las comunicaciones electrónicas», en *La Ley Penal* núm. 75, 2010, en <www.laley.es> (últ. vis. 2-5-2012).

PARIENTE DE PRADA, I., *El Espacio de libertad, Seguridad y justicia: Schengen y protección de datos.* Ed. Azanzadi. Cizur Menor, 2013.

PEYROU, S., «Algunas reflexiones sobre la protección de datos en el ELSA o la crónica de una esperanza frustrada», en *El espacio de libertad, seguridad y justicia: Schengen y Protección de datos*. Ed. Aranzadi, Cizur Menor, 2013.

QUINTERO OLIVARES, G. / GONZÁLEZ CUSSAC, J. L., «Sobre una política criminal común europea», en *La adecuación del Derecho penal Español al ordenamiento de la Unión europea. La política criminal europea.* Ed. Tirant lo Blanch, Valencia, 2009.

RECUERO, P., «La protección de datos y Schengen: Una visión desde la experiencia española», en *El Espacio de libertad, seguridad y justifica: Schengen y protección de Datos*. Ed. Aranzadi. Cizur Menor, 2013.

RODRÍGUEZ LAINZ, J. L., «El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones», en *LA LEY* núm. 6859 y 6860, 2008, en <www.laley.es> (últ. vis. 12-2-2014).

- «Secreto de las comunicaciones e intervención judicial de comunicaciones electrónicas en el marco de la Unión Europea: Derecho derivado», en *LA LEY* núm. 7373, 2010 en <www.laley.es> (últ. vis. 12-4-2014).

- «Hacia un nuevo entendimiento de gravedad del delito en la Ley de conservación de Datos relativos a las Comunicaciones Electrónicas», *LA LEY* núm. 7789, 2012 <www.laley.es> (últ. vis. 4-2-2014).

SCHÜNEMANN, B., «Forschritte und Fehltritte in der Strafrechtspflege der EU», en GA, 2004.

SANTOS GARCÍA, D., *Nociones generales de la Ley orgánica de protección de datos y su reglamento: adaptado al RD 1.720/2007 de 21 de diciembre*. Ed. Tecnos, 2012.

SILVA SÁNCHEZ, J. M., «Los principios inspiradores de las propuestas de un Derecho penal europeo. Una aproximación Crítica», *RP* núm. 13, 2004.

SOLAR CLAVO, P., «La doble vía europea en protección de datos», en LA LEY núm. 2832, 2012, en <www.laley.es> (últ. vis. 10-4-2014).

TIEDEMANN, K., «EG und EU als Rechtquellen des Strafrechts» en *Festschrift für Claus Roxin.* V Walter Gruyter. Berlín. Nueva York, 2001.

TINNEFELD, M. T./ BUCHNER, B. /PETRI, T., *Einführung in das Datenschutzsrecht.* V. Oldenburg, München, 2012.

VOGEL, J., «Política criminal y dogmática penal europea», en *RP* núm. 11, 2003.

-«Cooperación penal: cinco tendencias. Cinco propuestas para una acción futura», en *El Derecho penal de la Unión europea. Situación actual y perspectivas de futuro.* Ed. UCLM. Cuenca, 2007.

-«EU-Arbeitsweisevertrag Artículo 82 Gegenseitige Anerkennung; Angleichung», en *Das Recht der Europäischen Union.* 51 Ergänzungslieferung, V. Becks, München, 2013.

CYBERLAW by CIJIC

# TECNOLOGIAS DE INFORMAÇÃO E SEGURANÇA PÚBLICA: UM EQUILÍBRIO INSTÁVEL

# INFORMATION TECHNOLOGIES AND PUBLIC SECURITY: AN UNSTABLE EQUILIBRIUM

**ANDRÉ INÁCIO** [1]

[1] Ex-Inspetor da PJ, Auditor de Defesa Nacional, Doutorando em Direito Público.
Correio eletrónico: andrenacio@gmail.com

**SUMÁRIO: 1. INTRODUÇÃO; 2. A *ACCOUNTABILLITY* COMO GARANTE DA SEGURANÇA PÚBLICA; 3. CONCLUSÃO**


## RESUMO

As Tecnologias de informação constituem-se como base dos sistemas de informações de segurança, porém operam também como importante ferramenta ao serviço da Criminalidade Organizada. No Estado de Direito Democrático, a Segurança constitui-se como um direito fundamental dos cidadãos, uma prestação a que o Estado se encontra obrigado, sendo que os novos fenómenos criminógenos, altamente complexos *determinam o recurso a novas metodologias de prevenção e combate, mais intrusivas nos Direitos Liberdades e Garantias do Cidadão.* O recurso às tecnologias de informação (TI) pelo sistema de segurança do Estado é uma necessidade premente, devendo porém assentar num quadro legal claro e objetivo, e ser alvo de sindicância adequada.

O presente estudo concentra ideias desenvolvidas na tese de doutoramento, cuja marcação da defesa o autor aguarda, e abordará o difícil equilíbrio decorrente do recurso às novas TI no hodierno modelo de segurança do Estado, incidindo na complexa, embora crucial, componente da *intelligence* policial.



**Palavras-Chave:** *Accountability*; Criminalidade; Direitos; Informações; Segurança Pública; TI.

## ABSTRACT

Information Technologies are based on the security of information systems, but also operate as an important tool in service of Organized Crime. In a Constitutional State, Security was established as fundamental citizen's rights, a benefit to which the State is bound. The new, highly complex criminal phenomenon involves the use of new methods to prevent and combat more effectively the Rights and Freedoms guarantees the Citizen**.**

The use of IT by the state security system is urgently needed, but must be supported by a clear and objective framework. These reflections are based on the study which the author is developing in his doctoral thesis that examines the difficult balance the use of new IT in the State security model based on complex but essential component of police intelligence.

**Keywords:** Accountability; Criminality; Rights; Informations; Public security; IT.

## 1.INTRODUÇÃO

O Mundo tem vindo a sofrer mutações profundas ao longo das últimas décadas em consequência desse fenómeno *plúrimo* que se convencionou designar por "Globalização", o qual acarreta progresso, desenvolvimento mas também novos riscos e ameaças cuja natureza é cada vez mais incerta e dissimulada. As Tecnologias de Informação, vulgo TI, uma realidade indiscutivelmente omnipresente, encontram-se na vanguarda deste processo, constituindo-se como o mais recente desafio aos governos, indústria e público em geral, operando como facilitador do progresso tecnológico ou do incremento do nível de ameaça, conforme os fins para que sejam usadas.

Contemplando o conjunto dos recursos tecnológicos e computacionais destinados à produção e utilização de informação, a designação TI conglomera todas as formas de tecnologia destinadas à criação, armazenamento, troca e utilização de informação nos seus diversos formatos[2], possibilitando a inclusão das tecnologias de computação e de telecomunicações num mesmo conceito, englobando para além do processamento de dados, os sistemas de informação, a engenharia de *software* e a informática, sem descurar o "fator humano", questões administrativas e organizacionais[3]. Do *Tablet* pessoal às tecnologias de satélite, cabo e naturalmente às redes sociais, as TI constituem-se como o sustentáculo do atual modelo de vida.

Na base desse fenómeno encontra-se a disseminação da *internet,* criada inicialmente pela DARPA[4], para garantir comunicações fiáveis, mesmo em casos de ataques nucleares maciços ou de precisão e que acabou por se disseminar, impulsionando o conhecimento e o comércio globais, revelando-se também um extraordinário instrumento de aproximação entre o cidadão e a máquina governamental, permitindo a transmissão de documentos, arquivos e mensagens, bem como a consulta a repositórios remotos, desde que disponíveis em rede. Porém,

[2] A informação pode apresentar-se sob o formato de dados corporativos, imagens, vídeo, áudio, multimédia, etc.
[3] KEEN, P.G.W. *«Information Technology and the Management Theory: The Fusion Map»*. IBM Systems Journal, 1993, v.32, n.1 p. 17 e segts.
[4] *"The Defense Advanced Research Projects Agency (DARPA) was established in 1958 to prevent strategic surprise from negatively impacting U.S. national security and create strategic surprise for U.S. adversaries by maintaining the technological superiority of the U.S. military". http://www.darpa.mil/*

simultaneamente tal ferramenta origina fundados receios relativamente à dimensão dos danos que pode causar ao cidadão e/ou ao Estado.

Ao mesmo tempo que se constituem como base dos sistemas de informações de segurança, as TI operam também como importante ferramenta ao serviço da Criminalidade Organizada[5], alimentando as redes de pedofilia, exploração sexual e tráficos das mais variadas naturezas. Também o terrorismo de pendor salafista – de que a *Al-qaeda*, e mais recentemente o auto denominado Estado Islâmico, se constituem como os "*master franchising*" –, recorre às TI com enorme sucesso, para a difusão de propaganda, recrutamento e até a comunicação entre células terroristas.

Encontrando-se as economias modernas intrinsecamente dependentes de infraestruturas criticas como as redes de transportes, de fornecimento de energia e de comunicações, as quais operam totalmente dependentes das TI, a Cibercriminalidade, assume atualmente uma dimensão de arma política, económica e militar, operando sobretudo em três grandes domínios: as telecomunicações, a que recorrem para defesa própria e dissimulação da atividade, mas também pela exploração fraudulenta desses serviços; os meios eletrónicos de pagamento, nomeadamente pela falsificação de cartões de crédito e prática de burlas no domínio do comércio na *Internet* e, por fim, o acesso ilegítimo a alvos pré-definidos para sabotagem ou obtenção de dados confidenciais.

Assim, as TI têm introduzido novas fontes de conhecimento e criado novas vulnerabilidades, exigindo maior integração dos esforços operacionais e de *inteligência* entre as agências de segurança (militares, serviços de informações, policiais, etc.), face à crescente dimensão transnacional das ameaças. Os esforços vêm sendo empreendidos por indivíduos, organizações, empresas, bem como pelos Estados, de forma individual e coletivamente, visando desenvolver capacidades de resposta adequadas às hodiernas vulnerabilidades. Consequentemente, a forma como são coligidos, analisados, aplicados e acedidos esses dados pessoais, constitui-se

[5] Conforme «*computerworld*», 15 de Março de 2013 às 09:59:43*: "Os ciberataques são uma ameaça crescente. Estão perto do topo da lista das mais graves ameaças que os EUA enfrentam, com as preocupações a rivalizarem com o terrorismo e a Coreia do Norte, disseram as autoridades de inteligência da administração do presidente Barack Obama. O diretor de segurança nacional, James Clapper, e o diretor do FBI, Robert Mueller, estavam entre os funcionários que apontaram os ciberataques como as principais ameaças durante uma audiência realizada esta semana na Comissão de Inteligência do Senado. Clapper, um general reformado da Força Aérea, disse que não viu uma "matriz mais diversificada de ameaças e desafios" para a segurança nacional dos EUA durante o seu tempo na defesa e nas comunidades de inteligência."*

como um dos riscos imanentes que importa despistar de forma isenta e segura a cada momento, acautelando hipotéticas violações dos Direitos Liberdades e Garantias.

Em resposta às crescentes ameaças não tradicionais à segurança das instituições, negócios e pessoas – de que cibercrime é uma componente em franco crescimento – os governos vem implementando renovadas iniciativas visando mitigar os riscos, nomeadamente ao nível da troca de informações sobre ameaças e vulnerabilidades detetadas.

Por sua vez, também a indústria tem sido sujeita a muitas das ameaças e problemas enfrentados pelos Governos ao nível da segurança, desde a sabotagem à espionagem económica, exigindo avultados investimentos no domínio da proteção de sistemas. Na verdade, é no setor privado que muito do trabalho para melhorar e proteger o domínio digital se está a desenvolver, pela urgência de encontrar respostas seguras, pelo facto de os processos de decisão serem bem mais rápidos e eficientes do que na pesada máquina administrativa do Estado, e sobretudo porque os seus decisores, ao contrário dos políticos em geral, tem a consciência de que a sobrevivência económica dessas entidades depende do investimento na sua segurança[6]. Os setores público e privado tendem assim a incrementar parcerias[7],

[6] AMARAL, Paulo Cardoso do, «*TOP SECRET – Como Proteger os Segredos da sua Empresa e Vigiar os seus Concorrentes*», Academia do Livro, Lisboa 2008, ISBN: 978-989-8194-02-2. (Pag. 17 e 18) …"*a gestão das informações é essencial para antecipar e compreender a envolvente das organizações. Em competição a antecipação e a surpresa são o segredo do sucesso. (...) Já num cenário de ética duvidosa, as organizações têm de se proteger com técnicas da contra-espionagem, do terrorismo e da subversão. É o que se chama «segurança». Por tudo isso é importante compreender a importância dos serviços de informações e as suas atividades de produção de informações e de segurança e contras espionagem no ambiente empresarial. (...) Quando se fala em segurança está a considerar-se a existência de espionagem, terrorismo e subversão. Para todas estas três vertentes, a produção de conhecimento sobre o que se está a passar no meio envolvente e as atividades de contra-espionagem fazem parte da doutrina da segurança".*

[7] Nos Estados Unidos, essas parcerias adquiriram enquadramento legal por via do "*Cyber Intelligen*ce *Sharing Act*", vulgo CISA: "Passed House amended (04/26/2012) Cyber Intelligence Sharing and Protection Act - Amends the National Security Act of 1947 to add provisions concerning cyber threat intelligence and information sharing. Defines "cyber threat intelligence" as intelligence in the possession of an element of the intelligence community directly pertaining to: (1) a vulnerability of a system or network of a government or private entity; (2) a threat to the integrity, confidentiality, or availability of such a system or network or any information stored on, processed on, or transiting such a system or network; (3) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or (4) efforts to gain unauthorized access to such a system or network, including for the purpose of exfiltrating information. Excludes intelligence pertaining to efforts to gain unauthorized access to such a system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access. Requires the Director of National Intelligence (DNI) to: (1) establish procedures to allow intelligence community elements to share cyber threat intelligence with private-sector entities and utilities, and (2) encourage the sharing of such intelligence. (…)" disponível em: https://www.congress.gov/bill/112th-congress/house-bill/3523

visando aumentar a segurança de sistemas e infraestruturas, partindo para tal das lições aprendidas ao longo da última década em matéria de ameaças.

A dimensão da ameaça ultrapassa o âmbito nacional, pelo que a UE enquanto coletividade de Estados com fins comuns, vem desenvolvendo políticas comuns[8] nesta área. *Lord Robertson*, ex-Secretário-Geral da NATO[9], observou que a Europa "*...acordou coletivamente para a importância da recolha de informações e de partilha...*" e que a própria natureza da ameaça coletiva, bem como para uma nação em particular, mudou dramaticamente, em grande parte devido aos avanços na tecnologia. Hoje, muito do que fazemos tem lugar no domínio cibernético, sendo que a *inteligência* deve operar com base num leque maior de fontes de informação e técnicas adequadas, combinadas com o aumento da velocidade com que os eventos ocorrem.

É responsabilidade máxime do Estado controlar – no sentido de "assegurar da legalidade de" – os mecanismos de recolha, tratamento e utilização de informação, asseverando a necessária reserva da privacidade do cidadão e o direito à informação, ao mesmo tempo que tutela o bem comum, impedindo que a máquina administrativa e/ou judicial passem a controlar a vida das pessoas ou, evitando que se tornem tão legalistas que percam a noção do real e, na ânsia da defesa dos direitos do individuo de forma singular, ignorem a proteção de direitos fundamentais, também eles constitucionalmente protegidos, de natureza coletiva. Concomitantemente cumpre-lhe desenvolver as medidas atinentes à deteção e erradicação de vulnerabilidades, face ao elevado risco de entes criminosos acederem indevidamente aos sistemas de informações estatais ou de interesse público, manipulando-os ou destruindo-os.

---

[8] A exemplo dessa preocupação a Comissão Europeia, vulgo CE, elaborou a «Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social europeu e ao Comité das Regiões» Bruxelas 24.7.2003 *COM(2013)542 final* – "Para um Sector de Defesa e Segurança Mais competitivo e Eficiente" –, documento que se assume como um plano de ação, onde se esboçam as linhas de criação da nova moldura para o desenvolvimento da cooperação Civil/Militar em matéria de indústria de Segurança e Defesa, rentabilizando os meios e dando resposta ao atual quadro de riscos e ameaças. A CE, nesse documento, exorta à criação de sinergias e regulação das relações comerciais no domínio da indústria de segurança e defesa, potenciando as valências de cada Estado membro, evitando a duplicação de esforços e acautelando a perda de direitos de propriedade intelectual, bem como, o investimento por parte de países terceiros em empresas estruturantes da defesa e segurança europeia. Importa apurar que "*novas abordagens de inteligência e capacidades são necessárias, especialmente de forma colaborativa ou conjunta, a fim de atender às necessidades de segurança coletiva da Europa".*

[9] *«Fórum Global Intelligence»* OTAN, Bruxelas, 20 e 21 de Setembro de 2012. Discurso proferido na conferência Inaugural.

## 2.A *ACCOUNTABILLITY* COMO GARANTE DA SEGURANÇA PÚBLICA

A segurança constitui-se como um valor inestimável, um pilar do Estado Social de Direito. Exige porém um equilíbrio complexo, asseverando a legalidade dos meios, na medida em que a ação do aparelho de segurança do Estado incide diretamente sobre a esfera mais restrita das liberdades fundamentais do indivíduo. Assim, a segurança desempenha um duplo papel de *"*condição*"* e "qualidade", necessários para o bem-estar individual e coletivo, tendo de ser encarado sobre um novo prisma, sem delimitações fronteiriças, temáticas, organizacionais ou outras. Tem de ser suficientemente amplo para garantir o regular funcionamento do Estado Social de Direito, no respeito pelas liberdades individuais e na defesa do interesse coletivo. Para tal, as autoridades socorrem-se de soluções inovadoras, baseadas em tecnologias emergentes, com a dupla função de poder processar em tempo útil a informação e de tentar garantir a segurança de elementos críticos de infraestruturas e ambientes de trabalho, desenvolvendo complexos sistemas de proteção, *firewall's* e antivírus, recorrendo ainda a elaborados sistemas eletrónicos de gestão de direitos. Ainda assim, a segurança dos sistemas contra acessos indevidos é uma luta permanente "do gato e do rato[10]".

As TI constituem-se como ferramentas indispensáveis à Segurança do Estado, a que recorrem desde os Serviços de informações aos corpos de polícia criminal e autoridades judiciárias, consubstanciando novas metodologias de investigação, cooperação policial e formas rápidas e eficientes de obter dados, que podem constituir meios de investigação e probatórios decisivos. *El tratamiento de la información es una herramienta fundamental en el desarrollo de la labor de protección de la seguridad pública que llevan a cabo las Fuerzas y Cuerpos de Seguridad"* [11].

São exemplos de TI aplicadas à Segurança e Justiça a vídeo vigilância, as escutas ambientais, as interceções telefónicas, a localização por satélite e sobretudo, concentrando, processando e disponibilizando toda a informação sobre cada alvo, os sistemas de informações, mais concretamente as bases de dados. Aí se destacando o

[10] Recorde-se como exemplo a referência constante no *«Relatório Anual de Segurança Interna»*, vulgo RASI, documento emitido pelo Secretário-geral do Sistema de Segurança Interna, na sua edição referente ao ano de 2010 onde se assume a deteção de tentativas de acesso ilegítimo a bases de dados governamentais, nomeadamente por Serviços de Informações de países terceiros.

[11] GUERRA, Amadeu*«El Tratamiento de Dados Personales Para Fines de Prevención e Investigación Criminal.»,* Revista Espanhola de Proteción de Datos, nº 7, Julio-Junio 2009-2010, pag. 11.

Sistema Integrado de Informação Criminal, vulgo SIIC[12] e a Base de dados de ADN[13]. Mas, o exemplo que melhor ilustra a preocupação subjacente à opção pelo tema são as recentemente implementadas bases de dados supostamente destinadas à prevenção e repressão de atentados terroristas, das quais se constituem como controverso exemplo, as desenvolvidas no âmbito da segurança da aviação civil contra actos de interferência ilícita, cujo objeto são os dados contidos nos registos de identificação dos passageiros (*PNR – Passenger Name Records)*. Tais bases de dados constituem-se como autêntico vértice da pirâmide da informação de segurança, por visarem a deteção de perfis criminosos[14]. Tal questão tem vindo a sofrer uma significativa evolução na última década, sendo relevante citar, numa perspetiva histórica, o parecer 8/2004 do Grupo de Proteção de Dados do Artigo 29.º[15]*".*

Constituindo-se o recurso às novas tecnologias em geral e às bases de dados em particular como instrumentos fundamentais da segurança do Estado e do cidadão, importa porém garantir o equilíbrio indispensável nos mecanismos de recolha,

[12]SIIC, Sistema Integrado de Informação Criminal, previsto no art.º 8º da *«Lei de Organização e Investigação Criminal» (LOIC), Lei 49/2008 de 27 de Agosto,* onde se pode ler: *"*1- *O dever de cooperação previsto no artigo anterior é garantido, designadamente, por um sistema integrado de informação criminal que assegure a partilha de informações entre os órgãos de polícia criminal, de acordo com os princípios da necessidade e da competência, sem prejuízo dos regimes legais do segredo de justiça e do segredo de Estado. 2 - O acesso à informação através do sistema integrado de informação criminal é regulado por níveis de acesso, no âmbito de cada órgão de polícia criminal. 3 - As autoridades judiciárias competentes podem, a todo o momento e relativamente aos processos de que sejam titulares, aceder à informação constante do sistema integrado de informação criminal. 4 - A partilha e o acesso à informação previstos nos números anteriores são regulados por lei."*

[13]Em Portugal a *«Lei 5/2008 de 12 de Fevereiro»,* criou a base de dados de perfis genéticos de ADN para fins de investigação criminal e civil.

[14] A análise de perfis criminais constitui-se, na sua génese como uma técnica forense, auxiliar da investigação Criminal, a qual a partir dos indícios e vestígios resultantes da análise de uma cena de crime e da vítima, procura identificar padrões comportamentais com o objetivo de predizer o comportamento, as características de personalidade e os indicadores sócio demográficos do autor, diminuindo o leque de suspeitos. Na sua atual dimensão, a técnica do *profiller* está já a roçar o limiar da ficção, pretendendo antecipar potenciais comportamentos criminosos com base no tratamento da informação disponível sobre os passageiros. Sobre os perfis criminais ver SOEIRO, Cristina, *«Os Perfis Criminais: Contornos e aplicabilidade de uma Técnica Forense»,* Ousar e Investigar – Revista de Reinserção Social e Prova, nº 4, Lisboa 2009, pag. 9-20. No que respeita à ficção DICK, Phillipp K. *"Relatório Minoritário",* imortalizado no cinema, em 2002 por Steven Spielberg, com Tom Cruise no principal papel.

[15] *Grupo de Trabalho de Proteção de Dados do Artigo 29.º, parecer 8/2004.* Trata-se de um orgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições são descritas no art.º 30º *da Diretiva 95/46/CE e no art.º 15º da Diretiva 2002/58/CE. "(...)Nos termos da legislação norte-americana, o Serviço das Alfândegas e Proteção das Fronteiras dos Estados Unidos (Customs and Border Protection – CBP) recebe informação sobre viagens e reservas, conhecida como dados contidos nos registos de identificação dos passageiros ou PNR, relativa a passageiros de voos entre a União Europeia e os EUA. O CBP compromete-se a utilizar estes dados contidos nos PNR para fins de prevenção e combate ao terrorismo e outros crimes transnacionais graves. O PNR pode incluir informação fornecida durante o processo de reserva ou proveniente de companhias aéreas ou agências de viagens. A informação será retida durante três anos e meio, pelo menos, podendo ser partilhada com outras autoridades*

tratamento e troca de informações, nas diversas modalidades de bases de dados no seio da organização Policial e do aparelho do Estado, impedindo atropelos ao respeito pelos princípios da *necessidade* e da *competência*, impondo-se a salvaguarda dos Direitos Fundamentais dos Cidadãos, constitucionalmente consagrados, o que apenas pode ocorrer sobre escrutínio democrático, por via das instituições de controlo, assegurando a *accountabillity*.

Atualmente, as próprias fronteiras geográficas são essencialmente referenciais no que concerne à atuação da criminalidade organizada e especialmente violenta, o que conduz à necessária implementação de sistemas em rede de informação policial, cujo controlo efetivo da legalidade do seu âmbito e fins de utilização se revela forçosamente mais difícil. *"A abordagem clássica em matéria de segurança exigia uma compartimentação rigorosa do ponto de vista organizacional, geográfico e estrutural das informações em função da sua sensibilidade e categoria. Esta abordagem deixou de ser realmente viável no mundo digital, uma vez que o processamento da informação está fragmentado."* [16]

Entretanto as parcerias público-privadas não se esgotam ao nível da indústria, e é aí que a *accountabillity* tem de funcionar de forma exemplar. Os custos e os limites legais impostos à Administração têm paulatinamente conduzido a uma política de parcerias também no domínio da recolha, gestão e tratamento de dados, conferindo poderes a entidades privadas no desempenho da segurança pública, nomeadamente no que respeita à gestão de sistemas de informação, o que acarreta genuinamente preocupações acrescidas em termos de controlo da legalidade. Conforme resultou da divulgação pública pelo ex-Analista da NSA *Edward Snowden*[17], existem graves riscos na relação com o setor privado devido ao desenvolvimento de parcerias que permitem ao Governo obter por via de entidades privadas, informações de segurança através de métodos a que estaria constitucionalmente inibido por via oficial.

O corolário dos riscos para a Democracia e o Estado de Direito será seguramente o Sistema designado por *National Surveillance State, vulgo NSS, o qual* conforme

[16] *«Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões», COM(2000)890 final.* Bruxelas 26.1.2001 (pag.6).
[17] SNODWDEN, Edward, ex-agente da CIA que expôs a mega operação de espionagem levada a cabo pelos EUA através da Agência Nacional de Segurança (NSA)

*Jack M. Balkin*[18], tem vindo a ser desenvolvido pelos Estados Unidos, desde os finais do século XX. Constituído por um conjunto de elaboradas bibliotecas digitais, interligadas entre si e destinadas ao apoio à decisão, que recolhem, analisam e cruzam informação sobre cidadãos, assume-se como uma nova forma de *governance* em matéria de informações, permitindo a recolha, análise e cruzamento de informações sobre indivíduos não apenas nos Estados Unidos mas também no resto do mundo. A fundamentação doutrinal de tal sistema assenta na relevância da identificação antecipada dos problemas, permitindo repelir potenciais ameaças e prestar apoio social às populações. Assim o NSS é patenteado como um caso especial de "Informações de Estado", visando identificar e resolver questões de *governance,* no interesse das populações.

Criada e desenvolvida com fundamento na ameaça terrorista, esta ferramenta encontra-se maioritariamente nas mãos de entidades privadas, consequência do aproveitamento por parte do Governo da evolução da tecnologia de informação e das parcerias com o sector privado, privatizando áreas fundamentais da segurança nacional, com consequentes perigos para a liberdade e cidadania. De facto, o recurso a tal sistema permite uma via paralela de aplicação das regras de prevenção contornando as garantias fundamentais constantes do "*Bill of Rights*[19]". Ao mesmo tempo, e resultado da sua eficácia, esta nova ferramenta tenderá a sobrepor-se, por pressão política, aos restantes sistemas na aplicação da lei geral, na resolução dos problemas de segurança diários, conduzindo a que a Segurança e a Justiça, até por questões de redução de custos, sejam cada vez mais delegadas em entidades privadas.

Como se compreende, são enormes os riscos resultantes da promíscua relação com o poder privado, permitindo às entidades oficiais aceder a informação por vias a que estariam constitucionalmente inibidos por via oficial. Simultaneamente, essas empresas privadas ficam de posse de informação sobre os cidadãos, permitindo a elaboração de "*ratings*" em tecnologia de informação, identificando possíveis clientes e afastando os que considere indesejáveis.

[18] BALKIN, Jack M., *«The Constitution in The National Surveilllance State»,* Minnesota Law Review, Vol. 93 Nº 1. 2008 Yale Law School Working Paper Nº 168
*papers.ssrn.com/sol3/papers.cfm?abstract_id=1141524*
[19] «*Bill of Rigths*», nome pelo qual as dez primeiras emendas à Constituição dos Estados Unidos são conhecidas.

Assim, o NSS veio colocar graves questões em sede de modelo de Estado de Direito, constituindo-se como o corolário dos excessos que importam prevenir, exigindo novas estratégias de preservação dos valores constitucionais e do governo democrático. Os Direitos Fundamentais têm de ser considerados com a sua verdadeira dimensão, eles são Pilares do regime e não instrumentos de governos.

## 3.CONCLUSÃO

As TI vieram para ficar, sendo impossível conceber um modelo de progresso e desenvolvimento à margem dessa tecnologia. Já a segurança do Estado, das empresas, da comunidade e do próprio cidadão passa pelo conhecimento. As informações são inevitáveis e legitimas, desde que necessárias e úteis, sendo que a insuficiência de informações conduz ao sentimento de isolamento e consequentemente ao medo. Acarreta porém garantias de escrutínio democrático e institucional dos procedimentos atinentes às informações em geral e às bases de dados em particular, garantindo o enquadramento institucional e organizacional apropriado. O mesmo é dizer, encontrar-se alicerçado num regime legal e num sistema de fiscalização que permita definir de forma objetiva o que se recolhe e trata; porque se recolhe e trata; como se recolhe e trata; e por último, quem acede e com que fim. Neste modelo de *accountabillit*y cumpre aos órgãos de fiscalização desenvolver um duplo papel, controlando a atuação dos sistemas de informações e garantindo a legalidade da sua atuação, contribuindo assim para que a população confie no sistema de segurança do Estado. Esta questão é tanto mais relevante na medida em que os direitos do cidadão, perante esta "máquina", se encontram extremamente mitigados, não tendo acesso aos registos em seu nome e consequentemente vendo-se impossibilitado de exercer o "contraditório". Compete pois aos órgãos de fiscalização assegurar a legalidade e idoneidade do processo, evitando discricionariedades por parte do sistema.

Numa frase, importa garantir a legalidade e particularmente os Direitos Fundamentais do cidadão, na utilização dessa ferramenta indispensável à eficácia do sistema de segurança que são as informações policiais.

Cumpre ao Estado garantir que a informação recolhida, o foi pelos motivos corretos, será tratada e guardada em função dos princípios da necessidade e da

competência, sendo apenas utilizada para fins de prevenção e combate à criminalidade, e para tal, disponibilizada em função do "*princípio da necessidade do conhecer*" [20] , na exclusiva tutela da segurança da sociedade como um todo, acautelando o respeito pelos direitos de cada cidadão individualmente considerado. A tudo isto acresce o risco de acessos indevidos" às bases de dados policiais e consequente exposição pública, ilícita e difamatória, com as inerentes responsabilidades para os Estados. Ora, só um efetivo controlo democrático da atuação, permite assegurar o equilíbrio na complexa dicotomia "*dever de obter informações/respeito pelos Direitos fundamentais".*

[20] O Principio da necessidade do conhecer constitui o pilar basilar da segurança em matéria de informações. Apenas tem acesso à informação quem dela necessite de ter conhecimento de forma legalmente justificável e apenas na medida do que necessita de saber.

CYBERLAW by CIJIC

# CIBERSEGURANÇA E OBSCURANTISMO

# CIBERSECURITY AND OBSCURANTISM

**CARLOS CALEIRO** [1]

e

**ANDRÉ SOUTO** [2 3]

[1] Instituto Superior Técnico; SQIG – Instituto de Telecomunicações. Correio Eletrónico: ccal@math.tecnico.ulisboa.pt

[2] Instituto Superior Técnico; SQIG – Instituto de Telecomunicações. Correio Eletrónico: a.souto@math.tecnico.ulisboa.pt

[3] Pelo apoio financeiro, os autores estão gratos ao projeto FEDER/FCT PEst-OE/EEI/LA0008/2013 do Instituto de Telecomunicações. A. Souto agradece ainda à FCT a bolsa de Pós doutoramento SFRH/BPD/76231/2011.

**SUMÁRIO: 1. INTRODUÇÃO; 2. O PRINCÍPIO DE *KERCKHOFFS*; 3. CRIPTOLOGIA E CIBER(IN)SEGURANÇA; 4. A VULNERABILIDADE *LOGJAM*; 5. CONCLUSÕES**


## RESUMO

Com a democratização das telecomunicações e tecnologias da informação, a cibersegurança tornou-se, para além de uma preocupação global, um dos alvos mais insistentes de teorias da conspiração. Na transição de séculos de obscurantismo para o carácter universal que a segurança de informação hoje detém, tornou-se inevitável o conflito entre cibercrime e cibervigilância, e direitos fundamentais como a privacidade e a liberdade de expressão. Discutimos esta tensão colocando em perspetiva desenvolvimentos recentes, em particular a vulnerabilidade *Logjam* e o seu encaixe com revelações do caso *Snowden*, concluindo que a cibersegurança deverá sair da era da obscuridade, por via da crescente literacia científica e interdisciplinar, e tornar-se num esforço que deve ser partilhado por todos.



**Palavras-Chave:** Cibersegurança; Criptografia; Princípio de *Kerckhoffs*; Protocolo de *Diffie-Hellman*; *Logjam*.

## ABSTRACT

As a consequence of the democratic access to telecommunication and information technologies, cybersecurity has become not just a global concern but also a preferred target of conspiracy theories. Along with the transition from centuries of obscurantism to the current universality of information security issues, came an unavoidable conflict between cyber crime and surveillance, and fundamental rights like privacy and freedom of speech. We discuss this tension, putting in perspective recent developments, and in particular the recent Logjam vulnerabilities and their fit with the Snowden affair, to conclude that cybersecurity must leave the age of obscurity, through increased scientific interdisciplinary literacy, and become an effort to be shared by all.

**Keywords:** Cibersecurity; Cryptography; Kerckhoffs' Principle; Diffie-Hellman's Protocol; Logjam.

## 1.INTRODUÇÃO

Entrámos, quase sem darmos conta, na era digital. A velocidade a que os avanços tecnológicos inundam (e mudam) as nossas vidas, o tecido económico, os meios de governação, a organização política e militar dos estados, é avassaladora. Esta revolução tem um impacto bem vincado na forma como os diferentes atores se relacionam, e traz-nos para o limiar de um futuro onde a informação (e a forma como a comunicamos) é o bem mais precioso, que todos querem obter, preservar e usar em seu proveito. A cibersegurança é hoje, portanto, um tema inultrapassável, que a todos diz respeito. E se, em termos estritamente técnicos, é uma disciplina que se insere nas tecnologias de comunicação, informática, engenharia, física e matemática, a sua ubiquidade e implicações tornam-na naturalmente interdisciplinar, tocando igualmente as ciências sociais e humanas, nomeadamente a economia e o direito.

A abrangência e relevância que hoje se reconhece ao tema advêm da popularização das tecnologias de informação e comunicação, no âmbito das economias globais e abertas do final do século XX, em forte contraste com o passado. É desta rutura, nascida da conjugação dos desenvolvimentos em tecnologias de informação, do surgimento da denominada criptografia moderna, e da globalização económica, que se desenvolve (pelo menos) nas sociedades democráticas um crescente interesse científico pela cibersegurança. A segurança de informação já não é hoje um problema restrito aos estados e às organizações militares, ou à proteção de infraestruturas críticas, propriedade industrial ou fluxos de comércio internacional. A questão abrange também tudo aquilo que hoje se denomina por *internet* das coisas: o nosso automóvel, a nossa casa, os dispositivos médicos que usamos, e uma crescente quantidade de outras dimensões das nossas vidas, para além do nosso computador pessoal ou telemóvel.

No entanto, o caminho da luz nesta área de fulcral importância está ainda no seu início. A era moderna da criptografia nasce apenas no final do século XX com o trabalho seminal de *Whitfield Diffie* e *Martin Hellman* [1], que passa a possibilitar o acordo secreto de chaves criptográficas à distância e em canais de comunicação públicos. É este avanço que permite a explosão do ciberespaço, em frente de onda com a globalização das redes de comunicação e a popularização dos computadores. Os já conhecidos resultados matemáticos de *Claude Shannon* [2] sobre a

(im)possibilidade de segurança perfeita são o ingrediente final que nos traz à formulação de cibersegurança que hoje conhecemos.

Após séculos de permanência dos assuntos da segurança de informação na esfera militar e securitária, é natural que surjam conflitos com direitos fundamentais, como a privacidade e a liberdade de expressão, seja por ausência ou fraca regulamentação, excesso de zelo ou outras razões menos claras. Fenómenos como a cibervigilância, particularmente exacerbados na sequência dos atentados terroristas de Nova Iorque, EUA em Setembro de 2001 (uma discussão que se reavivou na sequência dos recentes atos terroristas de Paris, França em Novembro de 2015), ou o combate ao cibercrime, acabam inevitavelmente por conduzir a abusos, ou pelo menos a teorias da conspiração, a que casos como o de *Edward Snowden* [3] dão eco e expressão.

Em Maio deste ano, um coletivo de 14 cientistas de institutos de investigação e universidades francesas e norte-americanas descobriu e divulgou uma vulnerabilidade bastante preocupante, a que chamaram *Logjam* [4], com o potencial de comprometer uma larga percentagem das comunicações e servidores a nível mundial [5]. Este ataque coloca em causa a segurança de um dos componentes mais fundamentais da criptografia moderna - o protocolo de acordo de chaves de *Diffie-Hellman*. O ataque não determina fraquezas na matemática subjacente (tanto quanto se sabe, impoluta), mas explora uma conjugação de defeitos na sua implementação e utilização por parte dos protocolos criptográficos mais comuns. É hoje considerado (fortemente) plausível que esta vulnerabilidade fosse conhecida e explorada durante anos, pelo menos pela agência norte-americana de segurança (NSA) num seu programa de cibervigilância de massas. Claro que a emergência destes factos retira credibilidade às entidades envolvidas, para além de suscitar fundadas dúvidas sobre a eficácia da estratégia utilizada. Conhecer uma vulnerabilidade (séria) e optar, intencionalmente, por explorá-la, ao invés de a divulgar e mitigar, abre um perigoso caminho que pode permitir a exploração da mesma vulnerabilidade por terceiros, desde que bem equipados, mas quiçá pior intencionados.

Para além de vários outros casos pouco exemplares há também, felizmente, uma miríade de exemplos recentes que trazem à evidência as vantagens da clarificação. A discussão científica aprofundada e alargada destas matérias, no seio das sociedades ocidentais modernas, terá forçosamente de nos conduzir, por via da literacia sobre o ciberespaço, a um contexto onde, na ausência de soluções perfeitas, todos sejamos

abertamente corresponsáveis e ciberconscientes. Neste artigo, usaremos a descoberta da vulnerabilidade Logjam, na sua dimensão técnica e no seu impacto político, como paradigma das boas práticas a que, julgamos, estaremos inevitavelmente condenados, em defesa de um Princípio de *Kerckhoffs* generalizado (Kerckhoffs, 1883).

O artigo está estruturado da seguinte forma: na Secção 2 abordaremos, em perspetiva histórica, o conflito entre obscurantismo científico e segurança de informação, com ênfase nos bons exemplos recentes de aplicação do Princípio de Kerckhoffs; na Secção 3 daremos uma panorâmica da importância da criptologia em cibersegurança, enquadrando a sua relevância para a vulnerabilidade Logjam recentemente descoberta; consubstanciando o carácter técnico desta vulnerabilidade, a Secção 4 analisará a forma como uma conjugação de fraquezas (infeliz, ou talvez intencional) contribuiu para a vulnerabilidade em questão, bem como o papel fundamental da investigação científica na sua descoberta e mitigação; concluiremos, na Secção 5, defendendo o progresso científico, a ciberliteracia e a responsabilidade partilhada como pilares fundamentais da cibersegurança do futuro.

## 2.O PRINCÍPIO DE KERCKHOFFS

Sendo verdade que a comunicação de informação confidencial não é um exclusivo dos nossos dias, havendo exemplos conhecidos no antigo Egito com cerca de 4000 anos, é inegável que até à emergência da era digital nas últimas décadas do século XX se tratou de uma questão "apenas" relevante em contextos militares ou de soberania (e a partir do fim do século XIX também de algumas, poucas, grandes indústrias). Até há pouco mais de 50 anos atrás podemos afirmar que se vivia, globalmente, em regime de total obscurantismo no que diz respeito à segurança de informação, cujas técnicas eram do conhecimento quase exclusivo de algumas elites. Se a princípio a segurança de informação se sustentava no analfabetismo da maioria das populações, mais tarde passou a suportar-se na suposta dificuldade do comum mortal em executar corretamente operações matemáticas relativamente simples, e no obscurantismo que rodeava as técnicas utilizadas, conhecidas apenas dos iniciados. No entanto, a História foi-nos ensinando a olhar para estas questões com mais seriedade (ver por exemplo [7]).

A melhor forma de conceber sistemas criptográficos seguros era já objeto de discussão no final do século XIX, nomeadamente nos trabalhos do linguista e criptógrafo holandês Auguste Kerckhoffs [6]. Precursor da análise de boas práticas para a construção de sistemas criptográficos seguros, válidas até hoje, Kerckhoffs afirmou que a segurança dos mesmos não deve ser baseada no obscurantismo e portanto no desconhecimento das técnicas de cifra utilizadas. Em contraponto, e numa perspetiva completamente contrária, propôs que um sistema deverá ser seguro mesmo que o adversário conheça tudo sobre ele, incluindo as técnicas, o processo de cifra e até mesmo o próprio criptograma, isto é, a mensagem cifrada, ficando apenas incógnita a chave usada para cifrar.

Hoje conhecido como Princípio de Kerckhoffs, esta proposta é comummente considerada como a negação de todas as abordagens à segurança por obscuridade. Isto não significa que princípios menos transparentes de segurança de informação por obscuridade não continuem a ser usados até hoje, nem mesmo que essas abordagens sejam necessariamente menos seguras, mas a prática demonstra que há uma marcada distinção, em termos de qualidade da segurança de informação, quando os métodos propostos são publicamente discutidos, analisados e validados, e todos os detalhes de desenho dos sistemas são cuidadosamente justificados e verificados. Apesar desta evidência, ou talvez contribuindo ainda mais para salientar a sua importância, há diversos episódios relevantes que vale a pena recordar.

O papel crucial que a criptografia e a capacidade de criptanálise desempenharam no desenlace da II Guerra Mundial (ver [8] e [9]), bem como o contexto de guerra fria que se lhe seguiu, contribuíram de forma vincada para a obscuridade do tema. A criptografia foi classificada como arma de guerra pelos EUA e, a partir de 1949, a livre circulação de sistemas criptográficos foi regulada internacionalmente pelos países da OTAN ao abrigo do *Coordinating Committee for Multilateral Export Controls* (CoCom) [10].

É neste contexto que se dá a popularização das telecomunicações e tecnologias de informação, a partir da década de 1970 e no último estertor da guerra fria, no âmbito de economias globais e abertas em forte contraste com o passado. É desta rutura, nascida da conjugação dos desenvolvimentos em tecnologias de informação, do surgimento da denominada criptografia moderna e da globalização económica que se desenvolve (pelo menos) nas sociedades democráticas um crescente interesse

científico pela cibersegurança. A segurança de informação deixara de ser um problema restrito aos estados e organizações militares, ou à proteção de infraestruturas críticas e propriedade industrial, passando a abranger uma fatia muito significativa da economia mundial e da vida de todos nós.

Em 1991 dá-se um caso particularmente revelador do clima securitário que envolvia (e sempre envolverá) a segurança de informação, mas também de como a luz começava a raiar. *Phil Zimmermann*, informático norte-americano, decide disponibilizar publicamente um conjunto de implementações de sistemas criptográficos que pudessem ser utilizados pelo utilizador comum, que denominou de *Pretty Good Privacy* (PGP) [11]. Os seus programas rapidamente extravasaram as fronteiras territoriais dos EUA e *Zimmermann* acabou por ser acusado de traição. O processo foi arquivado em 1996, talvez por ser impossível conter o inevitável, e o PGP ainda hoje está disponível para quem o quiser usar [12].

Tendo ficado obsoleto por ser demasiado restritivo, na sequência do caso PGP e dado o fim da guerra fria, o controlo de importação/exportação de métodos criptográficos é hoje regulado internacionalmente pelo *Wassenaar Arrangement* [13], que substitui o CoCom a partir de 1996. Ainda assim é bom salientar, até por ser relevante para o que se segue, que praticamente até ao início do século XXI, todos os sistemas informáticos exportados pelos EUA comportavam criptografia propositadamente enfraquecida, de acordo com as normas então vigentes.

Dois organismos norte-americanos desempenham até hoje um papel particularmente importante, pela sua liderança nesta área: a *National Security Agency* (NSA), e o *National Bureau of Standards* (NBS) hoje denominado *National Institute for Standards and Technology* (NIST). É pela pressão crescente da necessidade global de dispor de sistemas de cifra robustos que é certificado pelo NBS em 1977 o *Data Encryption Standard* (DES) (National Institute of Standards and Technology, 1977), o primeiro *standard* de criptografia dita simétrica. Construído sob a custódia da NSA, o DES foi sempre severamente criticado por haver diversos elementos obscuros no seu desenho, nunca devidamente explicados, que foram dando azo a diversas teorias da conspiração sobre a possibilidade de o sistema conter vulnerabilidades não divulgadas que a NSA poderia explorar. Apesar disso, o DES foi usado intensivamente em todo o mundo, sem problemas de maior, até ser substituído por um novo *standard* em 2001. Pode até dizer-se que o escrutínio do DES ela comunidade científica desempenhou

um papel crucial nos avanços na ciência da cibersegurança das últimas décadas. Curiosamente, ou talvez como concessão inevitável ao Princípio de *Kerckhoffs*, o processo de seleção pelo NIST do novo *standard*, a cifra *Advanced Encryption Standard* (AES) [15], foi absolutamente distinto, exemplarmente aberto e profundamente escrutinado. Em 1997 realizou-se uma chamada internacional para apresentação de propostas, que foram sendo discutidas, debatidas, analisadas e escrutinadas pela comunidade internacional, ao longo de quatro anos, até ser finalmente escolhido um vencedor: a cifra *Rijndael* proposta por dois cientistas belgas. O processo repetiu-se, em 2015, para a seleção do novo *standard Secure Hash Algorithm* (SHA-3) [16], uma função de dispersão utilizada, por exemplo, em sistemas de assinatura digital.

Apesar dos bons exemplos citados e de outros, os problemas de cibersegurança não deixaram de existir, nem os princípios obscurantistas foram eliminados definitivamente, e as teorias da conspiração não pararam de crescer. Em 2013, na sequência da revelação de inúmeros segredos da NSA pelo seu ex-funcionário *Edward Snowden* [3], tornou-se público que os EUA tinham ativo um programa de cibervigilância de massas que lhes permitia analisar comunicações cifradas (quase todas, hoje em dia, mesmo que não tenhamos consciência disso). Esta perspetiva deu azo a todo o tipo de especulações sobre os mecanismos que poderiam estar a ser usados, e que iam desde a ficção científica à mistificação, passando também por algumas possibilidades mais sérias, envolvendo a inclusão de potenciais portas de escuta (*backdoors*) em *software* e *hardware* comercial de uso generalizado, ou a exploração de avanços não divulgados na matemática das cifras, ou mesmo da concepção em segredo de computadores quânticos. Finalmente, o artigo que divulga a vulnerabilidade Logjam [4, 5] vem trazer luz a esta questão, numa articulação engenhosa de pequenas vulnerabilidades que estão perfeitamente em linha com as capacidades da NSA, e que discutiremos de seguida.

## 3.CRIPTOLOGIA E CIBER(IN)SEGURANÇA

A vulnerabilidade *LogJam* enquadra-se num tipo de ataque muito sério à privacidade das comunicações. Nomeadamente, a vulnerabilidade permite violar a

segurança de uma das peças mais fundamentais da cibersegurança moderna: o protocolo de acordo de chaves de *Diffie-Hellman*. O referido protocolo permite o estabelecimento de uma comunicação privada via *internet* entre duas partes, sendo utilizado massivamente em quase todos os sistemas de comunicação que necessitem de qualquer tipo de privacidade. É através dele que as partes acordam uma chave secreta que usarão daí em diante em comunicações cifradas/privadas entre si. Sem ele, a menos que as partes se encontrem previamente, não é possível, na prática, estabelecer ligações privadas. A ideia de *Diffie* e *Hellman* está presente em quase todos os protocolos de comunicação segura, incluindo TLS, HTTPS, SSH, IPSec, SMTPS ou IKE, utilizados para estabelecer ligações remotas entre servidores e clientes, redes VPN, ou servidores de correio electrónico IMAP e POP [5]. A confiança que é depositada na segurança do protocolo de Diffie-Hellman é sustentada na firme opinião dos especialistas, que consideram estarmos cientificamente ainda muito longe de sabermos resolver eficientemente o problema do logaritmo discreto, em que o protocolo se baseia. Ou seja, a criptanálise eficiente do problema do logaritmo discreto está bastante para além do alcance do conhecimento matemático atual.

O problema do logaritmo discreto é um dos mais populares exemplos daquilo que, na criptografia moderna, se acredita ser uma função de sentido único. A designação provém do facto de, dado um valor (mensagem), ser computacionalmente simples calcular o valor da sua imagem (cifra), mas ser computacionalmente difícil inverter o processo (criptanálise) sem conhecimento adicional (sobre a chave utilizada na cifra). De acordo com a moderna teoria da complexidade computacional, isto não invalida a possibilidade de fazer criptanálise do sistema, mas implica que não possa ser feita em tempo útil para parâmetros de segurança suficientemente grandes (tamanho das chaves). Intuitivamente, uma função de sentido único pode ser comparada a uma construção Lego. Na verdade, dada uma construção já pronta, determinar o conjunto de peças que lhe deu origem é fácil (basta desmontar a construção). Contudo, dadas as peças, refazer a construção pode ser muito trabalhoso.

Para melhor compreender o protocolo de *Diffie-Hellman* é útil entender melhor o problema do logaritmo discreto: dado um número que sabemos ser uma potência

(módulo um número primo[4]) de uma certa base, determinar qual o expoente. Trata-se de um problema matemático, do domínio da álgebra e teoria de números (vide o texto introdutório [17]).

Os números inteiros (positivos e negativos) podem ser somados entre si, a operação de soma tem elemento neutro (0), e cada número inteiro *a* tem um elemento simétrico -*a* (que somado consigo dá resultado 0). Por esta razão, a estrutura $(\mathbb{Z}, +)$ é denominada um grupo, neste caso infinito. O problema do logaritmo discreto põe-se sobre estruturas de grupo muito semelhantes a esta, mas finitas. Nomeadamente, usa-se aritmética módulo um número positivo fixo $n$. Consideram-se apenas os valores $0, \dots, n-1$ e a operação de soma é tomada subtraindo $n$ ao resultado, várias vezes se necessário, caso seja maior que $n-1$. Por exemplo, em aritmética módulo $n = 12$ (como nos usuais relógios de ponteiros) tem-se que $10 + 5 = 15 - 12 = 3$. Isto não é surpreendente se pensarmos que se começarmos a ler um livro às 10h da manhã e demorarmos 5h a lê-lo, irão ser 3h da tarde no relógio (15h, na verdade) quando terminarmos.

Outra operação aritmética usual que podemos considerar é a multiplicação. Por exemplo, de novo em aritmética módulo $n = 12$ tem-se que $4 \times 7 = 4$. Podendo parecer estranho, a verdade é que $4 \times 7 = 7 + 7 + 7 + 7 - 12 - 12 = 28 - 24 = 4$. Quando $n$ é um número primo estas estruturas ganham propriedades ainda mais interessantes e $(\mathbb{Z}_n^*, \times)$, que consiste do conjunto de todos os números $1, \dots, n-1$ (excluímos 0) com a operação de multiplicação, torna-se também num grupo (convidamos o leitor a tentar perceber porquê). Mais ainda, estes grupos dizem-se cíclicos pois é possível percorrer todos os seus elementos calculando potências sucessivas de um elemento especial $g$ a que se dá o nome de gerador. Não podemos considerar agora $n = 12$, pois não se trata de um número primo, mas tomando por exemplo $n = 7$, tem-se que $g = 3$ é gerador pois calculando potências sucessivas de 3, módulo 7, obtém-se $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$, sequência que se repetirá se continuarmos o processo.

Podemos agora formular rigorosamente o problema do logaritmo discreto: conhecidos um número primo $p$ e um elemento gerador $g$, determinar para um número $A$ o valor $a$ do expoente que satisfaz $A = g^a$ em aritmética módulo $p$. De

[4] Um número diz-se primo se os únicos números que o dividem (exatamente) o número 1 e o próprio número.

facto, este problema parece relativamente simples para $n = 7$, mas a verdade é que não se conhece nenhum método eficiente para calcular o expoente pretendido quando o número primo $p$ considerado é suficientemente grande. O melhor método conhecido para resolver o problema é o denominado *index calculus*, que emana do importante algoritmo de factorização conhecido por *number field sieve* (NFS), um crivo algébrico que executa um número de passos exponencial no tamanho do número primo $p$ considerado, da ordem de $exp\left(\left(2 + o(1)\right)(\log p)^{\frac{1}{3}}(\log\log p)^{\frac{2}{3}}\right)$. O leitor interessado poderá aprofundar os detalhes em [18] ou [19].

É agora simples explicar o protocolo de acordo de chaves de *Diffie-Hellman*. Após a escolha e publicação de um número primo $p$ muito grande (na prática, o leitor pode pensar em $p$ com sendo um número com centenas algarismos) e de um gerador $g$ (de gerador), cada uma das partes, usualmente denominadas de *Alice* e *Bob*, escolhe secretamente um expoente, de entre os números $2, \dots, p - 2$. Após ter escolhido o seu expoente $a$, a *Alice* calcula $A = g^a$ em aritmética módulo $p$, e envia o valor $A$ para o *Bob*. Simultânea e simetricamente, o *Bob* escolhe o seu expoente $b$, calcula $B = g^b$ em aritmética módulo $p$, e envia o valor $B$ para a *Alice*. Depois desta troca de mensagens, em canais públicos, ambos calculam a chave partilhada $K = A^b = B^a = g^{a \times b}$ que podem de seguida utilizar para cifrar as comunicações entre ambos. Um atacante à escuta terá acesso, sem dificuldade, aos valores de $p$ e $g$, para além de $A$ e $B$, mas isso não lhe dá nenhuma vantagem óbvia para o cálculo da chave $K$. Para tal, o melhor método conhecido consiste em calcular o logaritmo discreto de uma das mensagens, por exemplo $A$, obtendo $a$ e permitindo-lhe então calcular $K = B^a$, tal como a *Alice* faria.

Neste ponto, revista a matemática subjacente ao protocolo de *Diffie-Hellman* e reafirmada a sua resistência à criptanálise, parece ser extraordinariamente difícil de imaginar em que poderá consistir a vulnerabilidade *Logjam*. É o que veremos de seguida.

## 4.A VULNERABILIDADE *LOGJAM*

Muito pouco se sabe acerca do verdadeiro conhecimento e poder computacional e intelectual das agências de segurança das grandes potências mundiais, com destaque para a NSA. *Quantos colaboradores tem? Quanto dinheiro investe? Que tecnologias possui?* As respostas a estas perguntas são certamente alguns dos segredos mais bem guardados do mundo, e abundam as teorias da conspiração, algumas decerto com fundamento. No que diz respeito à vulnerabilidade Logjam, em particular, que tipo de abordagem poderá estar por detrás da plausível capacidade para escutar, massivamente, comunicações cifradas com chaves acordadas usando o protocolo de *Diffie-Hellman*?

A resposta não é assim tão difícil de enquadrar. A cibersegurança está assente, para além do fator humano, que nunca é desprezável, em três pilares técnicos essenciais: a matemática da criptanálise, a correção dos protocolos de comunicação que usam as cifras e a boa implementação dessas funcionalidades. Assim sendo, naturalmente, há outras dimensões relevantes a ter em conta. Na verdade, a vulnerabilidade *Logjam* é uma conjugação de deficiências (propositadas ou negligenciadas) quer no desenho lógico dos protocolos de comunicação, quer na implementação das primitivas criptográficas.

Como vimos antes, todo o material criptográfico exportado pelos EUA até ao virar do milénio estava confinado, por lei, a utilizar parâmetros de segurança inseguros (*export grade*, como eram designados). Quase todos os sistemas mais populares exportados usavam, portanto, chaves criptográficas suficientemente pequenas para serem atacadas com a tecnologia de então (e muito mais facilmente com a tecnologia de que dispomos hoje) e, em particular, executavam o protocolo de *Diffie-Hellman* com números primos que não excediam 512 bits (cerca de 150 algarismos). Pode parecer muito (e é, num certo sentido), mas o que os investigadores que descobriram e divulgaram a vulnerabilidade Logjam mostraram é que, na prática e com investimento moderado em tecnologia, é possível resolver o problema do logaritmo discreto para números primos deste calibre em menos de uma semana. Não é demasiado reconfortante, mas ainda assim, tendo em conta os biliões de comunicações que necessitariam de passar por este método de análise, e o facto de pelo padrões aceites hoje se aconselhar a utilização de números primos com pelo

menos 1024 bits (o dobro do tamanho dos anteriores), parece ser um detalhe relativamente inócuo.

É neste ponto que temos de considerar os outros dois contributos decisivos para a vulnerabilidade *Logjam*. Comecemos pelo desenho de várias versões dos protocolos de comunicação, TLS, HTTPS, SSH, IPSec e outros, que utilizam acordo de chaves *à la Diffie-Hellman*. Ao estabelecer contacto entre duas entidades, os protocolos procuram antes de mais acordar quais os algoritmos criptográficos e parâmetros de segurança que vão utilizar. Basicamente, cada máquina envia à outra a lista de algoritmos e parâmetros de segurança que suporta, sendo escolhida por ambos a melhor possibilidade da lista fornecida pelo outro e que o próprio suporta. Sendo uma fase considerada não-crítica, esta fase dos protocolos não é cifrada, o que a torna vulnerável a um simples ataque de *man-in-the-middle*. O atacante intromete-se na comunicação e convence ambos os servidores a utilizar parâmetros de segurança *export grade*, que quase todos os sistemas ainda suportam por uma questão de compatibilidade com o passado e com sistemas mais antigos (infelizmente ainda em uso). Este erro lógico no desenho dos protocolos permite assim que um ataque ao problema do logaritmo discreto possa ser posto em prática, como vimos acima, mas com consequências muito pouco relevantes.

No entanto, há outro ingrediente decisivo para a vulnerabilidade se tornar efetiva que tem a ver com o descuido com que são implementadas as funções criptográficas em muitos sistemas. Como vimos, o protocolo de *Diffie-Hellman* começa por estabelecer, publicamente, um número primo $p$ e um gerador $g$. Não pretendemos discutir o assunto neste texto, mas existem métodos razoavelmente eficientes para construir números primos grandes de forma aleatória (vide [19]). Ainda assim, por ignorância, negligência, descuido, ou simplesmente por questões de eficiência, muitos sistemas simplificam o problema e utilizam sistematicamente um único número primo $p$, pré-estabelecido ou normalizado, ou um pequeno conjunto de números primos. Aqui entra o último contributo fundamental dos investigadores que descobriram a vulnerabilidade *Logjam*: ao determinar o logaritmo discreto de $A$ relativamente ao gerador $g$ módulo $p$, o algoritmo subjacente ao *index calculus* consiste essencialmente na inferência de uma quantidade considerável de relações relevantes, que não dependem do valor $A$, no fim da qual o expoente $a$ pode ser rapidamente calculado.

Desta forma, tendo conhecimento dos poucos números primos de 512 bits usados por uma percentagem assustadoramente grande dos sistemas a nível mundial, os investigadores usaram esta estratégia para pré-calcular toda a informação relevante para, conhecido o valor de $A$ poderem calcular rapidamente $a$ e atacar inelutavelmente a comunicação em tempo real. De notar que mesmo no caso em que as chaves usadas são de 1024 ou 2048 bits (e portanto fora do alcance do ataque proposto), se o conjunto de primos utilizados for pequeno a tarefa de pesquisa é ainda realizável dispondo de recursos computacionais adequados.

Sendo verdade que a conjugação de todos estes elementos é extremamente engenhosa, é certo que agências como a NSA têm certamente o *know-how* para as reconhecer e explorar. Mais, a coincidência de todas estas dimensões não será completamente inocente. Os investigadores que expuseram a vulnerabilidade *Logjam* mostram não só a plausibilidade da estratégia apresentada estar de facto a ser utilizada, mas também que isso é compatível com o nível de influência que a NSA detém junto de um grande número das empresas tecnológicas que produzem e comercializam soluções de segurança informática, e também com o que se sabe sobre o seu orçamento. Havendo ainda assim muitas implementações dos protocolos de comunicação que não são vulneráveis ao ataque de *man-in-the-middle* que permite relaxar o parâmetro de segurança do protocolo de *Diffie-Hellman* para níveis perigosamente baixos, os investigadores sabem ainda que a estratégia é replicável para atacar o problema do logaritmo discreto para primos com 1024 bits, estimando que a pré-computação necessária pode ser realizada, com investimento avultado em capacidade de processamento, mas ainda realizável à escala da NSA, em menos de um ano [4] [5]. Se 10% das comunicações usarem um certo primo $p$, esse esforço de um ano é depois facilmente recompensado com a escuta de quantidades consideráveis de informação.

Não saberemos ao certo, num futuro próximo, se de facto esta é a estratégia de cibervigilância usada pela NSA, apesar dos indícios que apontam nesse sentido. Tal prática, para além de pôr em causa a proteção dos direitos de cidadãos, empresas e estados, norte-americanos e não só, não contribui para a credibilidade de instituições que se pretendem idóneas, e levanta uma questão ainda mais inquietante: que outros estados poderão dispor de esquemas de vigilância semelhantes, possivelmente explorando exatamente a mesma vulnerabilidade?

## 5.CONCLUSÕES

Numa época em que as tecnologias de informação e comunicação são quase omnipresentes e se fala cada vez mais na *internet das coisas*, a consciencialização para as questões que envolvem o ciberespaço é cada vez mais pertinente. Segurança e privacidade da informação que circula na rede são um ponto fulcral para utilizadores comuns, estados e empresas. Quão seguras e confidenciais são de facto as comunicações?

Desde o obscurantismo de muitos dos sistemas ainda usados, a ataques que vão sendo conhecidos quase todos os dias, tudo vem contribuindo para minar a confiança dos utilizadores e adensar o clima de suspeição. Só a persistente evolução na forma de pensar as questões da cibersegurança, com o contributo de todos e particularmente das comunidades académicas e científicas, pode alterar este cenário e lançar-nos numa era de crescente iluminismo criptográfico. Alicerçada nos ideais subjacentes à proposta de *Kerckhoffs*, a comunidade começou já a operar esta revolução, propondo a participação de todos no desenho e desenvolvimento de funcionalidade criptográficas e protocolos *open source*, cuja segurança é testada e certificada diariamente por todos os intervenientes.

Neste artigo vimos, através do ataque *Logjam*, como as vulnerabilidades de segurança podem ser subtis, muitas vezes por resultado de interações complexas entre componentes aparentemente inócuas dos sistemas, talvez mesmo deixadas ou promovidas propositadamente por quem de direito para poderem ser usadas para fins menos confessáveis, mas que o esforço de investigadores apostados em transformar o ciberespaço num lugar mais seguro pode ajudar a descobrir e mitigar. É de salientar aqui que a vulnerabilidade *Logjam* foi previamente dada a conhecer pelos investigadores a várias entidades e empresas de relevo, e que muitos dos problemas estão já resolvidos.

Para que este processo seja cada vez mais a norma é essencial investir na investigação científica nesta área verdadeiramente multidisciplinar, apostar na formação de cidadãos cada vez mais competentes e conscientes dos desafios da cibersegurança, e mudar a mentalidade acomodada de que alguma entidade, algures, se encarregará de garantir os nossos direitos, de regular o ciberespaço, e de garantir que estamos seguros. Nesta área, o papel a desempenhar pelas entidades reguladoras, pelos estados ou pelas empresas idóneas é fundamental, mas carece ainda assim de ser

continuamente acompanhado, até porque os problemas de segurança não vão deixar de existir. A cibersegurança deve ser, cada vez mais, uma tarefa partilhada por todos. Só sociedades atentas, conscientes e competentes terão a capacidade de tornar o ciberespaço num lugar mais luminoso.

Este processo é feito de avanços e recuos, e é ingénuo imaginar que possa chegar o dia, mesmo que longínquo, em que assuntos tão sensíveis como estes serão total e abertamente escrutinados. Mas a verdade é que de cada vez que uma nova vulnerabilidade é descoberta está-se, por um lado, a pôr em causa o sistema, mas por outro a criar oportunidade de colmatar essa falha, tornando o sistema resultante mais resiliente. Não sabemos ao certo se a NSA explorava, de facto, a vulnerabilidade *Logjam*, mas não sobram muitas dúvidas de que usa de facto técnicas de cibervigilância sofisticadas. Não será implausível pensar que outros estados poderosos tenham capacidades similares, e haverá sempre muitos recantos obscuros nesta área. A questão é que proceder de forma pouco transparente acaba por trazer, quase inevitavelmente, mais problemas a jusante. Ainda recentemente o jornal satírico americano *The Onion* sugeria que o estado chinês está com dificuldade em encontrar mão-de-obra qualificada suficiente para explorar todas as vulnerabilidades dos sistemas norte-americanos [20]. Em última análise este é um jogo de equilíbrios difíceis, em que as más práticas não podem trazer bons resultados a prazo, e em que parece claramente preferível divulgar uma vulnerabilidade quando é encontrada, do que explorá-la em segredo. Todos são vulneráveis. Nesta linha, em Agosto deste ano, a NSA publicou uma nota de imprensa em que dá conta da necessidade de se fazer uma aposta séria no desenvolvimento de criptografia resistente à computação quântica. Não tendo dado nenhuma boa justificação para esta aposta, logo surgiu um escrutínio sério por parte dos especialistas sobre o alcance e implicações da afirmação. Estará a NSA em condições de executar ataques quânticos sobre os sistemas? Estará com receio que outros o façam, ou haverá algo mais subtil por detrás desta posição? Vide [21] para uma discussão científica informada sobre o assunto. Certamente, muita água passará debaixo das pontes a propósito deste assunto. Se tudo correr bem, no final, todos saberemos um pouco mais sobre cibersegurança (e computação quântica) e o ciberespaço ter-se-á tornado um lugar um pouco mais seguro.

"*It is a riddle wrapped in a mystery inside an enigma, but perhaps there is a key.*" - *Winston Churchill*, rádio BBC, 1 de Outubro de 1939

# Bibliografia


[1] W. Diffie e M. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, n.º 6, p. 644–654, 1976.

[2] C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, n.º 28, 1949.

[3] Wikipedia a., "Edward Snowden," 2 12 2015. [Online]: https://en.wikipedia.org/wiki/Edward_Snowden. [Acedido em 2 12 2015].

[4] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin e P. Zimmermann, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," em *22nd ACM Conference on Computer and Communications Security (CCS '15)*, Denver, 2015.

[5] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Beguelin and P. Zimmermann, "Weak Diffie-Hellman and the Logjam Attack," Março 2015. [Online]: https://weakdh.org/. [Acedido em 01 12 2015].

[6] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, pp. 161-191, 1883.

[7] S. Singh, The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, Doubleday, 1999.

[8] Wikipedia b., "Enigma machine," 29 11 2015. [Online]: https://en.wikipedia.org/wiki/Enigma_machine. [Acedido em 2 12 2015].

[9] Wikipedia c., "Cryptanalysis of the Enigma," 12 2015. [Online]: https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma. [Acedido em 02 12 2015].

[10] Wikipedia d., "CoCom - Coordinating Committee for Multilateral Export Controls," 2 09 2015. [Online]: https://en.wikipedia.org/wiki/CoCom. [Acedido em 03 12 2015].

[11] Zimmermann, *Pretty Good Privacy*, 1991.

[12] Open PGP Alliance , "Welcome to The OpenPGP Alliance," 2015. [Online]: http://www.pgpi.org/ [Acedido em 01 12 2015].

[13] The Wassenaar Arrangement , "The Wassenaar Arrangement: On Export Controls for Conventional Arms and Dual-Use Goods and Technologies," 2015. [Online]: http://www.wassenaar.org/ [Acedido em 01 12 2015].

[14] National Institute of Standards and Technology, *Data Encryption Standard*, Federal Information Processing Standards Publication, 1977.

[15] National Institute of Standards and Technology, *ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards

Publication, 2001.

[16] National Institute of Standards and Technology, *Announcing Draft Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Draft Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard, and Request for Comments*, Federal Information Processing Standard, 2015.

[17] R. L. Fernandes e M. Ricou, Introdução à álgebra, Lisboa: IST Press, 2014.

[18] H. L. J. A. Lenstra, The development of the number field sieve, Lecture Notes in Mathematics ed., vol. 1554, Springer—Verlag, 1993.

[19] C. C. Richard Pomerance, Prime numbers - A computational perspective, Springer, 2005.

[20] The Onion, "China Unable To Recruit Hackers Fast Enough To Keep Up With Vulnerabilities In U.S. Security Systems," *The onion*, vol. 51, n.º 43, 26 10 2015.

[21] N. Koblitz e A. Menezes, "A riddle wrapped in a enigma," 2015.

CYBERLAW by CIJIC

# CYBER SECURITY VS. CYBER DEFENSE – A PORTUGUESE VIEW ON THE DISTINCTION.

# CIBERSEGURANÇA VS. CIBERDEFESA – UMA VISÃO PORTUGUESA DA DISTINÇÃO.

**MIGUEL FERREIRA DA SILVA**[1]

[1]Correio eletrónico: mjnfds@gmail.com

**SUMMARY: 1.DEFENSE AND SECURITY; 2.SOME INTERNATIONAL DISTINCTIONS; 3.PORTUGUESE CYBER DISTINCTIONS; 4. CONCLUSIONS.**


## ABSTRACT

The current Portuguese academic landscape shows a growing interest for research and debate on cyber security and cyber defense. Yet, as in most countries, there is not yet a consensus on which concept is what.

On the public sphere, and despite grate care in assuring the proper legal functioning of cyber security initiatives and institutions, there is a clear, although discrete, move to strengthen Cyber Defense capabilities and authorities. Amongst all the "Political Guidance for Cyber Defense" clearly being the leading Strategy.



**Keywords:** Cyber Security, Cyber Defense; concepts; political guidance.

## RESUMO

A atual paisagem acadêmica Português mostra um crescente interesse pela pesquisa e debate sobre cibersegurança e ciberdefesa. No entanto, como na maioria dos países, não existe ainda um consenso sobre qual destes conceitos é o quê.

Na esfera pública, e apesar das cautelas em assegurar um funcionamento legalmente correcto das iniciativas e instituições de cibersegurança, há uma clara, embora discreta, tendência para reforçar as capacidades e as autoridades de Cyber Defesa. Entre todas sendo a "Orientação Política para a Ciberdefesa" claramente a principal estratégia.



**Palavras chave:** Cibersegurança; Ciberdefesa, conceitos; orientações políticas.

## 1. DEFENSE AND SECURITY.

The Portuguese translation of security – "segurança" – translates both the concept of security and that of safety. The fortunate translation (elsewhere rather problematic) encompasses in itself the holistic approach security has to have in cyber. As we know, in this particular environment – cyberspace – the barriers between actors of security (from individual users to States) and the types of risks (from continuity assurance to data theft) all further blur that distinction. In a way, the portuguese wording for cyber security is more accurate then itself, as it includes not only security but also safety. This becomes more obvious when most references to protective measures (usually referred to as cyber hygiene), and certainly within the scope of safety, are clearly included in the concept of "segurança" ("security").

There is however a more difficult distinction, one to which the legal and cultural understanding of the functions and duties if the State, vis-à-vis civil and economic rights, has an enormous impact. A properly capitalized "Defense" concept appeals to that basic function of the State to provide protection from outside threats. A concept mostly identified with Armed Forces, as well as with its capabilities for military action in defense of an entire nation.

We recognize the common doubts about the double meaning of "cyber defense", both as operational continuity assurance and military cyber capabilities.

- As operational continuity assurance, cyber defense might be understood as cyber security of a (yet another) unique critical infrastructure – the military.

- As cyber capabilities, understood as the capabilities to gain advantages upon an adversary, either we are considering self-resilience – where the defensive capabilities might be thought of as functions which could be traced back to cyber security (leaving only a problem of scale) – or we are considering offensive capabilities.

From a democratic "western" point of view, we usually understand "defense" as defensive, and not offensive. That, however, is a misconception in the cyber space. Even if, in cyber, we might think of (military) self-resilience as a type of security ("security of the force"), that in practice falls short of reality. First because "security of the force" may include preemptive action (offensive in nature during campaign),

but also as, for Defense institutions to be able to actively defend, they must also be capable of preemptive military action (offensive in nature also at the planning stage). Meaning that such function is not only aimed at the protection of the force itself but to the general goals of the Defense sector, i.e. the protection of the nation.

That doesn't mean such military capabilities, or operations, are necessarily considered as "offensive". In fact one could almost quote, in identifying "offensive action", U.S. Supreme Court Justice Potter Stuart[2] – " I'll know it when I see it". There is however an indisputable fact: Defense capabilities in Cyber differ, even when cumulative, with cyber security capabilities.

Furthermore, there is a generalized trend for understanding Defense as a part of a larger Security Sector. In this sense, the distinction between responses (as functions) follows the target objectives of the threats.[3] Such a view puts less emphasis in the specific actions (e.g. phishing, trojans) and their actors (e.g. a national of country "X", a criminal network). On the contrary it highlights the function to be activated (Security or Defense) and the nature of the threat (private or public).

That is to say that there are two levels of assessment: one that distinguishes the targets and actors, as private or public/state; and another that regardless of the target, distinguishes the objectives of the threat.

In the first case it's relatively easy to establish if the threat aims to harm a state, even when the targets are private (e.g. not only conventional inter-states armed conflicts, but also small scale terrorist attacks against general population or critical infrastructure of a specific state). On the other it is more difficult to assess whether the State faces a security challenge or a "defense level" attack (e.g. private motivations for attacks against public assets or information security breaches).

One thing seems to be widely accepted: more obviously then elsewhere, in the cyber space Defense cannot operate in the absence of (or without an adequate level of) Security, and there is an operational continuity between Security and Defense, which can only be assured by cumulative capabilities. Such overlap may pose some

[2] USSC Justice Potter Stuart, referring to "hard core" pornography, Jacobellis v. Ohio, 378 U.S. 184 (1964).
[3] We are highlighting a distinction between functions and threats instead of one between actions and actors.

challenges to the accepted principle limiting *Posse Comitatus*[4], so widely criticized were it is not observed. But a far more present challenge relates to the possible conflict of rights, as this necessary overlap between Security and Defense may put a stress between assuring safety and security and the full exercise of individual liberties by individual citizens.

## 2. SOME INTERNATIONAL DISTINCTIONS

According to the Open Technology Institute's listing of international definitions, and mostly using sources with entries in both concepts, one could make a few comparisons.[5] This source lists 34 countries (or international organizations) with a "definition" of cyber security, but only 8 with a parallel definition of cyber defense. It is interesting to see the differences among them:

### - AUSTRIA -

**Cyber Security**

*Cyber security describes the protection of a key legal asset through constitutional means against actor-related, technical, organizational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cyber security helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimize the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services.*

Note the emphasis in the protection of legally protected "assets" (thus including individual rights) by constitutional means (thus equally limited).

[4] Posse Comitatus Act of 1878 – 18 U.S. Code § 1385.

[5] Adapted from http://opentechinstitute.github.io/cyber-definitions/web/search.html?q=Cyber+Security and http://opentechinstitute.github.io/cyber-definitions/web/search.html?q=Cyber+Defense.
Notes: We didn't kept the original English version of *defence* instead of the American version (defense), for consistency; for comparison purposes, most sources mentioned here with own definitions in both concepts; Our italics, for highlighting purposes; mention to "(Translations)" are from the authors of the original compilation.

**Cyber Defense**

*The term "cyber defense" refers to all measures to* defend cyber space with military and appropriate means for achieving military-strategic goals. *Cyber defense is an integrated system, comprising the implementation of all measures relating to ICT and information security, the capabilities of milCERT and CNO (Computer Network Operations) as well as the support of the physical capabilities of the army.*

An open definition encompassing all aspects of military activity and capabilities as mentioned above, yet focusing on the (military) function facing the threat (to military-strategic goals).

## - EUROPEAN UNION -

**Cyber Security**

*Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain,* both in the civilian and military fields, *from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.*

Despite an ambiguous reference to confidentiality, the poor wording points us towards a safety perspective of security.

## - FRANCE -

**Cyber Security**

*The desired state of* an information system *in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cyber security makes use of information systems security techniques and is based on fighting cybercrime and* establishing cyber defense.

The rather ample definition not only (more explicitly then Austria) points towards the operational integrity and availability of assets, in this case "an information system", but also encompasses a more proactive face of security (in fighting crime), recognizing the needed overlap with Defense capabilities.

**Cyber Defense**

*The set of all technical and non-technical measures allowing* a State *to defend in cyberspace information systems that* it *considers to be critical.*

Function seems to be the key assessment standard, although giving less emphasis to the threat and more to the (State) actor of the (defense) function. To note also that no reference is made to the nature of those executing the function, as nowhere do we read "military" as the only state power with this objectives.

## - MONTENEGRO -

**Cyber Security**

*Cyber security refers to* efforts to prevent damage *caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.*

*Cyber security seeks to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. General security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality".*

The listing that follows the first definition attempt appears to deviate from the functions/threats logic and to focus on actions. Yet after a closer look that listing may offer examples of a subjective but wider view of continuity and availability, while still mentioning "organization and user's assets" and "confidentiality".

**Cyber Defense**

*Cyber defense is mainly used in* military context, *but it may be also related to criminal and espionage activities.*

*NATO uses the following definition when referring to cyber defense: the ability to safeguard the delivery and management of services in an operational Communications and Information Systems (CIS) in response to potential and imminent as well as actual malicious actions that originate in cyberspace."*[6]

## - NATO : NORTH ATLANTIC TREATY ORGANIZATION -

**Cyber Defense**

*(Active Cyber Defense) A proactive measure for detecting or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber counter-operation against the source.*

There seems to be an inner contradiction in the last part of the definition. As in the (possible) phrase "proactive measure" "for determining the origin of an operation that involves launching…", whatever is launched (preemptive, preventive, or cyber counter-operation) is *not* included in the definition. Only the measure for determining the origin is. As James Lewis[7] tells us such a position cannot hold, but it is useful to highlight the shyness of admitting it.

## - ROMANIA -

**Cyber Security**

*(Translation:) The state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information electronically for public and private resources and services in cyberspace. Proactive and reactive measures may include policies, concepts, standards and guidelines for security, risk management, training*

[6] The reference to NATO is made, according to the source, by Montenegro. As we can see below the wording by NATO is not exactly the same as the one Montenegro seems to quote.
[7] Lewis, James A. *The role of offensive cyber operations in NATO's collective defence*, Tallin Papers n. 8, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallin, 2015.

*and awareness activities, implementing technical solutions to protect cyber infrastructure, identity management, and consequence management.*

**Cyber Defense**

*(Translation:) Actions in cyberspace to protect, monitor, analyze, detect, counter aggression, and ensure appropriate response against specific cyber threats to national defense infrastructure.*

## - U.S.A. / RUSSIA -

**Cyber Defense**

*Cyber Defense is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attacks.*

In sharp contrast with the previous, this proposed definition enlarges the scope of "defense" to functions including most, if not all, of those of "security".

## - COLUMBIA -

**Cyber Security**

*(Translation:) Capacity of the state to minimize the risks they and their citizens are exposed to, in the face of threats and incidents of the cyber nature.*

If in the concept of cyber defense (below) "State" as an actor and "national sovereignty" as a target limit the scope of "defense" to State actions, here the private sector and the individual are taken off their central role in security.

**Cyber Defense**

*(Translation:) State capacity to prevent and counter any threat or incident that is cybernetic in nature which affects national sovereignty.*

## - BELGIUM -

### Cyber Security

*(Translation:) Cyber security is the desired situation or protection of cyberspace and is proportional to the cyber threat and potential consequences of cyber attacks. In a situation of cyber security, disruption, attack, or misuse of ICT does not cause any danger or harm. The consequences of abuse, disruption or attack may include restricting availability and reliability of ICT, the violation of the confidentiality of information, or the damaging of the integrity of information (addition, deletion, or modification [of information] are illegal).*

*The desired situation in which the protection of cyberspace is proportionate to the cyber threat and the possible consequences of cyber-attacks. At Defense Cyber Security comprises three pillars: Cyber Defense, Cyber Intelligence and cyber counter-offensive.*

*(Translation) a favorable situation where the protection of cyberspace is proportional to cyber threats and the possible consequences of cyber attacks. In a situation of cyber security, the disruption, an attack or abusive utilization of information and communications will not provoque danger or damage. The consequences of abusing, disruption or an attack can provoke inability to use, and untrustworthiness of information and communications systems, and the violation of confidentiality of information or damage the integrity of the information (illegal adding, deleting or modifying of information).*

### Cyber Defense

*The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defense's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defense consists of following duties: Protect, Detect, Respond, and Recover.*

## 3. PORTUGUESE CYBER DISTINCTIONS.

Reviewing the current Portuguese research in this field, we find a number of examples of commonly accepted conceptualizations. Among research products, the reference standard is offered by Lino Santos' entries at the (Portuguese) Encyclopedia of Law and Security[8].

3.1. Cyber security seems to be a more widely used, if not accepted, term. In fact, the Portuguese Encyclopedia of Law and Security has an entry for "cyberspace" [9] and another for "cyber security" [10] yet none for "cyber defense". In his work, Lino Santos tells us in this encyclopedia that "cyber security" may have a double meaning: one for the security of the entire "cyberspace" as an autonomous "entity" and another for the security of the cyber component of a specific system. Yet he offers three different approaches.

On a first approach, this same author recognizes the conceptual importance of the "subject" ("object" in the original) of cyber security for the definition.[11] In his particular case identifying these subjects of (cyber) security as: the State; market(s); and individuals.

On a second conceptual approach to a definition of Cyber Security, Santos highlights the "set of systems or domains that the state and society in general have to deal with cyber security". In this sense, he identifies four of them: simple protection; criminal prosecution; war; and diplomacy.

i. At the simple protection level we are redirected to the International Telecommunications Union definition, although with a substantial explanation of the technical, procedural and human resources needed to prevent, react and manage within cyber security.

ii. When addressing criminal prosecution, Santos highlights not only the possible new "cyber means" of perpetrating already established crimes against

[8] Bacelar Gouveia, Jorge and Santos, Sofia (Coord.), Enciclopédia de Direito e Segurança, Almedina, Coimbra, 2015.
[9] Santos, Lino, "Ciberespaço", op.cit., pp. 60.
[10] Santos, Lino, "Cibersegurança", op.cit., pp. 63.
[11] Ibidem, pp.64.

existing rights, but autonomous cybercrimes capable of harming rights connected with the cyberspace.

iii. The author's reference to war – without any prefix (re. "cyber") – points towards the continuity of military operational capability and the acquisition of advantages against adversaries. To note that despite a reference to National Defense as equally empowered to assure command and control in war and emergencies ("also in cyberspace"), no reference is made in this author's article to "cyber defense".

iv. In diplomacy only the aim – as prosecution of national objectives – is referred.

The third and last approach gives us six "axis of intervention" for the set of policies in most "known national cyber security strategies". In this sense Santos proposes the primacy of the function when grouping measures in different categories of policy efforts (an approach already explored by the author in his MPhil dissertation[12]):

i. Combating cybercrime. Which would include not only the updating and harmonization of relevant criminal legislation, but also regulating Information and Communications Technologies (ICT) industry so as to assure an "adequate level of cyber security". In this later sense the emphasis is given to the regulation of the telecommunications market.

ii. Standardization and certification. Understood as the national and international efforts to establish "references, rules, conditions or requisites of security" as well as the due compliance of products and services with those patterns.

iii. Training and awareness. As technological training and updating (capacity building), but also awareness and alert initiatives.

iv. Protection of critical infrastructures. Including risk analysis, preceded by mapping functional dependencies, and implementation of protective measures in critical functions.

[12] Santos, Jose Lino Alves dos. *Contributos para uma melhor governação da cibersegurança em Portugal*, Masters dissertation presented at the Universidade Nova de Lisboa, Lisboa, 2011. A shorter work by this author was publishes as a paper at pp. 217-305 in *Estudos de Direito e Segurança*, Vol. II. Jorge Bacelar Gouveia (Coord.), Almedina, Coimbra, 2014.

v. Warning and response. Actions to mitigate cyber security incidents and alerts for new vulnerabilities and emerging threats.

vi. Research and development. Not only aimed for technological development, but including other social areas of research ("namely ethics, behavioral security, criminology or risk").

3.2. In Octávio Militão's[13] research, cyber security is identified more with policing functions: "*Cyber security is the guarantee or control and 'policing' of cyberspace so as to ensure an effective response to criminal activity*". Safety is not considered, nor does the specific challenges of jurisdiction or level of threat considered.[14]

A much more complete view is presented on cyber defense: "*Cyber defense - has the task of ensuring the achievement of security and national defense missions, namely to guarantee state sovereignty in the global cyberspace.*"[15]

Later in his research, Militão underlines that both concepts "*are considerably different and each one encompasses a specific sphere of action in cyberspace*" [16] yet stating again a parallel between cyber security and police and intelligence services, on the one hand, and cyber defense and armed forces on the other:[17]

| | | |
|---|---|---|
| Cyber security | Security forces | Cybercrime |
| | | Hacktivism |
| | IT ("Informatics") | Cyber espionage |

[13] Militão, Octávio Pimenta. *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional*, masters dissertation, FCSH, Univ Nova de Lisboa, April 2014.
[14] Although he is here quoting: Nunes, Paulo Viegas. "*Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço*", Conference, Beja, IV SimSIC, 2013.
[15] Here too quoting another article by the same original author: Nunes, Paulo Viegas. "*A Definição de uma Estratégia Nacional de Cibersegurança*", Cibersegurança, N.o133, IDN, 2012.
[16] Militão, op.cit., pp. 25.
[17] Idem.

| | | |
|---|---|---|
| | Services[18] | Cyber terrorism |
| Cyber defense | Armed Forces | Cyber war |

It is therefore with surprise that this author further develops the concept of cyber security in this research: "*Cyber security is the set of measures that seek to ensure the wellbeing and the proper functioning of the action of a state and its people in cyberspace and beyond, if derived from actions directly deriving from it.*"[19]

3.3. On a more official stance, we now look to the use of the terms "Cyber Security" and Cyber Defense" in two Acts of the Portuguese Government. One creating the National Cyber Security Center, established in the Decree-Law n.º 69/2014,[20] of May 9th, and the other approving the National Security Strategy in Cyberspace, published as annex to the Resolution of the Council of Ministers n.º 36/2015, of June 12th.

3.3.1. The National Cyber Security Center was created by an Executive Act, thus a law. We must first consider the almost immediate need of the Portuguese Government to comply with guideline both from the European Union and from NATO, so as to establish such a Center. That being said, the architecture chosen for this institution hardly meets the needs announced in the preamble.

Furthermore, the concept of Cyber defense is:

a) Completely absent from any reference while defining the mission, duties and responsibilities of this new Center; and is only

[18] Although translated correctly from the original in Portuguese, we believe there might be a misunderstanding between the Portuguese and English terms for information/intelligence. In Portuguese "intelligence" is translated with the plural of "information", thus capturing the need for additional treatment on each information gathered. Yet it is common to mistranslate that Portuguese concept with the English for "information" instead of the correct "intelligence". On the other hand *informático* refers to IT related, e.g. IT technician. In this particular case the original author does use the Portuguese equivalent to "information technology", despite our belief that such use rises from the referred mistranslation. In the same dissertation, the original author later refers to these same types of threats as addressed by Intelligence Services. For accuracy purposes we kept the correct translation, although understanding it as referring to aimed to "intelligence services".

[19] Militão, op.cit., pp. 26.

[20] This Executive Act (Decree-Law n.º 69/2014, of May 9th) amends, by introducing three new articles, the Decree-Law n.º 3/2012, of January 16th. Therefore, any mention hereinafter to the law establishing the Center refers to the new version of the amended law of 2012.

b) Expressly mentioned as a responsibility of other(s) structure(s) in the n.º 3 of article 2.º-A. In fact that is what results from mentioning that the Center being created "*also operates in conjunction and close cooperation with the responsible national structures by cyber espionage, cyber defense, cyber crime and cyber terrorism*", r.e. other structures.

And despite its mission including the "*implementation of measures and instruments needed to anticipate, detect, react and recover in situations which, imminence or occurrence of incidents or cyber attacks, may jeopardize the functioning of critical infrastructure and national interests*" (at the end of n.º 2, article 2.º), the competences of the Center do not "*affect the powers and competences assigned by law to other public entities in matters of cyberspace security and is exercised in coordination with these*" (n. 2 of article 2.º-A). Meaning that the Center has, operationally at least, more of a coordination role.

That seems to be made explicit by the law itself when, in the following rule (n.º 3 of the same article 2.º-A), states that the Center also "*works in articulation and close cooperation with the national structures responsible for cyber espionage, cyber defense, cyber crime and cyber terrorism*". Such an interpretation is misleading, as, in continuation of the previous rule, what is here stated is that in this cases – which include Cyber Defense – the Center has less intervention.

Had we any doubt and paragraph h) of n.º 1 of the same article 2.º-A enlightens us by "empowering" the Center only to "*ensure the planning of the use of cyberspace in crisis and war situations, within the civil emergency planning* (context)".

Summarizing, the Portuguese National Cyber Security Center was established by a Law that only refers to Cyber Defense to state it is a duty of other agency(ies), further clarifying that even in a state if war, the Center is confined to continuity planning in the framework of civilian emergency response.

3.3.2. The National Strategy for Cyberspace Security (hereinafter "Cyber Security Strategy"). As a National strategy should, this one starts with an holistic view of the threat and pursue of objectives.

Among other less relevant themes for our purpose of accessing the Portuguese view of a distinction between cyber security and cyber defense, the Strategy, in its

preamble, refers at length the public, national level of a threat to the sovereignty and survival of the State:

"*The society, the economy and the state are dependent on information and communication technologies (ICT). We have witnessed* (…) *a growing reliance on ICT in vital functions of running the country.* (...)

*Internally as international there are evident capabilities of political and religious activisms, criminals or terrorists to conduct actions impacting on the safety of critical information infrastructures, creating serious threats to the survival of democratic rule of law State and the space of freedom, security and justice.*

*The need to protect the areas that embody national sovereignty, ensuring the political and strategic independence of the country, as well as the growing number of incidents and malicious attacks, require that the security of cyberspace is regarded as a national priority.*"

These words immediately take us to identify an analysis that points to what might be called a Defense level event (threat, with reactive strategy, planning and operations).

It is this national Cyber Security Strategy that, in the 3rd paragraph of the first of its "six axis of intervention", explicitly sets the goal of developing cyber defense capabilities.

Three aspects of this strategy should be highlighted:

i. The mention to the command and control authorities, with the strategic responsibilities committed to the JCS and the planning and immediate response to the Cyber Defense Center and the branches – paragraph c) of n.º 3 of Axis 1;

ii. The reference to the dual use of military capabilities in this regard, i.e. promoting the use of military capabilities not only in military operations but also in national cyber security, including information sharing – paragraph d) of n.º 3 of Axis 1;

iii. A rather detailed set of objectives for a cyber defense capacity (and capabilities) building (infra) – paragraph c) of n.º 3 of Axis 1.

Regarding this later, and given its relevance for our understanding of the Portuguese conceptualization of "cyber defense", we follow the original wording, which this Resolution carries from an earlier, and still in force, Order of the Minister of Defense (Despacho n.º 13692/2013, from October 28th), establishing the "Political Guidance for Cyber Defense". This document is rather clear when addressing the objectives of the Portuguese Cyber Defense, which are not necessarily only defensive:

"*The objectives of cyber defense policy are:*

*1) To ensure the protection, resilience and security of networks and ICS of National Defense against cyber attacks;*

*2) To ensure the freedom of action of the country in cyberspace and, where necessary and directed, proactive exploration of cyberspace to prevent or hinder their hostile use against the national interest;*

*3) Contribute cooperatively to national cyber security.*"

Clearly this wording is in sharp contrast with all the caveats and uncertainties of the academic approach. Yet it is here, in Defense policy, that we find clear basis of the distinction made by the Portuguese decision makers. If, in security, continuity and resilience are the objectives, in Defense the full spectrum of planning and operations may be considered, including the dual use of the force.

## 4. CONCLUSIONS.

The international conceptual diversity is somewhat mirrored in Portugal, with the available debates revealing the usual uncertainty about the distinction between cyber security and cyber defense.

At times there seems to be some reluctance in addressing military aspects of cyber security (as if the prohibition of some sort of *posse comitatus* of the military would not be as inadequate as the distinctions between domestic and foreigner in intelligence gathering). Since our subject doesn't dwell on civil rights and privacy, we will not anticipate any reasons for the absence of the military references in the civilian discourse.

We can find in the official cyber security centric documents a discourse much closer to safety, awareness, research and development. The operational emphasis is then guided to continuity of service: with prevention, recovery and resilience, all mainly aimed at critical infrastructures.

Oddly, it is the "Political Guidance on Cyber Defense" (an Order by the Minister of Defense) and the later "National Strategy for Cyberspace Security", which both recognize the needed interaction between cyber defense and cyber security. Thus admitting the need of capabilities, but building the bridge from the military unto the civilian side of the equation, and affirming the (necessary) dual use of such military capabilities.

In this sense we tend to follow the Defense´s view: the distinction is usually pointless, given the shared area of operations and the vast majority of actions. The differences may occur on the level of classification of the information on or about certain critical infrastructures (although far more civilian critical infrastructures are more vital), or in what is euphemistically or unintentionally called "*proactive exploration of cyberspace*" in the text of the "Political Guidance for Cyber Defense".

We can, in any case, affirmatively state that (like with reality and fiction) policy is, in this regard, more advanced then academia.

CYBERLAW by CIJIC

# LA RESPONSABILIDAD DE LOS PROVEEDORES DE SERVICIOS Y DE LOS USUARIOS DE INTERNET POR PUBLICACIONES OFENSIVAS: UN BREVE MUESTRARIO JURISPRUDENCIAL

# A RESPONSABILIDADE DOS PROVEDORES E UTILIZADORES DA INTERNET POR PUBLICAÇÕES OFENSIVAS: UMA BREVE AMOSTRA JURISPRUDENCIAL

**ÓSCAR R. PUCCINELLI** [1]

[1] Doctor en Derecho Constitucional por la Universidad de Buenos Aires y profesor de Derecho Constitucional y de Derecho Procesal Constitucional y Transnacional en la Universidad Nacional de Rosario (Argentina) y en la Facultad de Derecho y Ciencias Sociales de Rosario, dependiente de la Pontificia Universidad Católica Argentina. Correo electrónico: opuccine@fderec.unr.edu.ar

## RESUMO

Neste artigo procuraremos dissertar sobre alguns aspectos jurídicos, doutrinários e jurisprudênciais, mais recentes, quer europeus quer norte-americanos, relativos aos serviços da sociedade de informação, em especial quanto à responsabilidade de jornalistas e *bloggers* por publicações difamatórias disponibilizadas na *Internet*.

**Palavras-Chave:** Responsabilidade civil; Serviços de internet e Imprensa; Protecção de dados; *bloggers* e liberdade de expressão; Intenção dolosa e publicações difamatórias

## RESUMEN

En este artículo se propone informar sobre algunos aspectos legales y doctrinarios y sobre jurisprudencia reciente en el ámbito de Europa y los Estados Unidos, con relación a los servicios de la sociedad de la información, y más concretamente sobre los alcances de la responsabilidad por publicaciones ofensivas en Internet provenientes de periodistas y de bloggers.



**Palabras clave:** responsabilidad – servicios de internet y prensa – protección de datos – bloggers y libertad de expresión - real malicia y publicaciones injuriantes

## 1. EL DERECHO DE DAÑOS Y LA RESPONSABILIDAD CIVIL DE LOS SUJETOS INVOLUCRADOS EN LA INSERCIÓN -Y DIFUSIÓN- POR INTERNET DE CONTENIDOS LESIVOS

La tensión entre la libertad de expresión y los derechos que pueden verse afectados por su ejercicio encuentran respuestas bastante homogéneas en las convenciones regionales sobre derechos humanos, donde se admiten precisamente restricciones a aquella siempre que ellas se encuentren expresamente fijadas mediante ley –entendida ésta en sentido formal- y sean estrictamente necesarias, en una sociedad democrática, para asegurar: *a*) el respeto a la reputación u otros derechos de los demás, o *b*) la protección de la seguridad nacional, la salud o la moral[2].

Estos parámetros, aplicables a cualquier medio de expresión, encuentran ciertas variantes cuando tal libertad se ejerce dentro del marco de otra libertad preferida como lo es la libertad de prensa, criterio que es generalmente seguido en Latinoamérica en aplicación de los criterios estadounidenses, como el de la *actual malice* (ordinariamente traducido por "real malicia", y que habilita la reparación del funcionario público ofendido cuando la afirmación se hizo con conocimiento de que era falsa o con temerario desprecio de si era falsa o no), que fuera establecido por la Corte federal en el *leading case* "New York Times vs. Sullivan"[3], aunque implique dotar a la prensa institucional de "algún privilegio constitucional mayor del que gozan otros oradores"[4], ni que autorice a concluir que se esté creando una exención general para la difamación por "cualquier cosa que pudiera ser etiquetada de opinión"[5], sean las expresiones vertidas por medios institucionales o no institucionales[6].

El nuevo contexto tecnológico obliga a revisar la aplicabilidad actual de tales prescripciones ya que, como lo indica Cotino Hueso, actualmente resulta difícil

[2] En ellas coinciden el art. 10 del Convenio Europeo de Derechos Humanos y el art. 13 de la Convención Americana sobre Derechos Humanos (aunque respecto de la salud y la moral, la norma americana le adiciona la palabra "públicas" ausente en la regla europea). Discordantemente, mientras la regla americana refiere a la protección del orden público, el convenio europeo menciona la prevención del delito, impedir la divulgación de informaciones confidenciales y garantizar la autoridad y la imparcialidad del poder judicial.
[3] "New York Times Co. v. Sullivan", 376 U.S. 254 (1964).
[4] "Citizens United v. Federal Election Commission", 558 US 310, 352 -2010.
[5] "Milkovich v. Lorain Journal Co.", 497 US 1, 18, 1990.
[6] "Bartnicki v Vopper", 532 US. 514, 525 y n. 8, 2001; "Cohen v Cowles Media Co." 501 US 663, 669-70, 1991, "First National Bank de Boston v Bellotti" 435 US. 765, 782 n.18, 1978; "Henry v Collins", 380 US 356, 357, 1965.

distinguir material y jurídicamente a los medios de comunicación clásicos de los diferentes modos de comunicación de internet a fin de atribuirles alguna protección reforzada, pues la comunicación de masas, y la comunicación interpersonal, e incluso en Internet los roles de informador e informado se trastocan, desde que "el público no es consumidor, sino 'prosumidor' (*prosumer*) de información, esto es, un híbrido de consumidor y productor de contenidos… El usuario ya no es simple receptor pasivo de la comunicación, sino que se convierte en muchos casos en emisor y creador de la información. Todo el mundo es editor; la ya de por sí e imprecisa figura del periodista, redactor, editor, director, etc. acaba por ser casi imposible de concretar… hasta el momento, las respuestas constitucionales a estos nuevos fenómenos parecen anacrónicas y difícilmente proyectables para el futuro. Se hace referencia al esquema de responsabilidad del Tribunal Constitucional respecto de las *cartas al director*. Los tradicionales sujetos del periodismo clásico pueden identificarse ya en muy pocos casos de los nuevos fenómenos de internet"[7].

La cuestión es tan interesante que todavía se están debatiendo en distintas latitudes, por ejemplo, qué debe entenderse por periodista y por medio de prensa en un entorno digital (de hecho aunque no cabe duda que las versiones digitales de los medios de prensa institucionales gozan de las mismas garantías que sus versiones originales, pueden encontrarse muy interesantes debates relacionados con la eventual asimilabilidad entre las páginas web o blogs no pertenecientes a medios de comunicación institucionalizados y éstos); a qué supuestos de las comunicaciones realizadas a través de Internet pueden extenderse las garantías típicas de la libertad de prensa (v.gr., la confidencialidad de las fuentes de información, la prohibición de someter a esos medios a la jurisdicción federal, la aplicación de la teoría de la real malicia para juzgar la responsabilidad por informaciones agraviantes, etc.), y si son aplicables ciertas normas tuitivas previstas en favor de los particulares respecto de las publicaciones de los medios tradicionales (como el "derecho de réplica"), a nuevas formas y espacios de comunicación, como twitter[8].

---

[7] Lorenzo Cotino Hueso, "Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los "blogs")", en AA.VV. Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías, Facultad de Derecho de Burgos, Burgos, 2005, disponible en línea en http://documentostics.com/component/option.com_docman/task.doc_view/gid.7/.

[8] Sobre estos dos aspectos, ver, entre otros, los artículos ubicados en www.eluniversal.com/2010/10/31/int_art_tribunal-electoral-d_2082870; www.ernestovillanueva.blogspot.com.ar/2013/03/derecho-de-replica-y-aclaracion-en.html.

Acerca de los nuevos contornos del "derecho de daños en la sociedad de la información", recuerda Peguera Poch que hacia el ámbito de las comunicaciones electrónicas se trasladaron muchas de las actividades que hasta ahora estaban enmarcadas en un escenario físico, y que n un escenario en el que ya no hay fronteras ni largas distancias, y que en todos los momentos históricos marcados por la innovación y el progreso industrial y tecnológico, el sistema de responsabilidad civil, o en sentido más general el derecho de daños, emerge con un protagonismo especial, estableciendo una serie de reglas que son claves para el desarrollo y puesta en marcha de las nuevas actividades y tecnologías (nuevas fuentes de riesgos y de potenciales daños), redefiniendo con mayor precisión los supuestos resarcibles, y en qué medida, en qué condiciones y con qué requisitos lo serán, jugando así este sistema el difícil papel de distribuir entre los diferentes sujetos implicados la carga de los costes asociados al desarrollo y a la aplicación de los nuevos progresos. Asimismo, debe establecer "los mecanismos jurídicos oportunos que incentiven a los operadores a adoptar medidas adecuadas de prevención para reducir al máximo el número de accidentes y daños... conjugando adecuadamente los intereses en presencia [y determinando] hasta qué punto una carga excesiva en términos de responsabilidad por daños podría poner (o no) en peligro la propia consolidación o expansión de los operadores económicos que tienen que hacer realidad la nueva economía. En otras palabras: de qué límites, en términos de responsabilidad, podrá (o no) disfrutar el prestador de un determinado tipo de servicios… en particular en los denominados servicios intermediarios de la sociedad de la información [por] la importancia decisiva de estos servicios para el funcionamiento de la red…"[9].

Algunos ordenamientos jurídicos han regulado expresa y más o menos precisamente las obligaciones que les cabe a estos servicios, a fin de brindar cierto marco de seguridad y previsibilidad a quienes los operan y a quienes pudieran ver afectados por el accionar de aquellos (v.gr., Comunidad Europea, España); otros sólo han dictado algunas reglas limitadas para determinadas áreas, dejando amplio margen a la jurisprudencia (v.gr., Estados Unidos), y en algunos casos sólo se han dictado normas que intentan extender ciertas garantías previas al caso de Internet (v.gr., Argentina).

[9] Miquel Peguera Poch, "Mensajes y mensajeros en Internet: la responsabilidad civil de los proveedores de servicios intermediarios" (2001), en http://www.uoc.edu/web/esp/art/uoc/0103008/peguera.html.

En este contexto, sentencias con diferentes contenidos y a veces con sentidos contradictorios, han ido resolviendo –con mayor o menor fortuna- los principales conflictos surgidos al calor del uso de los servicios de la sociedad de la información. El objetivo de este trabajo es abordar algunas de ellas, dictadas en ordenamientos que no cuentan con bases normativas comunes.

## 2. NORMATIVA COMUNITARIA EUROPEA.

En el ámbito comunitario, además de las prescripciones específicas del Convenio Europeo, se dictaron otras más específicamente relacionados con la temática *sub examine*, entre otras, la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos"; la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 08/06/00, "relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior", y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12/07/02, sobre la protección de la intimidad en el entorno digital, normas que como consecuencia llevaron a la aprobación de normas nacionales de transposición (v.gr., en España, las leyes de protección de datos de 1992 y 1999, y la de Servicios de la Sociedad de la Información y de Comercio Electrónico, 34/2002).

Estas "normas marco" han sido interpretadas por la doctrina y por la jurisprudencia, aspectos de los que nos ocuparemos de inmediato, aclarando que si bien son las vigentes al momento de conclusión de este trabajo, resultaba inminente en tal tiempo la aprobación de otras dos normas con seguro impacto en la temática, en concreto: el "Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)"[10] y la "Propuesta de Directiva del parlamento europeo y del consejo

[10] "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)" 2012/0011 (COD), en http://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-regulaztion/. Esta

relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos"[11].

### 2.1. **SU INTERPRETACIÓN DOCTRINARIA**

Al calor de sus principales propósitos[12], la específica Directiva 2000/31/CE, en lo que aquí nos interesa, refiere a este tipo de servicios especialmente entre los arts. 12 y 14, estableciendo distintos tipos de responsabilidades según se trate de servicios de transmisión y acceso a los datos, de *caching* (el almacenamiento automático y provisional de datos) y de *hosting* (el alojamiento de datos), definiendo los supuestos que configuran dicha responsabilidad y los de exención de ella.

A fin de evaluar ese sistema de exenciones de responsabilidad establecido para estos servicios, resulta relevante primeramente tener en cuenta -como lo explica Peguera Poch- que la directiva trata separadamente distintas actividades intermediarias de los "prestadores de servicios intermediarios de la sociedad de la información", y que si bien no establece propiamente una regulación general de la responsabilidad de los prestadores de servicios intermediarios, fija a favor de tales prestadores unos ámbitos concretos de exención de responsabilidad que constituyen una especialidad respecto del régimen general de responsabilidad, para las cuales se ha tenido en cuenta la verdadera naturaleza de los actos que estos operadores lleven a cabo y no sólo a la denominación que quieran dar a su actividad. Agrega que por ello, pese a que unos datos (que conforman un mensaje) sean ilícitos, o causen un daño, y hayan circulado por la red gracias a la intervención de un determinado prestador de servicios intermediarios (que sería el mensajero), éste no necesariamente será responsable de aquellos, ya que en la medida en que la actuación del prestador de servicios se haya limitado a la realización de operaciones puramente técnicas, pasivas

propuesta fue objeto de diversas modificaciones desde su presentación y se encuentra en un estado avanzado en su tramitación, previéndose su aprobación antes de la finalización de 2015.

[11] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0010_/com_com(2012)0010_es.pdf

[12] En concreto: a) evitar que las normativas locales diverjan de tal modo que obstaculicen el mercado interior, provocando distorsiones en la libre competencia o dificultando los servicios transfronterizos, y b) fijar ciertas bases que faciliten el arribo a acuerdos voluntarios que establezcan mecanismos rápidos y fiables para la retirada o bloqueo del acceso en relación a los contenidos ilícitos

y automáticas, o en la medida en que observe determinados deberes de diligencia, la directiva lo exime de responsabilidad, bajo ciertas condiciones[13].

Siguiendo con el esquema de análisis propuesto por el autor en función del orden normativo previsto en la Directiva, cabe ponderar primeramente que en el caso del prestador de servicios de mera transmisión de datos (*mere conduit*) y de provisión de acceso, el legislador comunitario lo exime de responsabilidad, cuando el prestador de tales servicios: a) no haya originado él mismo la transmisión (lo que debe entenderse en el sentido de que el prestador de servicios no debe ni ser el creador del contenido de la transmisión, ni tampoco debe ser él quien tome la iniciativa de realizar una concreta transmisión, ya que esta decisión la toma el destinatario del servicio, que es quien suministra los datos y pide que se transmitan); b) no haya seleccionado al destinatario de la transmisión, y c) no haya seleccionado ni modificado los datos de la transmisión. Exención que abarca también a las operaciones técnicas y pasivas de almacenamiento automático, provisional y transitorio de los datos transmitidos, siempre que este almacenamiento sirva

[13] Agrega el autor que el sentido de establecer esas exenciones se basa en la posibilidad de imputación de responsabilidad en función del nexo causal, puesto que cualquier daño concreto producido en o a través de la red habrá tenido como una de sus concausas necesarias (o *sine qua non*) la actuación de un prestador de servicios intermediarios, pues sin éste el elemento dañoso no habría podido hacerse presente ni circular en la red. Y explica que si se tiene en cuenta la teoría de la equivalencia de las condiciones, donde todos los factores causales concurrentes implican la responsabilidad de sus agentes, entonces el servicio llevado a cabo por el prestador intermediario habrá constituido un elemento suficiente como para imputarle el deber de resarcir y ello llevaría a imputaciones de responsabilidad exageradas, de muy difícil justificación. Por ello, con frecuencia se ha entendido que para imputar responsabilidad no basta con que la actuación del agente haya sido un factor causal *sine qua non* en relación con la aparición del resultado dañoso que la víctima no esté obligada a soportar. Será necesario, además, que el daño fuera previsible. Esto es, que el agente, en el momento de llevar a cabo su acción u omisión, pudiera prever (tuviera la posibilidad razonable de prever) los resultados dañosos —considerados abstractamente— que pudieran llegar a derivarse de su actuación. Así, el agente no tendrá que responder de los daños que superen los límites de lo que era razonable prever, a pesar que su actuación haya constituido uno de los elementos necesarios del conjunto de circunstancias causales, esto es, a pesar de existir relación de causalidad entre su acción/omisión y el daño. Finaliza sosteniendo que parece, por tanto, imprescindible, a los efectos de establecer satisfactoriamente la imputación del deber de resarcir, valorar la distinta relevancia de cada una de las acciones u omisiones que han contribuido a la aparición del daño, y que en este sentido, a veces se formula la distinción entre causas próximas, que comportarían responsabilidad, y causas remotas, que no implicarían el deber de reparar, y se ha dicho también que el agente sólo podrá ser considerado responsable cuando haya desplegado una acción u omisión que constituya causa adecuada para la producción del daño, entendiendo por tal aquella acción u omisión que con gran probabilidad producirá un daño, sin necesidad de particulares alteraciones inesperadas de curso causal, por lo que, de este modo, sólo quien ha puesto en marcha una causa adecuada deberá responder del daño, y no responderán del mismo los agentes de aquellas otras concausas, que, no obstante ser causas *sine qua non* en el caso concreto, no resultan abstractamente y *ex ante* adecuadas para generar responsabilidad en relación con este tipo de daños. (Miquel Peguera Poch, "Mensajes y mensajeros en Internet: la responsabilidad civil de los proveedores de servicios intermediarios" (2001), en http://www.uoc.edu/web/esp/art/uoc/0103008/peguera.html).

exclusivamente para ejecutar la transmisión a la red de comunicaciones, y que su duración no supere el tiempo razonablemente necesario para dicha transmisión –ello aunque advierte que esta exclusión de responsabilidad no afectará a la posibilidad de que los tribunales o autoridades administrativas exijan a un prestador de servicios intermediarios que impida o ponga fin a una infracción (art. 12.3), de modo que si los continua prestando ya no podrá hacer uso de la exención de responsabilidad-.

Ya con respecto al *caching* (almacenamiento en memoria caché), la directiva dispone que el prestador del servicio no podrá ser considerado responsable del almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de éstos (art. 13), siempre que no modifique la información (art. 13.1.a) y: a) cumpla con las condiciones de acceso a la información establecidas por el propietario del sitio original (art. 13.1.b); b) cumpla con las normas relativas a la actualización de la información especificadas de manera ampliamente reconocida y utilizada por el sector (art. 13.1.c); c) no interfiera en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector con la finalidad de obtener datos sobre la utilización de la información –esto porque muchas visitas se hacen en la copia caché y al titular de la web le interesa saber cómo, cuándo, quién, y sobre todo cuántas veces, se consulta su página- (art. 13.1.d); d) actúe con prontitud para retirar la información que haya almacenado, o hacer que sea imposible acceder a ella, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se hallaba inicialmente, o de que se ha imposibilitado el acceso a la misma, o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir el acceso a la misma (art. 13.1.d). Además, al igual que en el caso anterior, se establece también aquí que esta exención de responsabilidad no afectará a la posibilidad de que los tribunales o autoridades administrativas, de acuerdo con los sistemas jurídicos de los Estados miembros, exijan a un prestador de servicios intermediarios que impida o ponga fin a una infracción.

Finalmente, en el caso del servicio de alojamiento de datos facilitados por el destinatario del servicio de forma que puedan ser consultados a través de la red, la directiva eleva notablemente los requisitos subjetivos que deben concurrir en la actuación del prestador de servicios para que de ella no pueda derivarse

responsabilidad, exigiéndole a tal fin: a) la falta de conocimiento efectivo de la ilicitud de la actividad o de la información que aloja, y en particular, ante una acción de reclamación de daños y perjuicios, no haber tenido conocimiento de hechos o de circunstancias por las cuales se revele el carácter ilícito de la actividad o de la información, y b) desplegar una actividad positiva tan pronto como el prestador de servicios tenga conocimiento de aquellos extremos; actividad que consiste en actuar con prontitud para retirar los datos, o bien hacer que el acceso a los mismos sea imposible. Para que opere la exención debe existir una verdadera independencia entre el prestador del servicio de alojamiento y el destinatario que lo solicita, pues si este último actúa bajo la autoridad o el control del prestador de servicios, la exención de responsabilidad no será aplicable, y como en los casos anteriores, esta exención no afecta ni la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios poner fin a una infracción o impedirla, ni la de que los Estados miembros establezcan procedimientos que por los que se rija la retirada de los datos o el hecho impedir el acceso a los mismos (art. 14)[14].

También resulta pertinente advertir que, como también lo señala el autor: a) en los casos de servicios de alojamiento de datos la exención de responsabilidad del prestador del servicio se mueve entre dos extremos: o bien el prestador no tiene conocimiento del carácter ilícito de la actividad o de la información, quedando en tal caso cubierto por la exención; o bien tan pronto como tiene conocimiento de la ilicitud desarrolla una actividad diligente de retirada de los datos o de bloqueo del acceso, con lo que resultará también cubierto por la exención; b) entre el conocimiento y el desconocimiento existe una gran zona gris, que es la situación en la que se halla el prestador que ignora culpablemente, y razona que esta ignorancia puede a veces parecer precisamente una falta de diligencia en el sentido de no haber tomado ninguna iniciativa para conocer si la información alojada era o no ilícita, de modo que cabe preguntarse acerca de si el régimen que establece la directiva deja espacio para que los Estados miembros impongan al prestador, como deber de diligencia, la obligación de inspeccionar o examinar los datos que aloja al efecto de conocer si la actividad o la información es o no ilícita, asunto sobre el cual concluye

[14] Miquel Peguera Poch, "Mensajes y mensajeros en Internet: la responsabilidad civil de los proveedores de servicios intermediarios" (2001), en http://www.uoc.edu/web/esp/art/uoc/0103008/peguera.html.

el autor en que es preciso distinguir entre obligaciones de carácter general y obligaciones específicas, y entonces, de acuerdo con el artículo 15.1 de la directiva, los Estados miembros no pueden imponer a los prestadores de servicios una obligación general, ya sea de supervisar los datos que transmitan o almacenen, ya sea de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas en relación a los servicios de alojamiento, y también en los de transmisión de datos, de provisión de acceso a la red y de *caching*, pero igualmente la directiva no excluye la posibilidad de establecer obligaciones de supervisión que no sean de carácter general (por ejemplo obligaciones de supervisión del contenido procedente de algún sitio determinado de la red) ni pone impedimento alguno a los Estados miembros para establecer obligaciones de comunicación, ya que concretamente prevé la posibilidad de que los Estados exijan a los prestadores de servicios de la sociedad de la información que comuniquen con prontitud a las autoridades los datos presuntamente ilícitos o las actividades ilícitas llevadas a cabo por los destinatarios de sus servicios; o también que les impongan la obligación de comunicar a las autoridades, a solicitud de éstas, información que permita identificar a los destinatarios de sus servicios con los que hayan celebrado acuerdos de almacenamiento (cfr. art. 15.2), de modo que son muchos, pues, los aspectos en los que el legislador comunitario deja un amplio margen de decisión a los Estados[15].

### 2.2. **SU APLICACIÓN –E INTERPRETACIÓN- JURISPRUDENCIAL**

En los asuntos de "Google France" y "Louis Vuitton", la Gran Sala del Superior Tribunal de Justicia de la Unión de la Unión Europea, en sentencia del 23/03/10 señaló que el art. 14 de la Directiva 2000/31/CE "debe interpretarse en el sentido de que la norma que establece se aplica al prestador de un servicio de referenciación en Internet cuando no desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados. Si no desempeña un papel de este tipo, no puede considerarse responsable al prestador de los datos almacenados a petición del anunciante, a menos que, tras llegar a su conocimiento la ilicitud de estos datos o de las actividades del anunciante, no actúe con prontitud para retirar los datos o hacer

[15] Miquel Peguera Poch, "Mensajes y mensajeros en Internet: la responsabilidad civil de los proveedores de servicios intermediarios" (2001), en http://www.uoc.edu/web/esp/art/uoc/0103008/peguera.html.

que el acceso a ellos sea imposible"[16].

En 16/02/12, el Tribunal de Justicia de la Unión Europea resolvió una cuestión prejudicial en la cual se declaró contrario a la normativa comunitaria el requerimiento judicial que ordenara a un prestador de servicios de alojamiento de datos establecer sistemas de filtrado para bloquear la transmisión de archivos que vulneraran los derechos de autor, porque ello podría vulnerar la libertad de información, "dado que se corre el riesgo de que el citado sistema no distinga suficientemente entre contenidos lícitos e ilícitos, por lo que su establecimiento podría dar lugar al bloqueo de comunicaciones de contenido lícito"[17].

En 13/05/14, en "Costeja" el Superior Tribunal de Justicia de la Unión Europea dictó sentencia en el asunto relacionado con Google Spain SL y Google Inc, la Agencia Española de Protección de Datos y Mario Costeja González, y en esencia dispuso: a) la actividad de los motores de búsqueda como Google constituye un tratamiento de datos de carácter personal, del que es responsable el propio motor, dado que éste determina los fines y los medios de esta actividad, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado; b) ese tratamiento está sometido a las normas de protección de datos de la Unión Europea, dado que Google ha creado en un Estado miembro un establecimiento para la promoción y venta de espacios publicitarios y cuya actividad se dirige a los habitantes de ese Estado; c) las personas tienen derecho a solicitar del motor de búsqueda, con las condiciones establecidas en la Directiva de protección de datos, la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexación; en caso de no atenderse su solicitud, las personas tienen derecho a recabar la tutela de la AEPD y de los Tribunales; d) el derecho a la protección de datos de las personas prevalece, con carácter general, sobre el "mero interés económico del gestor del motor de búsqueda" salvo que el interesado tenga relevancia pública y el acceso a la información esté justificado por el interés público; e) a fin de viabilizar el pedido se tiene que analizar en concreto "si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no

[16] Asuntos acumulados C-236/08 y C-238/08.
[17] Asunto C-360/10.

esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado; f) puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona; g) Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate", y h) de cumplirse los requisitos para el ejercicio de estos derechos, "el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita".

Ya en el ámbito del Tribunal Europeo de Derechos Humanos, la Sala Primera de este tribunal y luego la Gran Sala dictaron –en 2013 y 2015, respectivamente- dos sentencias concordantes en "Delfi AS vs. Estonia", al evaluar la responsabilidad de los portales de información frente a los comentarios que realizan los lectores a noticias publicadas en el sitio, confirmando la condena que realizaron los tribunales nacionales estonios, sentencia que se alinea con la teoría -que se utiliza tanto en lo civil como en lo penal- que responsabiliza a quien, debiendo sospechar una violación a la ley, decide no investigar –conocida como la de la "ceguera voluntaria" (*willful blindness*)-, que ha tenido recepción normativa en el ámbito penal, en el art. 28 del Estatuto de Roma[18] y en el caso "Hard Rock Café"[19].

[18] En lo pertinente, la norma dispone: "Responsabilidad de los jefes y otros superiores… Además de otras causales de responsabilidad penal de conformidad con el presente Estatuto por crímenes de la competencia de la Corte... 2. En lo que respecta a las relaciones entre superior y subordinado distintas de las señaladas en el apartado a), el superior será penalmente responsable por los crímenes… que

El caso originado en Estonia se relacionó con el más importante portal de noticias de ese país ("Delfi.ee"), que fue localmente condenado a abonar una indemnización a un particular perjudicado por comentarios enviados por varios lectores al portal y publicados en el sector precisamente destinado a insertar dichos comentarios relacionados.

La noticia que desató tales comentarios fue un artículo que el portal titulara "*SLK broke the planned ice route*", en el cual se daba cuenta de la destrucción accidental de una carretera de hielo que, en invierno, une el continente con algunas islas, y se indicaba como responsable a la empresa de ferris SLK, que cubre el mismo trayecto y que resultaba directamente beneficiada por el hecho (con perjuicio notorio para la comunidad puesto que el costo de ese servicio era mayor al que se tenía si se cruzaba por aquella carretera). Tal publicación –como era lógico esperar- desató muchos comentarios de los lectores, entre ellos una veintena injuriosos y que apuntaban contra el principal accionista de la empresa (refiriendo incluso a su origen judío), quien solicitó y obtuvo (en el mismo día en que lo pidió) el retiro de esos comentarios insultantes, pero también pretendió que el portal se hiciera cargo de una indemnización (a la cual no accedió) de unos 32.000 euros por daños morales.

Al tiempo de los hechos, entre las múltiples funciones que tenía el portal, se permitía a los lectores enviar comentarios sobre los artículos publicados y se los publicaba sin requerirles identificación a los remitentes y de manera automática, aunque existían algunas medidas tendientes a prevenir daños provocados por esos comentarios, en concreto al disponerse de: a) un filtro de mensajes que automática y previamente a la publicación detectaba los que contenían palabras inapropiadas y los descartaba, y b) un sistema de eliminación inmediata de mensajes perjudiciales, que se activaba a partir de la notificación del carácter ofensivo de los mensajes y del cual podía hacer uso tanto el ofendido como cualquier lector.

---

hubieren sido cometidos por subordinados bajo su autoridad y control efectivo, en razón de no haber ejercido un control apropiado sobre esos subordinados, cuando: a) Hubiere tenido conocimiento o deliberadamente hubiere hecho caso omiso de información que indicase claramente que los subordinados estaban cometiendo esos crímenes o se proponían cometerlos…"

[19] En el caso, proveniente de la jurisprudencia estadounidense, el Séptimo Circuito aplicó este criterio a la responsabilidad de un operador de un mercado de pulgas, donde se vendían mercaderías falsificadas de la marca "Hard Rock Café", el tribunal sostuvo que si bien no había ninguna prueba directa de que hubiese tenido conocimiento efectivo de esas ventas, el administrador era concurrentemente responsable con los vendedores de esas mercaderías si se encontraba que permitió la consumación de esos actos ilícitos dentro de sus instalaciones si tenía razones para saber que se estaba actuando o se actuaría ilegalmente ("Hard Rock Café", 955 F. 2d 1143)

Tramitado el pleito en Estonia, la demanda fue primeramente rechazada en baja instancia por considerar al portal exento de responsabilidad a la luz de la Directiva Europea sobre Comercio Electrónico. Sin embargo, tal criterio no fue confirmado en segunda instancia, lo que llevó al dictado de un nuevo fallo de primera instancia, que fuera luego confirmado por la Alzada y por el Tribunal Supremo de Estonia, y en el cual se entendió que a Delfi no le eran aplicables las exenciones de responsabilidad previstas en tal directiva y por ello debía considerársela autora de los comentarios escritos por los lectores y no un intermediario neutro, ya que invitaba a los usuarios a enviar comentarios, de modo que debía considerarse proveedor de contenidos y no prestador intermediario de servicios de la sociedad de la información, y para que las exenciones de la Directiva le fueran aplicables el proveedor no debía tener conocimiento ni control sobre la información transmitida o almacenada, cosa que no ocurriría en este caso, ya que Delfi tenía ese control a punto que podía retirarlos si así lo decidía mientras que el usuario no podía ni modificar ni borrar sus propios comentarios una vez publicados. Se evaluó especialmente que resultaban insuficientes los mecanismos adoptados para eliminar la responsabilidad de Delfi, y que en el caso se vulneró la obligación legal de evitar la causación de daños a terceros al permitirse la publicación de los comentarios y no retirárselos por propia iniciativa, y en consecuencia se la condenó por incurrir en culpa *in vigilando*, fijándose la indemnización en una cifra muy poco significativa (320 euros, en concreto una suma diez veces inferior a la pretendida).

La decisión fue recurrida por Delfi ante el Tribunal Europeo de Derechos Humanos (TEDH), argumentando que se vulneraba su derecho a la libertad de expresión (art. 10, CEDH) y que al generarse esa obligación de censura preventiva de los comentarios de terceros se vulneraba su derecho a "comunicar informaciones o ideas".

Al resolver el asunto, la Sala Primera del TEDH (cuya decisión fue luego recurrida ante la Gran Sala del Tribunal) señaló preliminarmente que no era su tarea sustituir a los tribunales nacionales en el rol de interpretar su legislación interna, y que en el caso se daban las condiciones previstas en la Convención Europea de Derechos Humanos para que se produjera una interferencia aceptable a la libertad de expresión, desde que estaba en juego la reputación de una persona que resultó aludida en los comentarios, y por ello rechazó el recurso sosteniendo que para que tal libertad de

expresión, en cabeza de Delfi (en el sistema europeo las personas jurídicas están legitimadas para acceder al tribunal comunitario) pueda ser interferida, la limitación debe estar: a) prevista por la ley; b) obedecer a uno de los motivos legítimos considerados en dicho precepto, y c) resultar necesaria en una sociedad democrática (art. 10.2 CEDH), condiciones que a entender del tribunal efectivamente se habían acreditado en el caso concreto[20].

En realidad, el Tribunal no analiza si a partir del Convenio, existe una obligación general de impedir los comentarios difamatorios sino que se limita a considerar si la interferencia ha sido proporcionada en el caso concreto, y entiende que, al publicar el artículo sobre los ferris, Delfi tenía que haberse dado cuenta de que podría originar reacciones negativas por parte del público en contra de la empresa de ferris, y que existía un riesgo mayor al habitual de que los comentarios se excedieran de los límites de la crítica aceptable, incurriendo en injurias, de modo que "era esperable que en las circunstancias del presente caso [Delfi] ejerciera una cierta cautela para no ser declarada responsable de una infracción de la reputación de otras personas", aunque se dice que, en función de las medidas técnicas que había adoptado, Delfi no fue completamente negligente en su deber de evitar causar daño a la reputación de terceros, y reconoce que en cuanto el agraviado notificó a Delfi la presencia de los comentarios dañinos, el portal los retiró sin demora, pero estuvieron accesibles durante seis semanas. "[Delfi] -y no la persona cuya reputación pudiera estar en juego- estaba en condiciones de saber que se publicaría un artículo, de predecir la naturaleza de los posibles comentarios suscitados por el mismo y, sobre todo, de adoptar las medidas técnicas o manuales para impedir que se publicaran manifestaciones difamatorias".

Agrega que el portal tendría interés en que hubiera muchos comentarios, porque

[20] Sobre el primer aspecto (la previsión de ley), el tribunal no entra a valorar si la responsabilidad de Delfi debería haber quedado excluida en virtud de las normas sobre responsabilidad de los intermediarios derivadas de la Directiva de Comercio Electrónico, sino que señala que los tribunales nacionales han llegado a la conclusión de que tales normas no eran de aplicación a Delfi, por carecer de la necesaria neutralidad, y que el TEHD no puede suplir a los órganos domésticos en esta valoración, limitándose su papel a valorar si los efectos de sus resoluciones son incompatibles con el Convenio, por lo que se cumplía con el recaudo de excepción prevista en ley si la imputación de la responsabilidad se basa en las leyes estonias, y según ella Delfi es un medio de comunicación y por ello debe ser responsable de cualquier manifestación difamatoria que se realice, resultaba aplicable tal régimen como empresa periodística.
Sobre el segundo aspecto (la existencia de alguno de los motivos legítimos), el tribunal lo encuadra en el objetivo de "la protección de la reputación o de los derechos ajenos".
Por último, entiende que efectivamente la restricción es una medida necesaria en una sociedad democrática según lo entiende Estonia.

estos atraen audiencia y por tanto publicidad, y que dada la dificultad de su identificación, no resultaba factible la alternativa de demandar a los ignorados autores de los comentarios, siendo "decisión de la compañía recurrente la de admitir comentarios de usuarios no registrados, y que al hacerlo debe entenderse que ha asumido una cierta responsabilidad por dichos comentarios". Por lo demás, dijo el tribunal que si bien existe una gran facilidad para publicar en la red y por ello gran cantidad de información que hace difícil detectar y retirar mensajes difamatorios, lo que hace que esta tarea sea ardua para el operador de un portal de noticias, aún es más gravosa para la persona potencialmente agraviada, que carecerá de los medios para supervisar continuamente la red.

El tribunal ponderó por último que las consecuencias que del fallo se derivan para el portal no son especialmente gravosas, ya que: a) los tribunales domésticos no le obligan a establecer medidas concretas, sino que dejan a su criterio el modo de impedir la publicación de comentarios injuriosos, y b) la cuantía de la indemnización fue escasa; c) se está ante un operador profesional del portal.

Dictado el fallo, Delfi solicitó la revisión del caso ante la Gran Sala, recurso que fue apoyado por el Centro de Derechos Humanos de la Universidad de Ghent (Human Rights Centre –HRC- of Ghent University) a través de una carta dirigida a la Corte y firmada conjuntamente por organizaciones de 69 medios de comunicación, empresas de Internet, grupos de derechos humanos e instituciones académicas, en la cual se señalaba que la sentencia tendría repercusiones adversas graves para la libertad de expresión y en la apertura democrática en la era digital. El 17/02/14 el panel de cinco jueces, en aplicación del artículo 43 de la Convención decidió la remisión del caso a la Gran Sala, que en su sentencia de 16/06/15 confirmó lo decidido, convalidando lo que a su criterio era una justificada y proporcionada restricción a la libertad de expresión a un portal de noticias que en definitiva no había adoptado medidas suficientes para eliminar una veintena de comentarios ofensivos pese a que era gestionado por profesionales y con una base comercial.

La Gran Sala compartió la opinión de que Delfi era responsable, como editor, de haber hecho accesible por algún tiempo los comentarios groseramente insultantes en su sitio web, ya que Delfi ejercía un grado sustancial de control sobre los comentarios publicados en su portal y su rol fue "más que meramente pasivo, puramente proveedor de servicio técnico" (§ 146). Hizo además alusión a los "deberes

y responsabilidades" de los portales de noticias de Internet en el marco del art. 10 § 2 de la Convención, cuando se proporciona, con fines económicos, una plataforma para comentarios de los usuarios y algunos de ellos -identificados o anónimos- participan en ella con expresiones que afectan a los derechos de la personalidad de los demás e incitan al odio y a la violencia contra ellos[21].

La Gran Sala afirmó además que esta restricción justificada y proporcionada a la libertad de expresión del portal está de acuerdo en que la Ley de Servicios de la Sociedad de la Información, que transpone la Directiva sobre el comercio electrónico (2000/31 / CE) a la legislación estonia, incluidas las disposiciones sobre la responsabilidad limitada de los ISP, no se aplica al presente caso ya que esta última relacionada con las actividades de una naturaleza meramente técnica, automática y pasiva, mientras que las actividades de Delfi reflejan los de un editor de medios, la ejecución de un portal de noticias de Internet.

Dijo también que la injerencia de las autoridades estonias en la libertad de expresión de Delfi era suficientemente previsible y justificada por el objetivo legítimo de proteger la reputación y los derechos de los demás, ello más allá de los importantes beneficios que se pueden derivar del uso de internet en el ejercicio de la libertad de expresión, porque las afirmaciones difamatorias y otros tipos de discursos ilegales deben, en principio, ser retenidos, y constituyen un remedio eficaz para evitar violaciones de derechos de la personalidad.

Se hizo hincapié en la decisión en que el portal era gestionado por profesionales y sobre una base comercial, con un importante grado de control sobre los comentarios y que pese a ello se publicó un reportaje en el que se invitó a los lectores a opinar sobre ellos, habiendo descuidado –aunque no por completo- su obligación de no causar daños a terceros (se destaca que los comentarios permanecieron durante seis semanas), ya que el filtro basado en el control de las palabras utilizadas falló para seleccionar y eliminar las expresiones evidentes de odio que incitaban a la violencia publicadas por los lectores (contenidos no amparados por el art. 10 de la Convención),

[21] En este aspecto, señaló el tribunal: "Donde los comentarios de los usuarios respecto de terceros se realizan en forma de expresiones de odio y amenazas directas a la integridad física de las personas, tal como se entiende en la jurisprudencia del Tribunal de Justicia (...), los derechos e intereses de terceros y de la sociedad en su conjunto puede dar derecho a los Estados contratantes a imponer responsabilidad en los portales de noticias de Internet, sin contravenir el artículo 10 de la Convención, si no toman medidas para eliminar los comentarios claramente ilegales sin demora, incluso sin previo aviso de la presunta víctima o de terceros"(§ 159)

sin que en el caso se observaran metáforas sofisticadas, significados ocultos o amenazas sutiles.

Agregó la Gran Sala que un portal de noticias grande tiene la obligación de tomar medidas efectivas para limitar la difusión de mensajes de odio e incitación a la violencia, y que la capacidad de una víctima potencial del discurso del odio para monitorear continuamente los contenidos de Internet es más limitado que la capacidad de un gran portal de noticias de Internet, de carácter comercial, para prevenir o eliminar dichos comentarios rápidamente, y finaliza destacando que la compensación de € 320 que Delfi había visto obligado a pagar por concepto de daño inmaterial, no debía ser considerado como una interferencia excesiva con el derecho a la libertad de expresión de la compañía de medios.

También el tribunal consideró que lo resuelto en el caso Delfi no concierne a "otros foros en Internet" donde los comentarios de terceros pueden ser difundidos, por ejemplo, un foro de discusión o un tablón de anuncios donde los usuarios pueden libremente exponer sus ideas sobre cualquier tema si la discusión no se canaliza mediante el gerente del foro, de modo que la constatación del Gran Sala no es aplicable a una plataforma de medios sociales en el que el proveedor de la plataforma no ofrece ningún contenido ni al caso en el que el proveedor de contenidos sea una persona privada que lleva como *hobby* un sitio web o un blog, que no se asemejan a un portal de noticias de Internet gestionado por profesionales y sobre una base comercial, aunque como los dos jueces discrepantes observan: "La libertad de expresión no puede ser una cuestión de una afición".

Finalmente, la Gran Sala resaltó que en el caso el carácter ilegal de los comentarios no requerían ningún análisis lingüístico o jurídico por parte de Delfi, de modo que la sentencia impone una forma de "censura privada", sino que requiere la adopción de medidas de interferencia y remoción de contenido tomadas por iniciativa de los proveedores de plataformas en línea, a fin de proteger los derechos de las personas afectadas, lo que crea un nuevo paradigma para los medios de comunicación participativos en línea[22].

[22] http://strasbourgobservers.com/2015/06/18/delfi-as-v-estonia-grand-chamber-confirms-liability-of-online-news-portal-for-offensive-comments-posted-by-its-readers/.

## 2.3. **LAS NORMAS DE TRANSPOSICIÓN NACIONALES Y SU APLICACIÓN JURISPRUDENCIAL**

Como se expresó *supra*, las Directivas europeas obligan a la adaptación o, en su caso, al dictado, de normativas nacionales compatibles con aquella.

En este contexto, v.gr., la "*Multimedia Act*" alemana establece diferentes tipos de responsabilidades según se trate de *Information Providers* (que tienen plena responsabilidad por los contenidos) o de *Hosting Providers* o de *Access Providers*, que sólo lo son si tienen conocimiento de los contenidos y no tomaron las medidas técnicas adecuadas frente a tal conocimiento; que en la jurisprudencia inglesa, como lo relata Melo se sigue este mismo criterio[23]. Y en España, la "Ley de Servicios de la Sociedad de la Información y Comercio Electrónico" (LSSICE, n° 34/02, modificada por la ley nº 56/07), establece una serie de reglas que rigen el accionar de los servicios de la sociedad de la información y fija los supuestos en los cuales incurren en responsabilidad (arts. 11 a 17, que refieren al deber de colaboración de los prestadores; a la responsabilidad de éstos; de los operadores de redes y proveedores de acceso; de los que realizan copia temporal de los datos solicitados por los usuarios; de los que prestan servicios de alojamiento o almacenamiento de datos y de los que facilitan enlaces a contenidos o instrumentos de búsqueda).

En la jurisprudencia francesa, tal como lo destaca Lipszyc, en "Lynda L. y otros c. Société Multimania Production –medida cautelar–" la Corte de Apelaciones de Versailles, 12e. Chambre, en 08/06/00 con motivo de la transmisión en línea, sin autorización, de fotografías de la accionante en condiciones que involucraban su derecho a la imagen, destacó que: a) la responsabilidad principal del proveedor de contenidos del sitio web "no excluye que se investigue si el comportamiento erróneo del prestador de alojamiento no ha contribuido a causar el perjuicio a la víctima"; b) "a una sociedad que provee alojamiento le cabe la obligación de vigilancia y de prudencia en cuanto al contenido de los sitios que acoge" y dicha obligación de vigilancia y de prudencia "se traduce en una obligación de medios referida a las

[23] Ver: Metropolitan International Schools Ltd. (t/a Skillstrain and/or Train2game) v Designtechnica Corp (t/a Digital Trends) & Ors, Court of Appeal - Queen's Bench Division, July 16, 2009, [2009] EWHC 1765 (QB), texto completo en http://www.5rb.com/case/Metropolitan-International-Schools-Ltd-v-%281%29-Designtechnica-Corporation-%282%29-Google-UK-Ltd--%283%29-Google-Inc, cit por Verónica E. Melo, "Responsabilidad civil del buscador de Internet por contenidos de terceros", en El Derecho - Rosario Digital, publicación del 26/08/13, en https://www.google.com.ar/#q=ver%C3%B3nica+melo+Responsabilidad+civil+del+buscador+de+Internet+por+contenidos+de+terceros.

precauciones y los controles a emplear para prevenir o hacer cesar el almacenamiento de mensajes contrarios a las disposiciones legales vigentes o perjudiciales a los derechos de a los derechos de terceros afectados"; c) "esta obligación de medios, que no implica el examen general y sistemático de los contenidos de los sitios alojados, sin embargo debe traducirse, en la etapa de la formación del contrato con el cliente creador del sitio, en medidas preventivas tales como la prohibición del anonimato o de la no identificación, la adhesión a las reglas de conducta y cualquier otro procedimiento que estimule el respeto a los textos legales y los derechos de las personas, y, en la etapa de la ejecución del contrato, en las diligencias apropiadas para detectar cualquier sitio cuyo contenido sea ilegal, ilícito o perjudicial, a fin de inducir a la regularización o proceder a la interrupción de la prestación", y d) "al margen de los casos en que sean requeridas por la autoridad pública o por resolución judicial, tales diligencias deben ser espontáneamente encaradas por la sociedad proveedora de alojamiento desde el momento en que tiene conocimiento o es informada de la ilegalidad o del carácter dañoso del contenido de un sitio o, cuando las circunstancias o modalidades de realización, evolución o consulta de un sitio –que debe vigilar mediante instrumentos, métodos o procedimientos técnicos de análisis, de observación y de investigación– le creen sospechas sobre el contenido"[24].

En España, las reglas comunitarias no sólo han sido objeto de aplicación por los tribunales españoles como veremos inmediatamente, sino también por la Agencia Española de Protección de Datos, que, v.gr., avaló la decisión de Google Spain de responder negativamente al ejercicio del derecho de oposición articulado por un particular respecto de una noticia que lo afectaba – y que no podía considerarse ni inexacta ni obsoleta- y por el cual pretendía la desindexación de 75 enlaces en los que se daba cuenta de que pesaba sobre él un auto de prisión dictado en 2009 vinculado con un caso de narcotráfico[25]. Por su parte, la jurisprudencia española ha interpretado

[24] Delia Lipszyc, "Responsabilidad de los proveedores de servicios en línea por las infracciones del derecho de autor y derechos conexos en el entorno digital: análisis de la jurisprudencia internacional", documento OMPI-SGAE/DA/ASU/05/7, en http://www.wipo.int/edocs/mdocs/lac/es/ompi_sgae_da_asu_05/ompi_sgae_da_asu_05_7.pdf.

[25] En el marco del procedimiento nº TD/00284/2012, la AEPD, mediante resolución nº R/01754/2012 sostuvo que el denominado "derecho de olvido" no puede convertirse en un instrumento indiscriminado de reescritura de hechos pasados y que la relevancia pública de los hechos narrados y la cercanía temporal de dichos hechos ameritaban la desestimación de la reclamación, resultando además que entre las direcciones web que se pretendían desindexar figuraban blogs y medios de comunicación. Agregó, respecto de los comentarios introducidos en los blogs de Internet por particulares, que el ejercicio del derecho para que se supriman del blog sus datos de carácter personal unidos a los comentarios que sobre él se realizan, debe ejercitarse ante el responsable del fichero, de modo que no procede exigir a

reiteradamente las normas comunitarias -aunque no siempre de manera uniforme-, en un contexto donde al calor de los arts. 13 y 17 de la LSSICE y del art. 15 de la Directiva 2000/31/CE, se busca responsabilizar a estos servicios por los contenidos ajenos que transmiten, alojan o a los que facilitan acceso, sólo cuando toman una participación activa en su elaboración o cuando, conociendo la ilegalidad de un determinado contenido, no actúan con celeridad para retirarlo o impedir el acceso.

Explica al respecto Turiño que al interpretar el juego de estas normas, originariamente los tribunales españoles habían configurado una tímida doctrina respecto del alcance del supuesto del "conocimiento efectivo", donde se requería alguna declaración de órgano competente previa a la demanda en la que se establezca la ilicitud de los datos almacenados o que se ha producido la lesión de los derechos[26], pero luego, tal tendencia primitiva cambió cuando el Tribunal Supremo entendió que dicho conocimiento "no está limitado a los supuestos en los que un órgano competente haya declarado previamente a la demanda la ilicitud de los datos almacenados o que se ha producido la lesión de los derechos de los actores, ordenado la retirada de contenidos, sino que, conforme a la normativa interna y comunitaria, pueden existir otros medios de conocimiento efectivo, como cuando existan circunstancias que posibiliten, aunque sea mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate"[27], quedando ratificado en este contexto la línea que considera que un operador de Internet puede ser responsable de actuaciones de terceros si, por cualquier medio, conoce de su ilicitud y no actúa prontamente en resguardo de los derechos de los afectados[28].

Así, v.gr., en el caso "Ramoncín vs. alasbarricadas.org", el 10/02/11 la Sala de lo Civil del Tribunal Supremo, mediante Sentencia n° 72/2011, analizó el supuesto en

---

Google la eliminación de los citados datos al no ser él el responsable del blog, resultando los comentarios introducidos en los blogs de Internet por los particulares una manifestación de la libertad de expresión proclamada que la Constitución reconoce para cualquier medio, incluso autocreado, de divulgación (sentencia del Tribunal Constitucional 12/82). (http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-00284-2012_Resolucion-de-fecha-09-07-2012_Art-ii-culo-16-LOPD.pdf)

[26] Sentencias de la Audiencia Provincial de Madrid, Sección 9ª, de 19/02/10 en el caso "particulares c/ Google" o el Auto del Juzgado de Instrucción núm. 9 de Barcelona, de 27/03/03, en el caso "ajoderse.com c/Ono".

[27] Doctrina que se fijó a partir del caso "putasgae.com" (sentencia nº 773/2009) y se reiteró en los casos "quejasonline.com" (sentencia nº 316/2010) y "alasbarricadas.org" (sentencia nº 72/2011).

[28] Alejandro Turiño, en Revista Digital ElDerechoInformatico.com, Edición Nº 8, Julio de 2011, en http://www.elderechoinformatico.com/index.php?option=com_content&view=article&id=678:iquien-es-responsable-en-internet-por-alejandro-tourinno&catid=85:articulos&Itemid=107.

el cual se publicaron, respecto de un cantante a su vez miembro de la Sociedad General de Autores y Editores (SGAE) una serie expresiones agraviantes (se lo trataba como “gilipollas”, “tocapelotas”, “imbécil”, “payaso”, etc.) provenientes de miembros del “Foro anarquista para el debate y contacto directo entre compañer@s” y se remitía, en un enlace externo, a una fotografía manipulada. El afectado solicitó el retiro de los contenidos agraviantes, pero ello sólo se efectivizó con el traslado de la demanda y sin que existiera resolución judicial alguna que lo ordenara.

El tribunal señaló que tanto las expresiones vertidas en la “web”, como la fotografía adjunta, implican una clara y evidente lesión al honor del actor, pues excede de la mera crítica o puesta en conocimiento de los demás de una simple información, dado que los mensajes y expresiones son claros insultos, incluso amenazantes para su integridad física, dirigidos simplemente a la vejación y menosprecio del afectado que implican un menoscabo en la fama, buen nombre y prestigio profesional, con independencia de que el mismo haya tenido o mantenga posiciones controvertidas de cara al público, sujetas a crítica y opinión, por la misma posición pública asumida voluntariamente, sobre todo en las polémicas cuestiones referidas a la SGAE.

Se agregó que es absurdo, en el actual mundo de las telecomunicaciones, caracterizado por la facilidad y rapidez de difusión de los datos, remitir al perjudicado a la previa obtención de una declaración formal de ilicitud cuando la intromisión en el derecho fundamental al honor es tan notoria por la calidad de las expresiones utilizadas, y la ilicitud de los materiales alojados es evidente por sí sola desde que no depende de datos o información que no se encuentran a disposición del intermediario, y por ello el prestador del servicio incurre en responsabilidad por no haber cumplido con el deber de diligencia a fin de detectar y prevenir determinados tipos de actividades ilegales.

Se aclaró además que, tal como lo ha destacado la Audiencia Provincial de Madrid en sentencias del 20/12/05 y 06/02/06, el derecho de crítica a la figura del actor en su actividad profesional no ampara ni la fotografía que lo representa con la cabeza cortada ni los ofensivos insultos a la persona misma manifestados por los usuarios de la web sus opiniones, ya que si bien el juicio sobre la actividad y la idoneidad profesional no constituye de suyo una intromisión ilegítima al honor, sí lo es cuando, evaluando las publicaciones dentro del contexto, el lugar y ocasión en que

se vertieron, ellas exceden de la libre evaluación y calificación de la propia labor profesional para encubrir una mofa o descalificación de la persona misma, a través de un lenguaje que se aparta de la neutralidad que supone criticar constructivamente.

A la luz de dicha doctrina y de las previsiones de la LSSICE, se evaluó que por parte del demandado se habían vulnerado las obligaciones impuestas por dicha norma, desde que si bien en principio no debe responder del contenido de las comunicaciones remitidas por terceros a su página web mientras no tenga conocimiento efectivo de que las mismas son ilícitas o lesionan bienes o derechos de distinta persona susceptibles de indemnización; sin embargo sí le es exigible una diligencia mínima para que, de producirse alguna de las situaciones descritas, pueda el perjudicado comunicarse con él de forma fácil y directa para interrumpir la publicación de aquellas manifestaciones verbales o fotográficas que le resulten lesivas, diligencia (prevista en el art. 10 de la LSSICE) que no observó ya que no actualizó los datos del registro que aportó a los organismos administrativos reguladores de su actividad, a efectos de registrar su dominio, y no se corresponden con su actual domicilio, como así tampoco probó (como le compete una vez verificada la lesión a un derecho fundamental al invertirse la carga de la prueba) que la dirección de correo electrónico aportada fuese efectiva para contactar con él ni que fuera imposible contar con un moderador o con filtros de contenidos, lo que implicó asumir y colaborar en la difusión de los mensajes y en prolongar indebidamente en el tiempo su difusión.

Más recientemente, en "SGAE vs. merodeando.com" se planteó una demanda por "atentado al honor" contra la entidad actora (lo que es perfectamente viable ya que la LSSICE se aplica también a las personas jurídicas), a partir de la publicación, por parte del autor del blog, de una breve entrada titulada "SGAE=ladrones" donde se refería al *Google bombing* que una web acababa de iniciar y que tenía por objeto relacionar, como criterio de búsqueda en Google, a la web de la SGAE con la palabra "ladrones".

La entrada recibió un buen número de comentarios de los lectores del blog, incluidos muchos despectivos hacia la SGAE, por lo que la entidad remitió un burofax al titular del blog instándolo a que inmediatamente procediera la eliminación del artículo y sus comentarios incluidos en su página web y frente al incumplimiento, inició la demanda.

La sentencia de primera instancia -en argumentos confirmados en segunda- condenó al demandado a retirar los contenidos denunciados y a indemnizar a la actora con la suma de 9.000 euros, afirmándose que el *blogger* fue "una suerte de colaborador necesario", y que "es claro y evidente (…) que las declaraciones objeto de denuncia, no son realizadas en su integridad por el demandado, quien sí interviene contestando en ocasiones, mas se corresponden con una línea argumentativa que se inicia con la información que el mismo ofrece en el blog que marca e insta a que se viertan opiniones sobre la actuación de la actora que finalmente sobrepasan los límites de una denuncia para derivar en manifestaciones atentatorias a su honor y dignidad tutelables en el ámbito de la ley 1/82".

El Tribunal Supremo, en sentencia n° 742/2012 de 04/12/12, revocó la sentencia de primera instancia, y en consecuencia rechazó la demanda por entender que si bien en abstracto no se cumplió con el requisito de actuar con diligencia para "retirar los datos o hacer imposible el acceso a ellos", o para "suprimir o inutilizar el enlace correspondiente", en realidad: a) la expresión "ladrones" en el lenguaje coloquial no necesariamente refiere a conductas delictivas, sino que abarca también la obtención de beneficios ilegítimos, pero legales y b) si bien dicha expresión podría resultar literal y aisladamente inadecuada, al ser puestos en relación con la información difundida y dentro del contexto en el que se produjeron, esto es, de crítica a la actividad desarrollada por una entidad, no llegan al extremo de impedir el carácter prevalente del derecho a la libertad de expresión sobre el derecho al honor.

Como lo indica Peguera Poch al comentar el fallo, el tribunal reiteró la doctrina ya fijada en sentencias previas (casos "asociación de internautas", "quejasonline" y "alasbarricadas") a favor de una interpretación amplia de la noción de conocimiento efectivo y dio por supuesto que el demandado lo obtuvo dado que en su propia página se indica, a través de enlaces, cómo acceder a otras en las que se proporciona una información explícita sobre la actividad comercial desempeñada por la SGAE y la condición de "ladrones" atribuida, pero novedosamente se extiende la interpretación del "conocimiento efectivo" del art. 16 LSSICE al supuesto de los enlaces, previstos por el art. 17 LSSICE, ya que si bien la definición de dicho conocimiento es idéntica en ambos preceptos, el principal argumento del TS para defender la tesis no limitativa en la sentencia del caso "asociación de internautas" fue que una interpretación estricta sería contraria a la Directiva, cosa que puede sostenerse en relación con el art. 16,

pero no en relación con el art. 17, pues la Directiva no contempla el supuesto de los enlaces[29].

En sentencia aún más reciente, en el caso "Ramoncín vs. eleconomista.es" y en sentencia 1441/13, del 26/02/13, la Sala Civil del Tribunal Supremo abordó la responsabilidad del titular de un medio de comunicación en entorno web por comentarios indudablemente vejatorios enviados por usuarios en un foro de debate abierto de la edición digital del periódico "El Economista" y en relación a la noticia titulada "Los usuarios de Facebook fusilarán virtualmente a Ramoncín", que obviamente también dirigidos contra ese personaje público miembro del SGAE y que lo eran a tal punto que el Tribunal anonimizó su identidad -no con mucha suerte, por el estado público del caso y las características del personaje demandante.

El núcleo de la discusión se afincó en el nivel de diligencia exigible a la web y la aplicación del régimen de exclusión de responsabilidad de los prestadores de servicios de alojamiento de datos previsto en el art. 16 LSSICE.

En primera instancia se condenó al demandado a indemnizar con 10.000 euros al actor ya que a pesar de que no quedaba acreditado que el titular de la web hubiera tenido conocimiento efectivo puesto que la intimación no fue recibida ya que no se dirigió precisamente al demandado sino al periódico y lo había enviado la SGAE y no el afectado, no puede valerse de la exclusión de responsabilidad porque no agotó la diligencia que le era exigible.

La sentencia fue revocada por la Alzada al ponderarse que no hubo falta de diligencia, pero el Tribunal Supremo entendió, en consonancia con lo sostenido por el fiscal en el recurso de casación, que hubo conocimiento efectivo del contenido vejatorio de las opiniones vertidas contra el actor, por ser éste notorio y evidente, de modo que no podía la demandada alegar desconocimiento, ya que como titular de la página web donde se vertieron tales datos, han estado a su disposición, no siendo preciso para su conocimiento, que fuera el demandante, como pretende la sentencia recurrida, quien indicara qué mensajes eran ofensivos, ya que la ilegalidad de los contenidos del foro era claramente patente e incumbe al titular de la web un deber de control de los contenidos potencialmente lesivos.

[29] Miquel Peguera Poch, "Notas sobre la sentencia del caso SGAE contra merodeando" en http://responsabilidadinternet.wordpress.com/2013/01/19/notas-caso-merodeand/.

Se entendió así que en atención a las características del foro en el cual se vertieron los contenidos injuriantes debió ejercerse –y no se hizo- un mayor control para retirar inmediatamente aquellas opiniones claramente ilegales, en conducta infractora agravada por el hecho de rehusarse el burofax circunstancia que "impidió la comunicación del afectado con el prestador y supuso la difusión y prolongación en el tiempo del contenido vejatorio".

Como lo indica Peguera Poch, dado que el TS dice que la sala "atribuye el mismo valor revelador del conocimiento efectivo al contenido y naturaleza de los mensajes, sumamente graves y claramente ofensivos al honor del demandante…", de esta declaración podría inferirse que el TS entiende que no es necesaria ninguna notificación del agraviado, situación que refuerza la idea acerca de que la demandada tenía un deber de control sobre las opiniones alojadas, pues se refiere a que: "la entidad demandada, como titular de la página web y creadora del foro de debate abierto, debió extremar las precauciones y ejercer un mayor control sobre las opiniones y comentarios alojados, cuyas connotaciones despectivas y peyorativas para el demandante no podían pasarle inadvertidas", y se agrega que "[n]o puede pasar inadvertido el papel desempeñado por el titular de la página que no solo alberga un contenido externo, sino que genera la posibilidad realizar comentarios, incorporándolos a la noticia y permite que se consideren como elemento de valoración de la misma", pero esto no queda claro, porque parece conectar el conocimiento con el hecho del envío del burofax que fue rechazado indiligentemente, cuando dice "…sin que pueda alegarse desconocimiento por parte de la entidad demandada a raíz del fax recibido, dado que en él se advertía con claridad la existencia de comunicaciones lesivas del derecho al honor y se reclamaba su retirada, hecho que respondía a la realidad y que impide que el titular de la página web pueda a partir de ese momento desconocer" y luego agrega "Dado que resulta probado que la demandada rehusó recibir el fax remitido por el demandante impidiendo a este poder comunicarse con ella y así conseguir la interrupción de la difusión de los comentarios lesivos y ofensivos para su persona facilitando su prolongación en el tiempo, cabe concluir que la entidad demandada incumplió el deber de diligencia que le incumbía".

Así, continúa el autor, la sentencia plantea importantes interrogantes pues la empresa titular de la web estaba perfectamente identificada y ponía a disposición del público un sistema para contactar con ella por correo electrónico. La situación, por

tanto, no es equivalente a la del caso "*alasbarricadas*". Existiendo dicho mecanismo de contacto, el hecho de rehusar un burofax que no estaba correctamente dirigido a la demandada y cuyo remitente no era el demandante sino la SGAE parece dudoso que se pueda entender como un hecho que "impidió" la comunicación entre el demandante y la compañía demandada.

Por otra parte, el Tribunal Supremo atribuye a la demandada un deber de vigilancia de los contenidos que parece difícil de cohonestar con el artículo 15 de la Directiva de Comercio Electrónico y, como hemos visto, la redacción del fallo no deja claro del todo si la sola presencia de comentarios vejatorios sin comunicación alguna por parte del agraviado implica automáticamente el conocimiento efectivo[30].

Por último, en el caso "Miguel c/Google Inc. y otro", el actor se vio afectado por la difusión en Internet de informaciones que lo vinculaban a una trama de corrupción en el sector inmobiliario de Marbella (conocida como "Operación Malaya"), situación que se daba porque los servicios que brindaba la demandada permitían el enlace a las páginas web de "PRNoticias", Telecinco ("Aquí Hay Tomate") y "Lobby per la Independencia" que contenían los artículos que lo involucraban en tal asunto. En vía extrajudicial reclamó a Google Inc. dos veces solicitó la retirada de determinados contenidos por su falsedad y luego, ya solo con respecto a la página de "PRNoticias" primero le informó acerca de la existencia de un procedimiento judicial en marcha; después lo anotició que en una resolución judicial se determinó que la información de PRNoticias era falsa y que su autor fue condenado a pagar una indemnización y a rectificar por reconocer en sede judicial que lo publicado era completamente falso, y finalmente le hizo saber que inició un procedimiento judicial civil contra PRNoticias que finalizó mediante auto de homologación de acuerdo transaccional.

Frente a lo infructuoso de su reclamo, inició una acción contra Google Inc. en función de las previsiones de la LSSICE y contra su director ejecutivo, por entender que su responsabilidad derivaba de la Ley 14/1966 de 18 de marzo de Prensa e Imprenta (no demandó a los autores de los artículos). Sostuvo que se produjo una intromisión ilegítima en su derecho al honor, especialmente en su faceta profesional y que no solo dicha información es falsa y carente de toda prueba, sino que además no

[30] Miquel Pequera Poch, ¿Deber de controlar los comentarios? En http://responsabilidadinternet.wordpress.com/2013/04/24/caso-eleconomista/

se ha empleado la mínima diligencia profesional en la comprobación de los hechos, permaneciendo la información "colgada" en Google pese a los requerimientos actorales, con lo que se produjo un efecto multiplicador porque a ella acceden otros medios de comunicación y diariamente se producen miles de visitas en la página.

En la sentencia de primera instancia se destacó que no se había demandado a los autores de los contenidos y que a la luz del art. 15 de la Directiva 200/31/CE el intermediario de la sociedad de la información no tiene una obligación general de supervisión de los contenidos, pero que frente a la publicación de uno de carácter lesivo podría ser responsable y sólo se eximiría de ello si el prestador no tuvo "conocimiento efectivo" del contenido dañoso, siendo que de acuerdo a las características del caso, para que exista la obligación de censurar los contenidos publicados debía existir una declaración emanada de un órgano competente que haya declarado la ilicitud de los datos o la existencia de lesión, lo que implica que deba existir una resolución dictada por órgano jurisdiccional o administrativo al que se refiere el apartado j) del anexo de la Ley al definir "órgano competente". Por ello, dado que los enlaces facilitados por Google se referían concretamente a artículos incluidos en las páginas web respecto de los cuales no existió esa resolución de "órgano competente" que declare la ilicitud, se tuvo por cumplidos los recaudos del art. 17 LSSICE (ya que Google encuadraba su actividad en dicha normativa al proporcionar enlaces a las copias almacenadas en su memoria *caché*, almacenamiento de carácter temporal y provisional, en copia del código "html", lo que implica brindar un servicio de intermediación consistente en la facilitación de enlaces al que se refiere el anexo de la Ley) respecto de aquellos, incluido el caso de PRNoticias, donde solo consta que se inició un procedimiento judicial en su contra y que se puso fin al mismo mediante la homologación de un acuerdo transaccional, pero no que se comunicara el contenido de dicho acuerdo a la demandada.

Con respecto a la demanda dirigida contra el director ejecutivo, se la rechazó por entenderse que el prestador de servicios no es equiparable al editor porque es un mero distribuidor de la información, desde que Google se limita a proporcionar enlaces a páginas web, por lo que no participa en ningún caso en la elaboración de la información incluida en ellas ni el director ejecutivo interviene en la redacción de las noticias incluidas en los resultados de las búsquedas ni en la selección de los contenidos a los que se remiten los enlaces, de modo que se acreditó la concurrencia

de los requisitos del art. 17 LSSICE para exonerar de responsabilidad a las empresas que prestan servicios de intermediación, dado que Google no tenía conocimiento de que la titular de la página PRNoticias había reconocido haber atentado contra el honor del demandante, y por ello era incluso innecesaria la notificación a Google puesto que cumpliéndose el acuerdo transaccional la titular de la página retiraría la información lesiva, hecho que supondría la desaparición automática del enlace en al resultado de búsquedas en Google.

La Audiencia Provincial de Madrid confirmó el veredicto en 19/02/10 reiterando que dado que en la información que aparece en las páginas web en cuestión se incluyen informaciones que objetivamente pueden considerarse atentatorias al derecho al honor del apelante, en cuanto le vinculan a un grave caso de corrupción, debe si la entidad demandada ha actuado con diligencia o no desde el momento en que tuvo conocimiento efectivo de la ilicitud de dicha información o que la misma lesionaba derechos de terceros susceptibles de indemnización ya que la Directiva comunitaria indica que no puede imponerse a los prestadores de servicios una supervisión previa de dichos contenidos, da una definición y alcance que debe darse a conocimiento efectivo, y para este caso, donde la información publicada implica una intromisión en el honor, debe existir una declaración de un órgano competente que establezca la ilicitud de los datos ordenando su retirada, o que la existencia de la lesión, de la cual el proveedor del servicio haya tenido conocimiento efectivo y recién allí se encontraría obligado a actuar con diligencia a los efectos de suprimir o inutilizar el enlace correspondiente. Agregó que en el caso cabía aplicar la exoneración de responsabilidad del art. 17 LSSICE, puesto que Google: a) se limitaba a ser un prestador de servicios en una red de comunicaciones, facilitando datos o acceso a una red de comunicaciones, y b) no había actuado de forma negligente al no retirar los contenidos, ante las comunicaciones remitidas por el demandante, pues si bien en una de estas se le comunicaba la existencia de un procedimiento judicial en el que se había dictado una resolución, no constaba la remisión de la copia de esta resolución.

La Sala Civil del Tribunal Supremo, en sentencia n° 144/2013, de 04/03/13, desestimó los recursos de casación y de apelación remitiendo a lo que entendió que en las STS de 09/12/09 y de 10/02/11 sobre el concepto de "conocimiento efectivo" a la luz de la Directiva, y a la no limitación de ese conocimiento sólo a los casos en que

exista una resolución dictada por órgano competente que declarara la ilicitud, ya que el art. 16 de la LSSICE prevé la posibilidad de "otros medios de conocimiento efectivo que pudieran establecerse", como el "que se obtiene por el prestador del servicio a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate" o en palabras del art. 14 de la Directiva, "hechos o circunstancias por los que la actividad o la información revele su carácter ilícito".

Aludió a la sentencia de 16/02/12 (C-360/10) del TJUE que declaró contrario a la normativa comunitaria el requerimiento judicial que exigiera a un prestador de servicios de alojamiento de datos establecer sistemas de filtrado para bloquear la transmisión de archivos que vulneraran los derechos de autor, puesto que éstos podrían no distinguir suficientemente entre contenidos lícitos e ilícitos, bloqueándose comunicaciones de contenido lícito y refirió a lo resuelto por la Gran Sala en STJUE de 23/03/10 (asuntos acumulados C-236/08 y c-238/08 Google France y Louis Vuitton) donde se expresó que el art. 14 de la Directiva 2000/31/CE se aplica al prestador de un servicio de referenciación en Internet cuando no desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados, supuesto en el que no puede ser considerado responsable salvo que tras llegar a su conocimiento la ilicitud de estos datos o de las actividades del anunciante, no actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

Ya aplicando esta doctrina al caso, encontró que la conclusión alcanzada por la Audiencia Provincial es conforme con la doctrina de la Sala, pues de los hechos acreditados no puede inferirse de forma lógica, al alcance de cualquiera, que la información era falsa ni tampoco que se revelara de su contenido su carácter ilícito, y que la circunstancia de que la persona que se consideraba ofendida se hubiera dirigido a Google para la retirada de la información por considerarla ilícita no es suficiente para que se produzca esta conducta, cuando, como aquí ocurre, la información por sí misma tampoco revelaba de manera notoria su carácter ilícito, siendo también a tal efecto insuficiente que se pusiera en conocimiento el inicio de acciones civiles y la carta comunicando la existencia de una resolución judicial, pues no se remitía junto a ella la resolución judicial de homologación de acuerdo y consistía solo en eso, una homologación que no determinó la falsedad de la información, ni condenó a pagar ni

a rectificar al demandado, siendo lo único cierto que el demandado había reconocido ante el Juzgado, porque así consta en el auto de homologación la falsedad de la noticia, pero este auto no fue remitido a la demandada, teniendo solo conocimiento de lo que el actor afirmaba.

Como lo explica Peguera Poch al referirse al fallo, si bien el Tribunal Supremo, ya en la STS 773/2009, había declarado que la noción de conocimiento efectivo del art. 16 debía interpretarse en sentido abierto, admitiendo la posibilidad de adquirir tal conocimiento por cualquier vía, es la primera que aplica el mismo criterio en el ámbito de los enlaces, esto es en el art. 17 LSSICE, y despeja la duda existente, ya que en este caso no se podía acudir al argumento de la interpretación conforme a la Directiva, puesto que esta no contempla ninguna exclusión de responsabilidad para la provisión de enlaces, y entonces el conocimiento efectivo puede adquirirse por cualquier medio también en el caso de los proveedores de enlaces y buscadores. Agrega que la diferencia con las sentencias anteriores, referidas a supuestos de alojamiento de datos, en este caso la ilicitud del contenido no resultaba evidente porque los contenidos no eran de carácter difamatorio ni surgía a simple vista, ya que lo que estaba en cuestión era la veracidad o falsedad de las imputaciones, algo que no resulta obvio a partir del solo texto de las noticias enlazadas, de modo que en este caso concreto el buscador solo podía obtener el conocimiento efectivo a través de una resolución judicial que declarara la ilicitud del contenido, sin que fueran suficientes las notificaciones del perjudicado, lo que implica en definitiva haber llegado a la misma solución que se alcanzaría con una interpretación restrictiva de la noción de conocimiento efectivo, esto es, viene a exigir un previo pronunciamiento que declare la ilicitud del contenido enlazado. Así, salvo que el TS altere la línea jurisprudencial de las anteriores sentencias citadas, habrá que entender, pues, que cuando los contenidos enlazados incluyan expresiones manifiestamente injuriosas, la mera notificación del agraviado será suficiente para que el buscador logre el conocimiento efectivo y tenga que retirar los enlaces so pena de perder el beneficio de la exclusión de responsabilidad."[31]

Desde otro ángulo, Cotino Hueso entiende que con la clara afirmación de sumisión de Google a la LSSICE como prestador, queda obligado a retirar o no

[31] Miquel Peguera Poch, Vulneración del derecho al honor y responsabilidad de los buscadores de Internet, en http://www.elderecho.com/www-elderecho-com/Vulneracion-derecho-responsabilidad-buscadores-Internet_11_556555005.html

facilitar el acceso (desindexar) contenidos ilícitos por vulnerar el derecho de protección de datos. Así sucederá cuando participe activamente de los mismos, o de forma no neutral (por ejemplo con la función autocompletar). Asimismo, Google debe desindexar cuando conozca efectivamente la ilicitud de los contenidos a los que enlaza. Como a continuación se expone, en cuanto recibiera una comunicación por el afectado de la que se deduzca una evidente vulneración de protección de datos debe desindexar. También, cuando reciba la resolución de una autoridad competente, como resoluciones de jueces, o de las autoridades de protección de datos, entre otras. Y esto también valdría para los grandes prestadores o redes sociales con alguna sede en España.

Se consolida así una clara interpretación material del "conocimiento efectivo" de la LSSICE, en función de una visión de justicia material del caso y circunstancias concretas, bastante alejada del texto de la ley española, fijándose como criterio, para hacer responsable al prestador de servicios, que la ilicitud de los contenidos debe estar "al alcance de cualquiera", se exige que la información revele "de manera notoria su carácter ilícito", y por ello la sentencia considera que las comunicaciones que hizo el afectado a Google no fueron suficientes para que conociera efectivamente la ilicitud de los contenidos que el buscador facilitaba[32].

## 3. LA RESPONSABILIDAD DE LOS *BLOGGERS* NO PERTENECIENTES A UN MEDIO DE PRENSA POR LA INSERCIÓN DE COMENTARIOS LESIVOS EN LA JURISPRUDENCIA ESTADOUNIDENSE

En el Sobre esta temática y por cuestiones de espacio nos limitaremos a comentar lo resuelto en el caso "Obsidian Finance Group vs. Cox", que transitó por varias instancias hasta llegar al máximo tribunal de Oregon.

Inicialmente entendió en la causa un tribunal de primera instancia de Oregon, al evaluar la conducta de una bloguera que dirigía tres *blogs* dedicados a cuestiones financieras por haber publicado en uno de ellos ("obsidianfinancesucks.com") un *post* en el que acusó a los actores (Obsidian, una financiera, y Padrick, el síndico de una

[32] Lorenzo Cotino Hueso, Comentario a la Sentencia Tribunal Supremo Google y LSSICE, en http://www.cotino.net/2013/05/comentario-a-la-sentencia-tribunal-supremo-google-y-lssice/

quiebra) de corrupción, fraude impositivo, lavado de dinero, difamación, acoso y otras actividades ilegales. Cox fue condenada porque se entendió que dado que los contenidos publicados no estaban formulados a partir de un lenguaje figurativo e hiperbólico y no podían ser probados como verdaderos o falsos, Obsidian no tenía necesidad de probar que Cox había actuado con negligencia ya que la bloguera no demostró ser periodista (sobre esto aclaró que ninguno de los demandados eran figuras públicas y que la ley de protección de los medios de comunicación se aplica sólo a las declaraciones hechas en medios impresos o de difusión, y no a los blogs de Internet y a una persona conectada con cualquier medio de comunicación dirigido al público, y que no cabía incluir a los blogs en la definición de "medio de comunicación") ni reveló la fuente interna de la cual se había nutrido para descargar su responsabilidad[33].

La sentencia fue apelada y la Corte de Apelaciones del 9° Circuito de Oregon la revocó ordenando la celebración de un nuevo juicio sobre ciertas y nuevas bases que debían ser instruidas al jurado, estableciendo que las protecciones a la libertad de expresión de un periodista tradicional se aplican a un *blogger* aunque no sea periodista, pues como la Corte Suprema ha advertido con precisión, la distinción, en el ámbito de la Primera Enmienda, entre la prensa institucional y otros oradores es inviable ya que con la llegada de Internet la línea entre los medios de comunicación tradicionales y otros que deseen formular observaciones sobre los temas políticos y sociales se vuelve más borrosa, y en los casos de difamación, es el carácter de figura pública del aludido (que aquí descartó) y la importancia pública de la declaración de que se trata -no la identidad del orador- la que brinda la protección de la Primera Enmienda. Agregó que el tenor general de las entradas del blog de Cox, con su lenguaje extremo, niega la impresión de que ella estaba afirmando hechos objetivos y llevan a leerlas más como un periódico o la entrada de un diario que revela los sentimientos de Cox (al expresar que "Padrick contrató a un sicario para matarla" o "que todo el sistema de los tribunales de quiebras está dañado") antes que hechos objetivos, de modo que no están suficientemente basadas en hechos como para demostrar que son verdaderas o falsas."[34]

[33] "Obsidian Fin. Grp., LLC v. Cox", 812 F. Supp. 2d 1220, 1232–34 (D. Or. 2011)
[34] http://cdn.ca9.uscourts.gov/datastore/opinions/2014/01/17/12-35238.pdf.

## 4. REFLEXIONES FINALES

La tan intrincada como relevante cuestión de la responsabilidad de quienes intervienen en alguna de las fases de la incorporación de contenidos disponibles en Internet ha tenido y tiene, en los países democráticos y respetuosos de los derechos humanos, variantes que van tendiendo a una bastante homogénea regulación internacional, sin por ello avasallar totalmente el margen de apreciación nacional, tal como puede observarse de lo resuelto en el aquí analizado caso "Delfi".

Particularmente, la aparición de ediciones digitales de medios de comunicación tradicionales y de nuevas formas de periodismo en línea, reavivó la antigua discusión respecto de la forma de resolver las tensiones entre el "derecho de prensa" y el "derecho a la protección de datos" y pone además –nuevamente- en claro que toda solución que se adopte en este sentido debe ponderar adecuada y equilibradamente tanto los alcances de la libertad de expresión como la de los derechos fundamentales que pueden contraponérsele. A los medios jurídicos tradicionales de reacción disponibles frente a tales violaciones de derechos de quienes son referidos en las publicaciones lesivas (el derecho de réplica, la indemnización de los daños y perjuicios y la persecución penal del ofensor), se han agregado en los últimos años otro medios (judiciales y administrativos) destinados a ejercer los derechos típicos del derecho a la protección de datos (v.gr., los derechos de cancelación, rectificación y desindexación, para cuya efectivización puede recurrirse a las autoridades administrativas de control –v.gr., las agencias de protección de datos- y a las judiciales, mediante procesos ordinarios o especiales –v.gr., en Argentina o Uruguay, entre otros, el de hábeas data[35]).

La libertad de expresión en línea ha sumado editores de contenido no tradicionales y ello también ha llevado a la inacabada discusión acerca de si cabe o no extender ciertas prerrogativas concedidas a los periodistas y a los medios de comunicación institucionales a estas nuevas formas de periodismo en Internet.

[35] En este sentido, por ejemplo, la Sala Segunda (Integrada) de la Cámara de Apelación en lo Civil y Comercial de Rosario (Argentina), en el Acuerdo n° 17 del 17/02/10, despachó favorablemente un hábeas data -ordenando la desindexación de una noticia notoriamente falsa y perjudicial- que fuera interpuesto contra una información falsa contenida en una noticia publicada en la edición digital de un periódico. Esta solución es simétrica a la adoptada posteriormente por el Superior Tribunal de Justicia de la Unión Europea en el ya tratado caso "Costeja".

La efectividad de las respuestas a estos nuevos fenómenos y conflictos -y a los que sigan surgiendo en el futuro- se encuentra condicionada por efecto del incesante y sorprendente avance tecnológico, actualmente liderado por los fenómenos del *big data* y la Internet de las cosas *(IoT)* -ambos en sinergia y potenciados por la computación en la nube (*cloud computing*)-, que provoca la multiplicación de fuentes y formas de las afecciones (v.gr., la multiplicación de aplicaciones que utilizan sensores, los *wearables*, la domótica, la aplicación de algoritmos para la formulación automatizada de perfiles de las personas). También se encuentra condicionada por el todavía insuficiente desarrollo normativo e institucional global que pueda brindar una inmediata y efectiva protección a los derechos de los afectados.

Por el momento, estas cuestiones deberán seguir siendo resueltas –en el tiempo que cada ordenamiento interno o comunitario permita- mediante la aplicación de los principios generales a los nuevos fenómenos -a falta o vetustez- de regulación expresa-, siempre teniendo en cuenta que deben buscarse soluciones que fomenten un equilibrio entre el avance de las tecnologías y los derechos fundamentales de las personas, tal como puede colegirse de los principios sentados, v.gr., por la Conferencia de Naciones Unidas sobre población y desarrollo, celebrada en 2012 en Río de Janeiro.

Un intento de actualización de las normas en función de tales principios que resulta destacable –aunque por supuesto insuficiente en términos globales, por tratarse de una norma dictada en el marco de la Unión Europea- es la Propuesta de Reglamento General de protección de datos al cual hemos aludido *supra*, que, v.gr., y con el fin de reforzar el derecho a la supresión en el entorno en línea, lo amplía de tal forma que: a) dispone que los responsables del tratamiento que hayan hecho públicos los datos personales sin justificación legal estarán obligados a tomar todas las medidas necesarias para que se supriman los datos -también por parte de terceros-, y a bloquear los datos que sean objeto de impugnación por el interesado o cuya exactitud o inexactitud no pueda determinarse, mientras la calidad de los datos esté en disputa (ver considerandos 54 y 54 bis), y b) incluye en su articulado principios novedosos en materia de protección de datos, entre los que se cuentan la *Privacy by design* (privacidad desde el diseño), la *Privacy by default* (privacidad por defecto) y la *Accountability* (principio de responsabilidad o compromiso de los responsables y encargados).

Las cuestiones aquí tratadas, como se ve, están en pleno despliegue normativo, doctrinario y jurisprudencial, y aunque como se dijo e intentó mostrarse, existe un progresivo acuerdo sobre las cuestiones centrales bajo estudio en los países tecnológicamente más avanzados, igualmente resulta más que probable que en un futuro no muy lejano surjan nuevas perspectivas de análisis a partir de nuevos avances tecnológicos que puedan alterar las conclusiones a las que se han arribado por estos días.

CYBERLAW by CIJIC

# CRITERIOS PARA IMPLEMENTAR EL DERECHO AL OLVIDO EN INTERNET: COMENTARIO A LAS DIRECTRICES DEL GRUPO DE TRABAJO DEL ARTÍCULO 29 DE LA UNIÓN EUROPEA

# CRITÉRIOS PARA IMPLEMENTAR O DIREITO AO ESQUECIMENTO NA INTERNET: COMENTÁRIO ÀS DIRETRIZES EMANADAS PELO GRUPO DE TRABALHO DO ARTIGO 29

**PABLO A. PALAZZI** [1]

[1] Profesor de Derecho Universidad de San Andrés, Director del Programa de Derecho de Internet y de las telecomunicaciones de la Universidad de San Andrés, especialista en Derecho de Internet y Propiedad intelectual, socio del estudio Allende & Brea. Correo electronico: ppalzzi@udesa.edu.ar

**SUMÁRIO: 1. INTRODUCCIÓN; 2. IMPORTANCIA DEL INFORME DEL WP29; 3. INTERPRETACIÓN DEL FALLO DEL TRIBUNAL EUROPEO POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29; 4. LISTADO DE CRITERIOS PARA RESOLVER PLANTEOS DE DERECHO AL OLVIDO IDENTIFICADOS POR EL GRUPO DE TRABAJO DEL ART. 29; 5. CONCLUSIONES PRELIMINARES**


## RESUMO

Prática comum ao acto de exclusão de um dado *link* para os resultados de uma determinada rede, passa por uma comunicação – de rastreamento, em alguns casos através de um e-mail para a página, revista ou blog - a informar dessa remoção. O relatório [2] propugnado pelo grupo de trabalho do artigo 29 (em inglês no acrónimo *WP29*) estabelece que este tipo de comportamento, por exemplo, da *Google*, carece de base legal e que esta apenas poderá estabelecer contato entre o motor de busca e a fonte somente na recolha de informações para ajudar a tomar uma decisão mais esclarecida sobre a desvinculação do índice. Este relatório clarifica ainda que *entrar em contato com a fonte original dos dados* deverá contemplar a tomada de medidas necessárias para salvaguardar os direitos do titular dos dados pessoais.



**Palavras-Chave:** Operadores de Internet; Responsabilidade; Remoção de conteúdos do índice; Dados pessoais; Direito ao esquecimento


[2] "Recomendações sobre a implementação da decisão do Tribunal Europeu de Justiça no caso 'Google Espanha e Google Inc. v. Agência Espanhola de Protecção de Dados e Mario Gonzalez Costeja".

## RESUMEN

Una de los prácticas que está llevando a cabo el buscador consiste en que cuando elimina de sus resultados un link de una web concreta, comunica en algunos casos por medio de un e-mail a la página, diario o blog, siendo rastreada para informarle de la eliminación. El informe[3] de las autoridades europeas[4] ha aclarado que este comportamiento de Google carece de base legal y que únicamente podrían establecerse contactos entre el buscador y la web de origen, para recabar información y poder tomar una decisión más informada sobre la desvinculación del índice. El informe aclara que pueden contactar a la fuente original del dato, pero que también deben adoptar las medidas necesarias para salvaguardar los derechos del titular del dato personal.

**Palabras-clave:** Operadores de Internet; Responsabilidad; Remoción de contenidos del índice; Datos personales; Derecho al olvido

[3] "Directrices sobre la implementación del fallo del Tribunal Europeo de Justicia en el caso 'Google Spain y Google Inc. v. Agencia Española de Protección de Datos Personales y Mario Costeja González".

[4] El Grupo del Artículo 29.

## 1. INTRODUCCIÓN

El 26 de noviembre de 2014 el Grupo de Trabajo del Art. 29 emitió el documento titulado Directrices sobre la implementación del fallo del Tribunal Europeo de Justicia en el caso "Google Spain y Google Inc. v. Agencia Española de Protección de Datos Personales y Mario Costeja Gonzalez" (Asunto C-131/12)[5].

El Grupo del Artículo 29 (en adelante Grupo del Art. 29 o WP 29) es un organismo de la UE creado por la Directiva Europea de protección de datos personales[6].

Este Grupo está compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión Europea.

El mencionado Grupo en cumplimento de sus funciones, elabora documentos y guías interpretativas que tienen gran influencia en la interpretación del derecho de la protección de datos personales[7]. Por ello ha un documento interpretativo sobre el caso "Google Spain" [8] del Tribunal de Justicia de la Unión Europa (TJUE), sentencia que como es sabido reconoció pretorianamente el derecho al olvido en Internet[9].

## 2. IMPORTANCIA DEL INFORME DEL WP29

Luego de dictado el caso "Google Spain" se presentaron miles de solicitudes de derecho al olvido a través de los formularios online implementado por los buscadores.

[5] Working Party Article 29, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"*, WP 225, disponible online en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

[6] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Diario Oficial n° L 281 de 23/11/1995 p. 31–50.

[7] Su influencia no sólo se limita a la Unión Europea, sino también a otras regiones, por ej. en América Latina es frecuentemente citado por algunas agencias de protección de datos personales.

[8] Sentencia del Tribunal de Justicia (Gran Sala) del 13 de mayo de 2014, asunto C‑ 131/12, Google Spain, S.L., y Google Inc. vs. Agencia Española de Protección de Datos.

[9] Sobre el caso ver nuestra nota *El reconocimiento en Europa del derecho al olvido en Internet* en LL 2014-C-407.

Asimismo ha existido un gran debate sobre los alcances, límites, y forma de implementar este derecho.

A raíz de ello, el WP29 ha emitido el documento que comentamos en esta nota y que pretende clarificar muchos de los problemas planteados hasta la fecha, así como sugerir elementos para la implementación del derecho al olvido en Europa.

El informe consta de dos partes. Una primera parte está destinada a brindar una interpretación del fallo de la Corte Europea por el WP29. Una segunda parte está destinada a brindar elementos para que las agencias de protección de datos personales puedan decidir con elementos concretos si corresponde delistar un hipervínculo del buscador con fundamento en el derecho al olvido.

El documento enumera trece elementos a tener en cuenta, que son sólo enunciativos pues surgirán muchos más en los casos que se están planteando y resolviendo día a día. Estos elementos suelen ser importantes para realizar el balance de derechos y decidir sobre la admisión o no del derecho al olvido en un caso concreto.

En la práctica, dado que el WP29 se ha transformado en la "voz oficial" de la política europea en materia de datos personales, este documento va a ser muy importante pues va a servir de guía a los reguladores locales, a los buscadores, y a los litigantes.

## 3.INTERPRETACIÓN DEL FALLO DEL TRIBUNAL EUROPEO POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29

### 3.1. El nomen iuris y el concepto del derecho al olvido

El informe realiza un detallado análisis de las cuestiones que fueron surgiendo durante la implementación del fallo.

En muchos casos el alcance del fallo europeo ha sido malinterpretada por la prensa, empezando por el nombre de este nuevo derecho. También ha sido

fuertemente atacado en su fundamento por la prensa y la doctrina en los Estados Unidos[10].

La confusión se genera en parte pues desde un comienzo se ha equiparado en la prensa al derecho al olvido con el derecho a borrar cualquier información negativa o contenidos de páginas de Internet[11]. Esto sucede en parte porque ambos derechos tienen mucho en común, pero el derecho al olvido no borra cualquier información negativa (ej. están excluidas las recientes, y los asuntos de interés público o personas públicas). Tampoco sirve para borrar del sitio de origen el dato, sino que sólo la remueve solamente del índice del buscador (sigue estando en el sitio original y es posible hallarla por otros términos de búsqueda diferentes al nombre).

Además algunos casos pueden comenzar como difamación y terminar como un caso de derecho al olvido. Hay también un solapamiento de pretensiones entre los casos de borrado de datos personales falsos y el borrado de datos personales donde ya no existe un interés legítimo para el tratamiento del mismo (por diversos motivos: falta de relevancia, antigüedad, etc.), o argumentando que el dato no refleja la realidad dada su extrema antigüedad.

Esta confusión de términos y conceptos va a ser inevitable dada la novedad de la materia. Es también imposible de evitar para los periodistas que abordan la cuestión del derecho al olvido superficialmente y sin mucho estudio detenido del tema (ej. sin leer el fallo completo y entender el contexto regulatorio europeo).

Pese a que el derecho al olvido se deriva de una norma jurídica redactada a comienzos de la década del noventa, y aprobada en el año 1995, no hay normas directas sobre el derecho al olvido con esos términos en la citada Directiva.

El problema es que el término derecho al olvido (*droit a l´oublie* o *right to be forgotten*) tiene mucho *appeal* pero no traduce su verdadero significado. Por eso es recomendable usar nuevos términos, como la palabra inglesa *de-listing*[12] o también

[10] Existen sin embargo algunas excepciones, ver por ejemplo Eric POSNER, *We All Have the Right to Be Forgotten*, en SLATE, Mayo de 2014.
[11] Ver por ejemplo la primera notas publicada en el New York Times comentando el caso y su título: David STREITFELD, *European Court Lets Users Erase Records on Web*, New York Times, 13 de mayo de 2014 (el subrayado nos pertenece).
[12] Este es el término que utiliza el documento del Working Party que comentamos en esta nota.

los conceptos *droit à la désindexation* o *droit au déréférencement* como ha propuesto la agencia francesa de protección de datos personales[13].

En castellano una traducción literal podría ser de-listar o deslistar, desindexar o des-referenciar, aunque también se puede usar "desvincular". Es decir, un *derecho al desindexado*. Todas estas palabras hacen alusión a la eliminación de una referencia o hipervínculo que aparece en el resultado o índice del buscador a determinado contenido. Esa referencia existe cuando se tipea o usa el nombre de un individuo como palabra de búsqueda en un motor de búsqueda en Internet.

Como esta forma de buscar información en Internet permitía encontrar sin ninguna clase de filtro todo tipo de información, incluso las irrelevantes, pasadas, antiguas o cuestiones que carecían de interés público muchos años después de su ocurrencia, la solución propuesta por el TJUE en el caso "Google Spain" fue algo muy simple: eliminar la aparición de hipervínculos a la noticia en cuestión del resultado (del índice) del buscador.

Cabe aclarar que este derecho al olvido o derecho de supresión no implica borrar o suprimir la información en la fuente original, que seguirá existiendo y en muchos casos estará amparada por una obligación legal de publicar el dato o por la libertad de prensa. Solo se requiere que el buscador adopte los mecanismos tecnológicos necesarios para que un resultado determinado no aparezca en los resultados de la búsqueda. El resultado sin embargo podrá aparecer si se busca con otros elementos distintos al nombre (ej. cargo, profesión, lugar y fecha del evento, etc.).

De hecho, como evidencia del problema que acarrea el *nomen iuris* del derecho al olvido, recordamos que en el año 2013 durante el trámite del Reglamento comunitario (que reemplazará a la Directiva) se decidió borrar el nombre de "derecho al olvido" y dejar solo el nombre "derecho de supresión". Ello se debió, como bien señaló un reconocido autor, a "un problema de comunicación y de expectativas sobre lo que realmente otorga el derecho y lo que los titulares de datos lograrán en la práctica"[14].

[13] Ver http://m.cnil.fr/fileadmin/documents/Vos_libertes/Droit_au_dereferencement-criteres.pdf .
[14] KOOPS, Bert-Jaap, *The trouble with European data protection law*, International Data Privacy Law (2014) 4 (4): 250-261, OUP, Octubre 2014 quien señala: "*The term 'right to be forgotten' has been floated as an appealing ideal for doing something about the persistence of embarrassing data on the Internet, but it is pretty obviously a misnomer: not only is it very difficult to have all copies of data removed from the Internet, but removing content from the Internet also cannot be equated to people actually forgetting what they have already read*".

Previo a listar y analizar los criterios para remover hipervínculos al índice de Google bajo el derecho al olvido, el documento explica su visión del fallo dictado por el tribunal Europeo a través de varios de sus aspectos.

### 3.2. **Los buscadores como responsables del tratamiento de datos personales**

El Informe del WP29 comienza señalando los puntos centrales del caso "Google Spain", los que a su juicio son:

- El fallo reconoce que los motores de búsqueda procesan datos personales y son "responsable del tratamiento" en los términos del art. 2 de la Directiva 95/46 (Párrafos 27, 28 y 33 del fallo "Google Spain").

-El tratamiento realizado por el buscador es distinto del tratamiento realizado por el editor del sitio web, que consiste en cargar la información en la página web (párrafo 35 del fallo "Google Spain").

-Las bases legales para procesar datos personales bajo la Directiva Europa de protección de datos se encuentran en el art. 7(f) de la Directiva Europea (Párrafo 73 del fallo "Google Spain").

El primer punto que analiza es que los buscadores de internet, según la conclusión del caso "Google Spain" son responsables del tratamiento, o "encargado del tratamiento". Bajo el Derecho Europeo, el responsable del tratamiento es definido como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales". Esta es la base para aplicar la ley de protección de datos a los buscadores.

Luego el informe recuerda que el procesamiento de datos realizado por el buscador tiene capacidad para afectar derechos fundamentales del titular del dato, pues cada vez que se tipea su nombre en el recuadro de búsqueda aparecen datos personales referidos en muchos casos a diversos aspectos de su vida privada y que permiten crear un perfil de su persona. El efecto que produce en la vida privada esos resultados aumenta por el rol que juega hoy en día los buscadores de Internet en la sociedad moderna (párrafo 80 del fallo "Google Spain").

En relación al balance de derechos, el Informe interpreta que el fallo claramente señala que los derechos del titular del dato están por encima de los derechos económicos del motor de búsqueda. Estos derechos del titular de dato personal también prevalecen sobre los derechos del público a acceder a esa información. Sin embargo se recuerda que el rol que en la vida publica tenga el sujeto en cuestión podrá hacer inclinar la balanza a favor del acceso a esa información (párrafo 81 del fallo "Google Spain").

Concluye que los titulares de datos personales tienen derecho bajo las condiciones de los artículos 12 y 14 de la Directiva Europea de Protección de datos personales a pedir la remoción de ciertos vínculos del listado de los buscadores, que señalan a datos negativos publicados por terceros.

Los fundamentos para el tratamiento de datos personales por el editor original y por el buscador son diferentes. El buscador deberá evaluar los diferentes elementos (interés público, relevancia pública, naturaleza de los datos, y relevancia actual) sobre la base de su propio fundamento legal para seguir tratando esos datos que deriva de un balance entre su interés económico y el de los usuarios en acceder a esa información a través del motor de búsqueda usando el nombre del titular del dato como elemento de búsqueda. Incluso aunque la publicación por el editor original sea legal, su difusión universal y continua accesibilidad a través de motores de búsqueda en Internet puede devenir ilegal o ser una desproporcionada invasión en la privacidad del titular.

El interés del buscador en procesar datos personales es meramente económico. Pero existe también un interés de los usuarios de Internet en recibir información usando motores de búsqueda. Este interés según el documento que anotamos se fundamenta en el art. 11 de la Carta Europea de Derechos Fundamentales y tiene que ser tenido en cuenta.

Un punto central del Informe es que reconoce que el fallo "Google Spain" no obliga a los buscadores a realizar en forma constante evaluaciones para ver si los datos deben ser removidos por darse las condiciones del derecho al olvido: solo deben actuar a petición de parte interesada. Creemos que una conclusión contraria hubiera sido contraria a la obligación de no monitorear prevista en la Directiva Europea de Comercio Electrónico.

### 3.3. **Ejercicio de los derechos por parte del titular del dato**

Así como las normas de protección de datos personales se aplican al procesamiento de datos personales realizados por el buscador, el titular del dato debe tener derecho a ejercer sus derechos contemplados en las normas de la Directiva 95/46 y las leyes nacionales que la implementan.

Es así como el informe del Grupo de Trabajo del Art. 29 enumera una serie de aspectos relacionados con el ejercicio del derecho al olvido.

Esto son:

- El titular del dato personal no está obligado a contactar al sitio original, en orden a solicitar al buscador el ejercicio de sus derechos. El informe aclara que son dos procesamientos de datos distintos, con fundamento legal diferente y con distinto impacto en los derechos e intereses del individuo.

- El titular del dato puede considerar que es mejor, dadas las circunstancias, contactar en primer lugar al webmaster del sitio y pedir el borrado o anonimización del dato del sitio original, o que se aplique el protocolo robots.txt ("no index") a los fines de evitar el indexado del sitio en cuestión en el buscador. Pero el informe es rotundo en aclarar que el caso "Google Spain" no exige "agotar esta vía" antes de ir al buscador.

- El titular del dato es quien decide cómo ejercer sus derechos y por eso tiene derecho a acudir a uno o a todos los buscadores para ejercer su derecho al olvido. Sólo el titular es quien puede decidir y evaluar el impacto que su información publicada en Internet tiene, y por eso esta es su decisión.

- Si bien la Directiva 95/46 no clarifica como ejercer los derechos del titular del dato personal, existe amplia facilidad en el derecho nacional para que el titular haga sus reclamos. Por eso el informe aclara que el titular del dato puede contactar al buscador de cualquier forma, independientemente de los procedimientos ad hoc que el buscador haya creado para tal fin. El informe aclara que el uso de formularios online implementados por los buscadores es una buena práctica pero no debe ser la única forma de recibir pedidos.

- Los buscadores deben seguir el derecho nacional a la hora de aplicar y procesar pedidos de desvinculación del índice del buscador. Ello implica que

el buscador debe solicitar alguna forma de identificación pero esos recaudos deben ser proporcionados y necesarios de acuerdo a la necesidad de verificar la identidad del peticionante. Asimismo, para que el buscador haga la evaluación necesaria para decidir si corresponde remover del índice el hipervínculo a la noticia, el titular del dato le debe brindar las razones necesarias para que ello ocurra, indicar la dirección de internet en cuestión que lo afecta, si tiene un rol en la vida publica o es una persona privada, y proporcionar la prueba de sus alegaciones.

- Si el buscador deniega el pedido, debe dar una explicación fundada de su denegatoria. En el mismo acto se debe informar al titular del dato personal que tiene derecho a recurrir a los tribunales o a la agencia local de protección de datos.

Finalmente el informe del WP29 señala que el caso "Google Spain" considera que las subsidiarias nacionales de un buscador en la Unión Europea son "establecimientos" de la empresa y que el procesamiento de datos personales por parte del buscador es realizado en el contexto de actividades del establecimiento, lo cual hace aplicable las normas de protección de datos al buscador en su totalidad.

El informe reconoce que la Directiva 95/46 no contiene normas específicas en relación con la responsabilidad de los establecimientos del responsable del tratamiento localizados en el territorio de países miembros de la Unión Europea. La única referencia se encuentra en el art. 4.1.a de la Directiva 95/46 que dispone "Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable". Esta norma está de algún modo clarificada en el considerando 19 de la Directiva[15].

[15] Que dice así: "…Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades".

Señala el informe que la efectiva vigencia del caso "Google Spain" requiere que los titulares de datos personales puedan ejercer sus derechos frente a las subsidiarias nacionales de su lugar de residencia en cada estado miembro de la Unión Europea. A su vez las agencia de protección de datos personales deben poder contactar a estas subsidiarias en relación a los reclamos presentados. El informe aclara que estas subsidiarias tienen total libertad de seguir y aplicar los procedimientos internos para tratar los reclamos o reenviarlos a otra subsidiaria. También resulta razonable que aconsejen al titular del dato que siga al procedimiento ad-hoc establecido por la empresa para un reclamo a través de un formulario electrónico. El informe del WP29 concluye que si el titular del dato personal insiste en contactar a la subsidiaria local por otro medio, no podrá negársele ese derecho.

### 3.4. **Ámbito de aplicación del derecho al olvido**

El informe contiene un extenso análisis del ámbito de aplicación del falo "Google Spain". Se tratan dos cuestiones: (i) a qué clase de buscadores se aplica (generalistas o dedicados) y (ii) el alcance de la orden de remoción basado en el derecho al olvido (aplicación europea o global).

En el n.17 el informe aclara que si bien el fallo se refiere a buscadores generales ("*generalist search engines*"), ello no significa que no pueda ser aplicado a otros intermediarios y concluye que si están reunidas las condiciones para la procedencia del derecho al olvido, el mismo deberá aplicarse.

El informe explica que los buscadores "internos" incluidos en diferentes sitios de internet no producen el mismo efecto que los buscadores "externos"[16]. Primero, sólo brindan información contenida en las páginas donde están instalados. Asimismo, el informe precisa que incluso si un usuario de Internet busca en un gran número de sitios, los buscadores internos no van a establecer un perfil completo del titular del dato y estos resultados no tienen un alto impacto sobre su persona. La excepción podrían ser los buscadores de datos de personas (ej. Spokeo, etc.)

Por eso el informe del WP29 aclara como regla que la desvinculación de resultados no debería aplicarse a buscadores con un ámbito de acción limitado,

[16] Ej. el buscador interno de Amazon, o el de LinkedIn o Twitter.

particularmente el caso de los motores de búsqueda internos de diarios de noticias disponibles online.

Se recuerda asimismo que el art. 8 de la Carta Europea de Derechos Fundamentales otorga derecho de protección de datos personales a "todas las personas" sin distinción. En la práctica la agencia de protección de datos personales se centrará en reclamos en los cuales existe una clara vinculación entre el titular del dato y el territorio de la Unión Europea, por ejemplo porque el titular del dato personal es un ciudadano o residente de un país miembro de la Unión Europea.

El informe del WP29 en el n. 20 recuerda que el caso "Google Spain" concluyó que el titular del dato tiene derechos sobre la actividad de un motor de búsqueda como proveedor de contenidos, que consiste "en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado".

Luego cita las conclusiones del fallo "Google Spain" y explica que "Los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado."

Google lleva tiempo borrando resultados de búsquedas pero sólo a ciudadanos europeos y dentro del territorio de la Unión Europea, cuando la propia sentencia del TJUE hace mención al "público en general". El fallo, en su última conclusión y en los apartados 97 y 99 explica que las personas físicas que ejerciten su derecho al olvido sobre un responsable obligado por la normativa de la Unión Europea, "podrán solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados".

Google sostiene la tesis que la decisión del TJUE es únicamente aplicable a los servicios ofrecidos a los usuarios europeos. Sin ir más lejos, en el formulario de

solicitud del derecho al olvido que ha publicado en Internet, se solicita que se indique un país para saber qué normativa aplicar.

De todo lo expuesto el informe (n.20) concluye que el fallo "Google Spain" establece una "obligación de resultado" que afecta a la totalidad de las operaciones de procesamiento llevadas a cabo por el buscador. La adecuada implementación del fallo "Google Spain", entiende el informe, debe ser hecha de modo que los titulares de datos personales "*estén protegidos en forma efectiva contra el impacto de la diseminación universal y accesibilidad universal de sus datos personales a través del buscador, cuando se realiza una búsqueda sobre la base de su nombre personal*".

El informe explica que si bien las soluciones concretas dependerán de la organización interna de la estructura del buscador, la implementación de la desvinculación debe ser hecha "*...de forma tal que garantice la efectiva y completa protección de los derechos garantizados de modo que el Derecho de la Unión Europea no pueda ser eludido*".

En este sentido, el informe aclara que la limitación de la desvinculación de resultados solo a nombres de dominio europeos (ej. google.fr), con la excusa que los usuarios tienen la costumbre a acceder a buscadores a través de dominios nacionales no puede ser considerado un medio suficiente de cumplir los derechos establecidos en el fallo "Google Spain". En la práctica, el informe concluye que la desvinculación debe ocurrir en todos los dominios relevantes, incluyendo el dominio gTLD (ej .com) del buscador. Esto implica que la remoción del índice debe ser una *remoción global*.

Este es uno de los aspectos mas delicados del Informe del WP29 y que ha generado mas críticas desde los Estados Unidos[17].

El informe del WP29 en este punto termina reiterando que sólo se remueve el resultado del índice, y aclara que el fallo "Google Spain" nunca sugirió que se borraran los contenidos del índice o base de datos del buscador. El contenido en cuestión estará accesible y será posible encontrarlo por otros criterios de búsqueda diferentes al nombre, por ejemplo la posición de la persona.

[17] Aunque también en Europa: ver por ejemplo el artículo de C. KUNER, *The European Union and the search for an international data protection framework*, en Groningen Journal of International law, Vol.2, Ed.1, criticando los efectos extraterritoriales del derecho europeo de protección de los datos personales.

Se aclara asimismo que el caso “Google Spain” usa el término “nombre” pero ello incluye otras versiones del nombre e incluso diferentes formas de pronunciar o escribir el nombre.

### 3.5. **Comunicación a terceros de la desvinculación del índice**

Remover contenido del índice del buscador significa que dicho contenido no va a aparecer mas en una búsqueda realizada por cualquiera que tipee ese nombre, sin perjuicio de la posibilidad de ir al sitio original a buscar la noticia.

El documento (n.22) señala que algunos buscadores han adoptado como práctica en algunos casos informar a los usuarios de Internet la desvinculación de ciertos nombres.

A partir del fallo “Google Spain”, el buscador Google adoptó la práctica, cuando se realiza una búsqueda de un nombre común (no de una persona famosa) de mostrar en la parte inferior de los resultados de búsqueda el siguiente aviso: "*Es posible que algunos resultados se hayan eliminado de acuerdo con la ley de protección de datos europea. Más información*".

Si se hace click en el enlace de “Más información”, Google explica que este aviso aparece aunque no se haya eliminado nada, es decir es una respuesta que el buscador ofrece por defecto.

Se ha entendido sin embargo que este aviso podría sugerir que una persona concreta (aquella cuyo nombre se puso en el buscador) ha solicitado el derecho al olvido sobre algún aspecto negativo que no aparece (y que el mensaje confirmaría tal borrado).

Podría darse también el caso de tratarse de un apellido muy común y generar el mismo efecto en el resto de internautas que tengan el mismo nombre y apellido y que no hayan hecho un pedido de derecho al olvido.

El informe del Grupo de Trabajo del Artículo 29 aclaró que este mensaje no tiene base legal alguna en el ordenamiento europeo. El informe explica que este mensaje sólo se puede incluir cuando no haya dudas acerca de la persona sobre la que se está buscando la información. El informe dice: "*Las decisiones que deben ser excluidas*

*del listado (de búsqueda), deben ser aplicadas de tal manera que se garantice una protección efectiva y completa de los derechos del sujeto*".

Por otra parte desde el lado de la empresa este mensaje tiene su lógica: si el buscador desea mostrar toda la información posible y disponible en la web relacionada con la búsqueda, y por una ley o fallo no puede hacerlo, un *disclaimer* es una forma de mostrar que la falta de resultados es ajeno al buscador.

Otra de los prácticas que está llevando a cabo el buscador consiste en que cuando elimina de sus resultados un *link* de una web concreta, comunica en algunos casos por medio de un e-mail a la página, diario o blog siendo rastreada para informarle de la eliminación.

Esto ya ocurrió varias veces [18] desde que se implementó el formulario de remoción luego del fallo "Google Spain". El buscador explica asimismo que solo comunican informacion de la url removida del indice, pero no de la persona que solicito la remocion pues entienden que la peticion es confidencial[19].

El informe de las autoridades europeas han aclarado que este comportamiento de Google carece de base legal y que únicamente podrían establecerse contactos entre el buscador y la web de origen para recabar información y poder tomar una decisión mas informada sobre la desvinculación del índice [20]. El informe aclara que pueden contactar a la fuente original del dato pero que también deben adoptar las medidas necesarias para salvaguardar los derechos del titular del dato personal.

[18] Google hizo esto en varias oportunidades. Por ejemplo con el New York Times (ver Noaam COHEN, *Times Articles Removed From Google Results in Europe*, New York times, 3 de cotubre del 2014) o con el diario inglés The Guardian, respecto a varias notas de interés público (ver James BALL, *EU's right to be forgotten: Guardian articles have been hidden by Google*, The Guardian, 2 de julio de 2014). También lo hizo con el diario español "Qué", en relación a algunas noticias sobre terrorismo (ver la nota *Google borra noticias de la ETA por el derecho al olvido*, diario ABC, 6 de noviembre de 2014, http://www.abc.es/espana/20141106/abci-derecho-olvido-201411061725.html y la nota *Los terroristas encuentran en el 'derecho al olvido' una vía para eliminar su rastro en internet*, en diario Qué, http://www.que.es/tecnologia/201411060800-terroristas-encuentran-derecho-olvido-para.html).

[19] William Malcolm, Senior Privacy Counsel, Google, opinion vertida en el panel sobre derecho al olvido titulado *The Right to Be Forgotten: Competing Interests and Cultural Divides* en la conferencia IAPP Privacy Summit 2015, 5 de marzo de 2015.

[20] Así el WP29 señala: "Search engines should not as a general practice inform the webmasters of the pages affected by removals of the fact that some web pages cannot be acceded from the search engine in response to a specific name-based query. There is no legal basis for such routine communication under EU data protection law. In some cases, search engines may want to contact the original editor in relation to particular request prior to any delisting decision, in order to obtain additional information for the assessment of the circumstances surrounding that request".

También introduce un nuevo problema: que la prensa puede republicar la información –incluyendo el nombre del titular del dato personal- sobre el borrado de la noticia del índice, y generar nuevamente interés público sobre algo que el titular del dato personal quería enterrar para siempre. Esto obligaría al titular del dato a volver a plantear la remoción de las nuevas noticias sobre su pedido al olvido del índice del buscador. Ahora bien, esas noticias tienen cierta actualidad, y parecería que no deberían ser "olvidadas" si son recientes. Por otra parte, si se acepta que esto suceda con frecuencia, el derecho al olvido quedaría en la nada, y se transformaría en un remedio inútil. De hecho podría caerse en un circulo vicioso de republicar cada nuevo pedido, sobre todo los controversiales (personas famosas o asuntos de interés público).

Por supuesto, esto ha causado un gran debate público. El efecto de esto es que se divulgasen aún más esas noticias. Es posible que Google quiera informar a los medios para que se hagan eco y de esta forma se traslade a la sociedad que el derecho al olvido en algunos casos puede equipararse a una forma de censura indiscriminada e ilógica.

### 3.6. **Rol de las agencias europeas de protección de datos personales**

En el punto 24 el documento del WP29 reitera la idea central del derecho al olvido sobre su pre existencia al fallo del tribunal europeo y sobre su base en el tradicional derecho de protección de datos europeo.

El documento señala que mas allá de la novedad del caso "Google Spain", la decisión de delistar un determinado resultado del buscador implica en esencia analizar la aplicación de principios tradicionales de protección de datos personales al buscador de Internet.

Por ello el WP29 concluye que los pedidos presentados a agencias de protección de datos en función de rechazos por parte de buscadores deben ser tratados y analizados como cualquier otro reclamo de protección de datos según lo previsto en el art. 28(4) de la Directiva[21].

[21] Que dispone: "Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su

Asimismo se hace saber a los buscadores que deberán indicar cual de sus establecimientos será el encargado de recibir los pedidos y los dará a conocer a la comunidad.

## 4.Listado de criterios para resolver planteos de derecho al olvido identificados por el Grupo de Trabajo del Art. 29.

### 4.1. Naturaleza del documento del WP29

Cabe aclarar el documento del WP29 constituye *soft law*, no es una norma vinculante. El WP29 tiene entre sus cometidos elaborar guías orientadoras en materia de protección de datos y por ello ha elaborado desde hace 15 años numerosos documentos interpretando los más diversos aspectos del derecho de la protección de los datos personales.

Un análisis de los primeros reclamos recibidos por las diversas agencias de protección de datos europeas les permitió a estas elaborar un listado de elementos a tener en cuenta para cumplir con el fallo "Google Spain". Estos criterios deben aplicarse caso por caso.

### 4.2. Forma de aplicar los criterios

El listado de criterios que presentó el Informe del WP 29 fue elaborado a partir de la breve experiencia que tuvieron las agencias en los meses posteriores al fallo "Google Spain", y debe ser visto como una herramienta de trabajo. El informe propone las siguientes pautas para resolver los pedidos de derecho al olvido:

- que se examine caso por caso,
- los criterios deben aplicarse de acuerdo con la legislación nacional relevante del caso,

solicitud. Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.".

- en general, más de un criterio será necesario para resolver la cuestión en cada caso concreto; en otras palabras, los casos de derecho al olvido no pueden ser resueltos con un solo criterio,

- Cada criterio debe ser aplicado a la luz de los principios establecidos en el caso "Google Spain" y en especial a la luz del "interés del público general en tener acceso a la información"[22].

### 4.3. **Análisis de los criterios del WP29**

A continuación analizamos cada uno de los elementos propuestos en el Informe del WP29 y los ilustramos con ejemplos.

#### 4.3.1. **Primer criterio: Búsqueda relacionada con una persona individual**

El primer criterio que trata el documento es formal y funciona como una suerte de elemento legitimador del reclamo pues está relacionado con la identidad de la persona que reclama la tutela del derecho al olvido.

El Informe del WP 29 explica que la búsqueda realizada en Internet debe estar relacionada con una persona natural, esto es un individuo. Esta premisa se basa en el hecho que la Directiva Europea de protección de datos vigente tutela los datos personales de individuos y no de personas jurídicas. Ello es así pues la definición de "datos personales" es "toda información sobre una persona física identificada o identificable" (art. 2 "a" de la Directiva Europea).

Esto planteará un interrogante en los sistemas de protección de datos personales cuyo ámbito subjetivo se extiende a personas jurídicas además de individuos, tal el caso del régimen de Argentina[23] o el de Uruguay[24]. En estos supuestos las personas jurídicas podrían también invocar el derecho al olvido si el

[22] Esta afirmación del Grupo de Trabajo podría ser interpretada como que en caso de duda deberá estarse a favor de la información y no de suprimir el acceso a la misma.
[23] Art. 1 in fine de la ley 25.326 que dispone "Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal".
[24] Artículo 2 ley 18.331 que dispone "…El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda".

mismo es reconocido en esa jurisdicción y se considera que ese derecho sería trasladable a personas jurídicas[25].

Asimismo, el resultado de búsqueda debe aparecer cuando se busca por el nombre del individuo. Si ello no ocurre, el reclamante no tendría derecho a delistar el dato del resultado de búsqueda.

De esta forma se tiene en cuenta que el fallo "Google Spain" reconoció el impacto que una búsqueda en Internet basada en el nombre de una persona puede tener en su derecho al respeto de su vida privada.

En este primer punto el Grupo de Trabajo agrega un aspecto no mencionado expresamente en el fallo "Google Spain", aunque surge por lógica de cualquier legislación civil. El documento aclara que los pseudónimos y apodos (*pseudonyms and nicknames*) usados como términos relevantes de búsqueda, cuando un individuo pueda probar el uso del mismo y la relación con su identidad, deben ser considerados como términos de búsqueda válidos para legitimar un reclamo por la agencia de protección de datos que estudie el caso.

Cabe agregar que este criterio trata sobre el uso del nombre como criterio de búsqueda pero no decide ni aclara qué se puede remover del índice. Entre las posibilidades que podrían plantearse incluimos, a modo de ejemplo:

- un vínculo a una fotografía en vez del texto del nombre,

- la foto o imagen misma,

- sugerencias de búsqueda (la función autocompletar de Google),

- primeras líneas de resultados de búsqueda que erróneamente dan a entender algo de alguien,

- la referencia a una nota que aparece en los resultados de búsqueda porque existe un *metatag* en la web donde se aloja la nota (pese a que no se menciona expresamente a la persona por su nombre en el texto visible de la nota).

Parece que en la valoración del criterio para determinar la legitimación del reclamo no importa si la persona está expresamente mencionada en la nota sino que lo

[25] Existen numerosos argumentos en contra, el principal es que el derecho al olvido en el caso Google Spain está asociado a la Carta Europea de Derechos Fundamentales como un derecho humano, lo que no sería predicable de un ente ideal.

que legitima el pedido es que aparece el vínculo en una búsqueda como consecuencia de aparecer en el resultado de la búsqueda en el motor de internet. Sin embargo si en la nota no se menciona al titular del dato, no parece lógico eliminar la aparición en el resultado del índice. En este caso el reclamante debería acudir al sitio original con algún otro planteo diferente al derecho al olvido.

### 4.3.2. **Segundo criterio: Rol del reclamante en la vida pública – Figuras públicas**

El Informe explica que el tribunal en el caso "Google Spain" hizo una excepción expresa para titulares de datos personales que (i) tienen un rol en la vida pública, o (ii) donde haya un interés del público en acceder a la información sobre su persona.

En efecto el párrafo 97 del fallo "Google Spain" establece una clara excepción a la obligación de delistar resultados del buscador al señalar: "*…tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate….*".

El informe del WP 29 aclara que este criterio es más amplio que el criterio de figura pública. Aclara asimismo que no es posible establecer con certeza el tipo de rol en la vida pública que una persona debe tener para justificar que sea posible encontrar información sobre ella en forma pública a través de un resultado de búsqueda.

Como ejemplo, el WP 29 señala que los políticos, los oficiales públicos, la gente del mundo de los negocios[26] y los miembros de profesiones reguladas suelen tener un claro rol en la vida pública. Existe un fuerte argumento de que el público debe poder buscar (y encontrar) información relevante sobre sus roles y actividades públicas.

Como regla práctica para decidir si la información personal en cuestión debe seguir estando accesible, la agencia de protección de datos deberá preguntarse si el acceso a esa información amparará al público de conductas impropias a nivel profesional o público de estas personas.

[26] Se menciona el mundo de los negocios pero no el mundo de las celebridades.

El informe aclara que es también difícil definir el subgrupo de figuras públicas. En general señala que "podría decirse que las figuras públicas son individuos que, debido a sus funciones, tienen un alto grado de exposición pública".

Para definir qué constituye un rol en la vida pública, el Informe del WP29 cita la Resolución 1165 (1998) de la Asamblea Parlamentaria del Consejo de Europa[27] sobre el derecho a la privacidad que nos da una posible definición de "figuras públicas": son "personas que tienen un cargo público, o que usan recursos públicos, y en forma mas amplia, todos aquellos que juegan un rol en la vida pública, ya sea en la política, la economía, las artes, la esfera social, el deporte y cualquier otro dominio"[28].

Pero las personas públicas también tienen derecho a cierta privacidad. Por eso el documento del WP 29 señala que puede existir información sobre figuras publicas que es genuinamente privada y que no debería aparecer en los resultados de búsqueda, por ej. información sobre su salud o los miembros de su familia.

Como ejemplo de estos supuestos en Europa podemos citar el caso de "Noemi Campbell"[29] o caso de la princesa (ahora reina) Máxima de Holanda[30]. En ambos casos los tribunales ampararon aspectos de la privacidad de diversas personas públicas.

En la Argentina son ejemplos de privacidad de figuras públicas el caso Ponzetti de Balbín[31] y el caso "Menem v. Noticias"[32]. Pero cabe recordar que en el caso "Menem v. Noticias" la Corte Interamericana falló a favor de la publicidad de datos del hijo extramatrimonial de un funcionario público[33].

---

[27] Consejo de Europa, Asamblea Parlamentaria, Resolución 1165 (1998), disponible en http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta98/eres1165.htm, Assembly debate on 26 June 1998 (24th Sitting). See Doc. 8130, report of the Committee on Legal Affairs and Human Rights (rapporteur: Mr Schwimmer), Doc. 8147, opinion of the Committee on Culture and Education (rapporteur: Mr. Staes) and Doc. 8146, opinion of the Social, Health and Family Affairs Committee (rapporteur: Mr. Mitterrand).

[28] En su idioma original "*Public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain*".

[29] Campbell v MGN Ltd [2004] UKHL 22 (6 de mayo de 2004), [2004] UKHL 22, [2004] AC 457.

[30] Tribunal de primera instancia del Distrito de Amsterdam (Holanda), sentencia del 28/8/2009, caso 434415/KG ZA 09-1626 SR/MN, "Zijne Koninkjke Hoogheid Willem-Alexander, Prins Van Oranje et al v. The Associated Press" (sentencia de primera instancia firme).

[31] CSJN, 11/12/1984, "Ponzetti de Balbin v. Editorial Atlántida" (se consideró ilegal la publicación de fotografías de un político muy conocido en su lecho de muerte).

[32] El fallo de la cámara civil en el caso "Menem v. Noticias" mencionaba expresamente el derecho al olvido.

[33] Ver sentencia de la CIDH del 29/11/2011.

El documento señala que como regla general, si los solicitantes son figuras públicas, y la información en cuestión no constituye información genuinamente privada, en el balance deberá estarse más a la negativa a remover los resultados de búsquedas relacionadas con esos datos.

Para realizar el balance de derechos el informe del WP29 cita como ejemplo relevante el caso "Van Hannover v. Alemania"[34]. En este caso el Tribunal Europeo de Derechos Humanos sostuvo:

"*El rol o función de una persona concernida y la naturaleza de las actividades que son objeto del reporte o fotografía constituye otro importante criterio relacionado con el punto anterior. En tal sentido debe hacerse una distinción entre personas privadas y personas que actúan en un contexto público, tales como políticos o figuras públicas. Si bien una persona privada que es desconocida para el público en general puede reclamar protección de su vida privada, lo mismo no será cierto respecto a figuras públicas (ver los casos Minelli v. Switzerland (dec.), no. 14991/02, 14 June 2005, y Petrenco, citados antes, § 55). Una distinción fundamental debe ser hecha entre reportar hechos que son capaces de contribuir al debate público en una sociedad democrática, relacionada con políticos en el ejercicio de sus funciones, por ejemplo, y el reporte de detalles sobre la vida privada de un individuo que no ejerce esas funciones …".*

Como conclusión, cabe señalar que las cuestiones de interés público son el límite externo del derecho al olvido. El interés público señala hasta dónde puede llegar un ciudadano borrando su memoria digital pasada, o hasta dónde podrá subsistir la memoria colectiva en Internet respecto de esa persona. El límite, como podrá apreciarse, por ahora es muy difuso y deberá verse caso por caso. Con el tiempo podremos ir formando un criterio en función de los casos que se vayan presentando.

Es altamente probable que el derecho al olvido tome prestado la casuística de la jurisprudencia sobre los casos del derecho al honor que diferencian entre personas privadas y personas públicas y los asuntos de interés público.

[34] Hay dos casos en el Tribunal Europeo de Derechos Humanos con el mismo nombre, el primero del año 2012 y el segundo del año 2014. La cita corresponde al caso del año 2012, en Von Hannover c/Alemania, sentencia del 7/2/2012 en el cual el tribunal concluyó que Alemania había violado el derecho a la privacidad de Carolina de Mónaco al no aceptar sus reclamos judiciales sobre protección de la vida privada fundados en el art. 8 de la Convención Europea de Derechos Humanos. El mismo día el tribunal resolvió el caso Axel Springer donde concluyó que Alemania había violado el art. 10, sobre libertad de información.

### 4.3.3. **Tercer criterio: Datos sobre menores de edad**

El informe del WP29 sostiene que como regla general, si el titular del dato es legalmente menor de edad (ej. menor de 18 años a la fecha de publicación de la información), es más probable que la agencia de protección de datos se incline por la desindexación de sus datos de los resultados relevantes del buscador. El documento menciona expresamente la fecha de la publicación, no del reclamo de desindexación, lo cual es correcto para juzgar si se trata de una noticia sobre un menor.

El documento también sugiere que la agencia de protección de datos respectiva aplique el concepto de "mejor interés del niño" ("*best interest of the child*") para resolver el pedido.

Se recuerda que este concepto está contenido en el art. 24(2) de la Carta Europea de Derechos Fundamentales que dispone: "En todos los actos relativos a los niños llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del niño constituirá una consideración primordial". Este estándar está vigente en todas las leyes de menores.

En general las leyes de protección de datos personales no contemplan normas diferenciadas para menores, salvo algunas excepciones como el caso de Colombia[35]. Pero en los tratados internacionales y en la legislación sobre menores es común encontrar el estándar del "mejor interés del niño". La conclusión es que la presencia de datos de menores involucrados en la nota original o el hecho que el titular del dato personal que solicita el olvido sea un menor, inclinará la balanza a favor del menor.

### 4.3.4. **Cuarto criterio: Exactitud o inexactitud del dato personal**

Este criterio requiere preguntarse si el dato personal es exacto o inexacto. La Directiva Europea requiere que los datos personales sean "… exactos y, cuando sea necesario, actualizados" agregando la norma que "deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados" (art. 6 "e" de la Directiva Europea).

Ahora bien, el WP29 interpreta que no es necesario que el buscador esté monitoreando activamente Internet para detectar este tipo de inexactitudes, que por

[35] Cfr. REMOLINA ANGARITA, Nelson, Tratamiento de datos personales. Aproximación internacional y comentarios. Ley 1581 de 2012, Legis, Bogotá, 2013, pag. 170/175.

otra parte sería imposible de realizar. Sólo cuando se recibe un pedido concreto para eliminar del índice del buscador determinado contenido se deberá investigar el asunto y decidir si corresponde delistar o no dicha referencia de los resultados de búsqueda.

El documento señala que el término "exacto" se refiere a "exacto como una cuestión de hecho". Añade que se debe diferenciar entre una búsqueda en Internet que arroja como resultado la opinión que una persona tiene de otra persona y la búsqueda que aparenta tener información fáctica.

El informe del WP29 explica que en el Derecho de la Protección de Datos Personales los conceptos de exactitud, adecuación e incompletitud están relacionados. Es más probable que una agencia de protección de datos personales acepte delistar un resultado de búsqueda cuando la inexactitud proviene de una cuestión fáctica que presenta un perfil inexacto, incompleto de una persona.

El informe del WP29 cuando el titular del dato objeta el resultado de la búsqueda en base a la inexactitud del dato indexado, la agencia de protección de datos podrá atender el reclamo si está probada dicha inexactitud con información aportada por el titular.

El documento del WP29 termina señalando que si la inexactitud está sujeta a un proceso judicial o administrativo o a una investigación, entonces la agencia de protección de datos podrá optar por no intervenir hasta tanto se resuelva ese proceso. Aunque esto se refiere a la decisión que debe adoptar la agencia, también el criterio es válido para un tribunal que tenga que resolver sobre el derecho al olvido[36].

Este criterio entonces no es un criterio directamente a favor del titular del dato personal, pues requiere diferenciar las expresiones fácticas de las meras opiniones expresivas, y asimismo verificar si existe un proceso judicial sobre la cuestión específica debatida en el pedido donde se podrá estar discutiendo la verdad o falsedad de los hechos. El resultado de este proceso podrá ser a favor o en contra del reclamante e impactar tanto a favor como en contra de su pedido de desvinculación del índice.

[36] Por ejemplo en un caso holandés que comentamos recientemente en el diario La Ley el tribunal rechazó el olvido sobre una condena penal que aun no estaba firme. Cfr. nuestra nota *Derecho al olvido en Internet e información sobre condenas penales (a propósito de un reciente fallo holandés)*, La Ley 17/12/2014.

### 4.3.5. **Quinto criterio: Datos personales relevantes o excesivos**

En esta sección el Grupo de Trabajo sugiere evaluar si la información contenida en los resultados de búsqueda es relevante o excesiva de acuerdo al interés del público en acceder a la información.

Un punto para determinar la relevancia del dato personal es la antigüedad de la noticia. Dependiendo siempre de los hechos del caso, la información que fue publicada hace 15 años puede ser menos relevante que los datos publicados hace un año o hace solo unos días.

Por eso la agencia de datos personales debe evaluar la relevancia en función de los siguientes criterios que en modo alguno son exhaustivos sino sólo un muestreo de la problemática en relación a datos sobre el trabajo, datos sobre injurias y datos sobre opiniones de la persona:

***a). Datos personales que se refieren a la vida laboral del titular del dato:***

Una primera distinción que sugiere el Grupo de Trabajo del Art. 29 es entre la vida privada y la vida profesional de un sujeto.

El informe explica que la protección de datos y el derecho a la privacidad están enfocados en asegurar el derecho fundamental a la vida privada. Agrega que si bien todos los datos de una persona son datos personales, no todos sus datos son privados. Hay una distinción básica entre la vida privada de una persona y sus aspectos profesionales o públicos. La disponibilidad de la información en una búsqueda sobre una persona será más aceptable mientras menos aspectos revele de su vida privada.

Como regla general, la información relacionada con la vida privada de un sujeto que no juega un rol en la vida publica debe ser considerada “irrelevante”. Sin embargo, las figuras públicas también tienen un derecho a la privacidad aunque de forma limitada.

La información va a ser mas relevante si se refiere a la vida laboral del titular del dato personal, pero también dependerá del tipo de trabajo y del interés legítimo del público en tener acceso a esa información en una búsqueda en Internet usando el nombre del titular del dato.

Dos preguntas adicionales aparecen en el informe del WP29 como relevantes para precisar la pertinencia del dato. La primera es si los datos personales referidos al trabajo de la persona son excesivos; la segunda es si el titular del dato sigue relacionado con ese trabajo.

En ambos casos, si la respuesta es afirmativa posiblemente la conclusión de la agencia de protección de dato se inclinará por desvincular el dato del índice del buscador.

***b). Resultados injuriosos, ofensivos o que constituyen una expresión basada en el odio racial:***

Este criterio requiere preguntarse si el resultado incluye información que es injuriosa, ofensiva o que constituye una expresión basada en el odio racial.

El informe del WP29 señala que las agencias de protección de datos no tienen facultades ni están preparadas para lidiar con información que constituya calumnias, injurias, u ofensas a terceros incluidas cuestiones de "*hate speech*", esto es el discurso motivado por el odio racial o religioso, que es ilegal en Europa. En esos casos es común que las agencias de protección de datos reenvíen al reclamante a los tribunales pertinentes o a la policía cuando corresponda.

El informe aclara que la situación es diferente si un tribunal concluyó que la publicación de la información es una ofensa criminal y constituyó una violación de otras normas. Sobre este aspecto igualmente las Agencias de protección de datos son competentes para verificar la violación de la ley de protección de datos.

***c). Opiniones personales vs. hechos verificados.***

El *status* de la información contenida en el resultado de una búsqueda puede ser relevante, en particular a los fines de diferenciar entre una opinión personal y hechos verificados.

Las agencias de protección de datos personales han reconocido que algunos resultados de búsqueda contienen hipervínculos a contenidos que pueden ser parte de una campaña personal contra una persona, o constituir exabruptos (*rants*) o tal vez comentarios con la finalidad de disgustar a una persona.

Si bien la disponibilidad de esa información podrá herir los sentimientos de un individuo o incomodarlo, esto no significa necesariamente que la agencia de protección de datos considerará necesario que el resultado en cuestión sea removido del índice del buscador.

Sin embargo el informe concluye "la agencia de protección de datos deberá estar mas propensa a remover del índice el contenido que aparenta ser un hecho verificado, pero que es factualmente inexacto".

El informe usa el término "*factually inaccurate*" sin embargo nos parece un error. El derecho al olvido no procede porque los datos son falsos, sino porque son antiguos o violentan el principio de finalidad, pero siempre los datos son verdaderos. Si no son verdaderos el titular del dato no debe recurrir al olvido sino al derecho a rectificar información inexacta.

### 4.3.6. **Sexto criterio: Datos sensibles y derecho al olvido**

El sexto criterio se refiere a la existencia de datos sensibles[37] y requiere analizar el impacto que esta clase de datos tiene en la evaluación de retirada del índice del buscador de los vínculos en cuestión. El documento señala que esta clase de datos tiene mayor impacto en la vida privada del individuo que los datos personales comunes u "ordinarios".

El informe cita como ejemplo a los datos sobre salud, sexo o creencias religiosas. Las agencias de protección de datos serán más propensas a intervenir y decidir a favor de la desindexación cuando el rechazo sea sobre cuestiones que revelen datos sensibles al público.

Es cierto que se deberá analizar el contexto de la noticia y la situación concreta del sujeto. Por ejemplo un sacerdote o un rabino que aparecen mencionados en una nota con sus posiciones no podrían cuestionar que se haga referencia a su religión pues en esos casos es algo notoriamente público[38]. Pero el ciudadano común

[37] El artículo 8 de la Directiva Europea dispone que "Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad". Curiosamente la directiva europea no menciona la palabra sensible al tratar datos sensibels. La Directiva Europea contiene una SECCIÓN III titulada "CATEGORÍAS ESPECIALES DE TRATAMIENTOS".

[38] Cfr. art. 8.2. inc. e) de la Directiva Europea: "Lo dispuesto en el apartado 1 no se aplicará cuando… e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos…".

puede tener reservas sobre la revelación indiscriminada de sus creencias religiosas en Internet[39].

### 4.3.7. **Séptimo criterio: Dato personal accesible mas allá de lo necesario para la finalidad para la cual fue procesado**

El séptimo criterio que analiza el grupo lleva a preguntarse si el dato personal accesible mas allá de lo necesario para la finalidad para la cual fue procesada. El principio de finalidad sostiene que los datos deben ser procesados exclusivamente para la finalidad por la que fueron recolectados.

En este punto el informe señala que como regla general, las agencias de protección de datos deben usar este factor con el objetivo de asegurarse que la información que ya no está razonablemente actualizada o que se ha vuelto inexacta por el transcurso del tiempo debe ser desvinculada del índice del buscador. Tal evaluación dependerá de la finalidad del procesamiento o de la recolección original de los datos personales.

Entendemos que este es un tema central en la evaluación de la procedencia del derecho al olvido, y en general esta evaluación debe hacerse caso por caso. Pero es lamentable que el Informe del WP29 le dedique tan poco desarrollo a este criterio, mas allá de su mera mención.

Este criterio tiene otro problema que es la fuente original del dato, generalmente un medio de prensa, que suelen estar exentos de l régimen de protección de datos personales (por ej. art. 9 de la Directiva Europea y normas locales concordantes). Este criterio termina aplicando en forma indirecta el principio de finalidad a una nota periodística (que deja de ser hallable a través del buscador tipeando el nombre del titular del dato) pese a que el fallo “Google Spain” divide los tratamientos del buscador y del editor de la página web como dos procesamientos distintos.

### 4.3.8. **Octavo criterio: El perjuicio al titular del dato personal**

Bajo el Derecho Europeo de protección de datos personales no es obligatorio que el titular del dato personal demuestre un daño concreto a los fines de obtener la desvinculación de su nombre del índice del buscador.

[39] Aqui nuevamente aparece la línea divisoria entre el derecho de supresión, el derecho al olvido y la supresión de un dato porque es íntimo, personal o privado.

En otras palabras, de acuerdo a la interpretación del Tribunal Europeo de Justicia en el caso "Google Spain" la existencia de un perjuicio concreto no es una condición para el ejercicio del derecho al olvido del titular del dato[40].

Sin embargo, el informe del WP29 aclara que cuando hay evidencia clara que los resultados de búsqueda están afectando concretamente al titular del dato, éste debe ser un factor que juega a favor de delistar el nombre de la persona del índice del buscador.

Cabe recordar que la Directiva permite al titular del dato personal objetar un tratamiento de datos cuando existen "*compelling legitimate grounds*". Cuando la objeción está justificada, el responsable del tratamiento debe cesar el tratamiento de datos personales.

También el documento señala que los datos pueden tener un impacto desproporcionado en el titular del dato personal cuando una búsqueda en Internet revela eventos triviales o "hechos ilícitos menores" que ya no son objeto de debate público y donde no hay más interés en hacer accesible la información en cuestión.

#### 4.3.9. **Noveno criterio: Información encontrada a través del buscador que pone en riesgo a la persona**

Este criterio hace alusión a las situaciones donde la disponibilidad de información en búsquedas de Internet puede dejar a los sujetos expuestos a un riesgo serio y concreto, y se ejemplifica con casos de robo de identidad, secuestros, amenazas o acoso (e.j. *stalking*). También cabe citar como otros ejemplos testigos de identidad reservada u oculta, cambio de nombre y domicilio de personas por protección en casos de terrorismo, casos de violencia familiar o de género donde se identifica la residencia de la víctima y ello causa un grave riesgo a su integridad personal o la de su entorno.

La existencia de este *riesgo* adicional es un elemento distinto a la exigencia de daño concreto, que, como se explicó, no resulta necesaria en el derecho europeo de la

[40] Así en el párrafo 96 del fallo "Google Spain" el tribunal señaló que "… al apreciar tales solicitudes presentadas contra un tratamiento como el controvertido en el litigio principal, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre. A este respecto, cabe señalar que la apreciación de la existencia de tal derecho no presupone que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado".

protección de los datos personales. Es un elemento –el riesgo a la persona o sus bienes- que de estar presente inclinará la balanza a favor del titular del dato personal.

Desde hace años, los buscadores rutinariamente remueven de su índice datos tales como números de tarjetas de crédito o cuentas bancarias, datos de identificación personal, números de seguridad social, pasaportes, firmas escaneadas, etc. con el fin de evitar la divulgación de estos datos personales. Por ende este punto no parece generar mayor controversia.

#### 4.3.10. **Décimo criterio: Contexto en el cual fue publicada originalmente la información.**

El informe del WP29 trata dos cuestiones importantes relativas al contexto en que fue publicado el dato personal. Primero se pregunta si se trata de una revelación voluntaria del titular del dato. Segundo, si el contenido estaba destinado a hacerse público y también si el titular del dato podría haber razonablemente sabido que se haría público.

En el primer caso podría suceder que el dato personal fue válidamente publicado con el consentimiento de su titular. Luego éste no quiere que siga estando accesible (revoca el consentimiento) y por ende la actividad de tratamiento y difusión del dato carece de base legal y debe cesar. El informe del WP29 explica que si la única base legal para la difusión del dato es el consentimiento, y éste es revocado, la actividad de procesamiento deja de tener base legal. Restaría analizar y enumerar –cosa que el informe del WP29 no hace- cuales son las bases o supuestos en los cuales se puede publicar sin consentimiento del titular del dato.

Al Informe del WP29 también le faltó aclarar que en ciertos contextos el titular del dato tiene un control casi absoluto sobre la información que él publicó (ej. en una red social) y en esos casos no tiene sentido recurrir al derecho al olvido: el sujeto simplemente debe configurar los controles de la red social, hacer privado su perfil o el dato, o simplemente borrarlo si las funcionalidades de la red social se lo permiten. Por eso en principio estos casos podrían quedar fuera del derecho al olvido.

### 4.3.11. **Undécimo criterio: Contenido publicado con fines informativos por la prensa**

Las agencias de protección de datos han considerando en algunos casos que dependiendo del contexto, puede ser relevante considerar que la información fue publicada con fines periodísticos o informativos.

Según el informe del WP29, el hecho que el dato fue publicado por un periodista[41] cuyo trabajo es informar al público debe ser un factor importante a valorarse en el análisis. Entendemos que debería jugar a favor de mantener el dato personal, lo cual sin embargo no implica que no exista derecho al olvido sobre notas periodísticas.

Sin embargo este criterio aislado no constituye un fundamento en si mimo para denegar un pedido para delistar contenidos del índice del buscador pues el fallo "Google Spain" claramente separa la base legal que usó la prensa para publicar una nota (o realizar tratamiento de datos personales), y la base legal que los buscadores tienen para organizar los resultados de búsqueda en función del nombre de una persona (que también implica realizar tratamiento de datos personales).

### 4.3.12. **Criterio decimosegundo: Obligación legal de publicar los datos personales**

El criterio n. 12 que analiza el documento del WP29 se pregunta si existe una obligación o facultad legal del editor de hacer públicamente accesible la información.

Ciertas autoridades públicas (ej. las que están a cargo de registros públicos) tienen el deber legal de hacer accesible al público cierta información personal. Esto varía y depende de cada jurisdicción y las reglas legales y costumbres allí imperantes.

En estos supuestos el Grupo de Trabajo sugiere que la autoridad de protección de datos no deberá desindexar la información mientras el requisito de publicidad del dato subsista. Sin embargo se sugiere analizar el caso específico, junto a otros criterios como la irrelevancia o no del dato y su actualidad.

El documento aclara sin embargo que la agencia de protección de datos puede considerar que la desindexación es apropiada incluso si existe una obligación legal de

[41] Cabe admitir que hoy en día el concepto de periodista se ha desdibujado por las numerosas personas que tiene canales alternativos para publicar noticias como es el caso de blogs, twitter, redes sociales, etc.

hacer accesible el contenido en el sitio original. Esto se justifica en la teoría de que hay dos tratamientos separados de datos personales, el del sitio original y el del buscador.

El Grupo de Trabajo no da ejemplos pero pensemos en las autoridades que tienen por fin informar, por ejemplo el registro de deudores de cuota alimentaria, o el boletín oficial que publica constantemente información con los fines de lograr la publicidad de los datos y actos administrativos allí contenidos. Estos registros pueden ser indexados por el buscador y arrojar resultados muy antiguos cuando se busca el nombre de una persona en la web.

### 4.3.13. **Criterio décimo tercero: Datos que se refieren a un delito penal**

El Informe del WP29 señala que los países miembros tienen diferentes legislaciones y enfoques en la materia. Existen diversas posiciones que se reflejan en multitud de normas regulando la posibilidad de publicar o no el nombre de quien cometió un delito, o el delito cometido y esto puede impactar en la disponibilidad de la información una vez transcurrido cierto tiempo. Por ello el informe del WP29 explica que cada agencia de datos personales deberá tratar el caso de acuerdo a los principios nacionales aplicables que varía según cada país[42].

Como regla general, se señala que la agencia de datos personales deberá ser favorable a considerar la desindexación de resultados que se refieran a ofensas penales menores que ocurrieron hace largo tiempo mientras que deberán rechazar pedidos de desindexación de hechos mas serios o que hayan ocurrido recientemente. El informe concluye que es necesario el enfoque caso por caso.

Un precedente reciente sobre este último supuesto tuvo lugar en Holanda. El actor había demandó ante los tribunales holandeses al buscador Google invocado el caso "Google Spain" y pretendía que se elimine de los resultados y sugerencias de Google la mención de su nombre, y un video en Youtube que fue la base de su condena penal por ser autor intelectual de una tentativa de homicidio. El tribunal de primera instancia holandés rechazó el pedido de derecho al olvido de la condena[43].

---

[42] Ver Elena LARRAURI PIJOAN, *Criminal record disclosure and the right to Privacy*, Criminal Law Journal n. 10, 2014, http://www.upf.edu/pdi/larrauri/_pdf/Elena__x2014x_Crim.L.R._10x1x.pdf

[43] Tribunal de primera instancia en lo civil de Amsterdam (Holanda), 18/9/2014, caso n. C/13/569654/ KG ZA 14-960 PS/BB, Arthur van M. v. Google Netherlands y Google Inc. y nuestro comentario: *Derecho al olvido en Internet e información sobre condenas penales (a propósito de un reciente fallo holandés)*, La Ley 17/12/2014.

## 5.CONCLUSIONES PRELIMINARES

El documento del WP 29 comentado en este artículo es muy importante pues refleja los primeros criterios meditados sobre la forma de implementar el derecho al olvido en Internet. El derecho reconocido en el caso "Google Spain" es muy complejo y difícil de implementar.

Muchos de las conclusiones que elabora el Informe del Grupo de Trabajo superan lo decidido por el Tribunal y llevarán a preguntarse a los operadores de Internet si no ha existido un avance mayor al fallo con posterioridad al caso "Google Spain".

En particular el Informe amplia no solo a nombres de personas sino también a apodos o sobrenombres. También expande en forma universal el alcance del derecho al olvido a todos los niveles de dominios, no solamente los europeos (ej. .co.uk, .fr., .es) sino al .com. Finalmente también se manifiesta en contra de notificar en forma individual las remociones y de poner avisos generales sobre remoción de contenidos del índice.

Todo estos "ajustes" eran de alguna forma necesarios. Es cierto también que el Grupo de Trabajo del Art. 29 abrió nuevos debates. Todo ello demuestra que el derecho al olvido es un derecho que va a estar en constante formación y evolución en sus primeros años.

Estos ajustes del WP29 podrán ser convalidados o no a nivel individual por cada miembro de la Unión Europea. Lo más probable es que ello ocurra pues el Grupo de Trabajo del Art. 29 está integrado por representantes de las propias agencias europeas de protección de datos personales. Los criterios elaborados por el WP29 son una "ida y vuelta" dentro del "dialogo europeo" en materia de protección de datos personales.

Es de esperar entonces que en una primera etapa, la jurisprudencia local validará o no estos criterios en cada caso luego de emitido un pronunciamiento por la agencia de protección de datos local. También podrá encontrar nuevos criterios mas allá de los 13 mencionados en el reporte del WP29.

En una segunda etapa, cuando la nueva Regulación europea sea aprobada y entre en vigencia (con una redacción final del derecho al olvido que aun se desconoce), se esperan nuevos debates sobre la interpretación del nuevo texto legal. Y estos nuevos

debates podrían dar lugar a un nuevo fallo del TJUE interpretando el nuevo texto de la Regulación y convalidando o no su criterio anterior, basado en la Carta Europea de Derechos Humanos. Como dijo un conocido especialista español al comentar el caso del TJUE sobre derecho al olvido: "…el fallo del Tribunal Europeo de Justicia fue sólo el comienzo".

CYBERLAW by CIJIC

# RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM DOTMLPI-I

# INFORMATION SECURITY INCIDENTS RESPONSE: AN DOTMLPF-I APPROACH

**PAULO J. BAPTISTA DAS NEVES** [1]

e

**FERNANDO JORGE RIBEIRO CORREIA** [2]

[1] Capitão-Tenente Marinha – DITIC. Correio Eletrónico: baptista.neves@marinha.pt
[2] Capitão-de-Fragata Escola Naval, CINAV. Correio Eletrónico: ribeiro.correia@marinha.pt

**SUMÁRIO: 1. INTRODUÇÃO; 2. A METODOLOGIA DOTMLPI-I; 3. CAPACIDADE DE RESPOSTA A INCIDENTES DE SEGURANÇA E O DOTMLPI-I; 4.CONCLUSÃO; 5.REFERÊNCIAS**


## RESUMO

O conceito de ciberespaço resulta da interligação das redes de comunicações e de diferentes sistemas de informação à escala global. A abstração deste espaço de comunicações apresenta evidentes vantagens para a sociedade de informação em que vivemos. A sua utilização maciça por indivíduos e organizações fez com que ele se tornasse crítico para as empresas e para o próprio estado, pois a exploração das vulnerabilidades dos diferentes sistemas que o utilizam podem afetar as infraestruturas que prestam serviços críticos à sociedade. Para assegurar a qualidade da informação que nele circula é necessário que existam mecanismos de monitorização permanentes, com capacidade de prevenção e resposta aos incidentes que coloquem em causa a segurança da informação.

Existem já vários modelos e normativos para a organização desta capacidade de resposta a incidentes de segurança da informação. Neste artigo iremos apresentar a metodologia utilizada pela OTAN para a edificação de capacidades operacionais, aplicando-a à identificação dos elementos críticos a considerar na edificação de uma capacidade de resposta a incidentes de segurança da informação no ciberespaço.



**Palavras-Chave:** Ciberespaço, Cibersegurança, Resposta a Incidentes, DOTMLPI-I.

## ABSTRACT

The concept of Cyberspace results from - on a global scale - the interconnection of communication networks and different information systems. This immense communication space produces clear benefits for the information society in which we live. Its massive use by individuals and organizations made him critical for companies and for the state itself, since exploiting vulnerabilities of different systems that they use may affect the infrastructures that deliver critical services to society. There has to be permanent monitoring mechanisms - capable in prevention and response to incidents that may undermine the security of information - to ensure the quality of the information that flows.

There are already several models and standards for organizing the capacity to respond to information security incidents. In this article we will present the methodology used by NATO to the edification of operational capabilities and apply it to the identification of critical elements to consider when building one capacity to respond to information security incidents in cyberspace.

**Keywords:** Cyberspace, Cyber Security, Incident Response, DOTMLPF-I.

## 1.INTRODUÇÃO

Para uma sociedade de informação como aquela em que vivemos, com comunicações omnipresentes quer a nível pessoal quer ao nível das instituições, o ciberespaço [3] apresenta evidentes vantagens, tornando realidade a sensação de ubiquidade. André Matias e Rogério Bravo no seu artigo sobre o ciberespaço "Geopolítica, geoestratégia e ciberespaço: Notas introdutórias" 0 mencionam que os vetores espaço, tempo e caminho percorrido para se movimentar de um ponto para o outro, praticamente desaparece.

A vantagem de poder chegar instantaneamente a todo o lado, a independência dos fusos horários, levou a que também os Estados e as Empresas utilizem o Ciberespaço como base para as suas infraestruturas de comunicações, não só entre si, mas também como rede de suporte ao comando e controlo das suas infraestruturas, muitas das quais disponibilizam serviços críticos à sociedade.

O Ciberespaço é assim uma realidade complexa onde interagem diferentes dimensões da sociedade e onde o valor maior reside na qualidade da informação que nele circula, seja na comunicação entre pessoas, entre organizações ou mesmo nas comunicações de comando e controlo de sistemas críticos. Este é um espaço virtual cujos acontecimentos se repercutem no mundo físico, tornando-se assim um problema global.

Sendo então a segurança do Ciberespaço vital para a garantia da qualidade da informação, que como vimos poderá ter impacto ao nível dos serviços básicos para o funcionamento da sociedade ou mesmo da soberania do país, estando este sujeito a ameaças que tanto poderão ter origem em atos de protesto social, ou relacionadas com objetivos de natureza criminosa ou mesmo de guerra, compete primariamente aos governos dos países a organização para a segurança e defesa deste espaço. A segurança da informação e a proteção das infraestruturas críticas são da responsabilidade do Estado que "terá de garantir não só a utilização segura do ciberespaço aos seus cidadãos como a salvaguarda da própria soberania" [3].

[3] "Um domínio global e virtual criado pela interligação de todas as redes de Comunicações, informação e sistemas eletrónicos e a informação armazenada e processada ou transmitida nesses sistemas" 0.

De modo a desenvolver as capacidades de Cibersegurança, o estado português, seguindo as recomendações da União Europeia onde cada estado membro deve implementar uma capacidade de resposta a incidentes de segurança cibernética [4], através do decreto-lei 69/2014 de 9 de maio, decidiu criar o Centro Nacional de Cibersegurança (CNCS). O Centro está na dependência direta da Autoridade Nacional de Segurança com "*a missão de contribuir para que Portugal use o ciberespaço de uma forma segura e as suas competências não prejudicam as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço, nomeadamente no que respeita a infraestruturas críticas e integridade das redes e serviços, sendo exercidas em coordenação com estas entidades"* [5].

Em 2015 o governo de Portugal definiu a estratégia nacional de Segurança do Ciberespaço, onde são apresentados como objetivos estratégicos a promoção de "*uma utilização consciente, livre, segura e eficiente do ciberespaço*", a proteção "*dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos", o fortalecimento da "segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais" e a afirmação do "ciberespaço como um domínio de desenvolvimento económico e de inovação*" [6].

A Cibersegurança materializa-se numa verdadeira capacidade de antecipar e responder a incidentes de natureza cibernética que afetem a qualidade da informação que circula no ciberespaço nacional. Existem vários normativos como a ISO/IEC 27035, o guia de boas práticas da ENISA ou o NIST SP 800-61, que apontam metodologias para a edificação de uma capacidade de resposta a incidentes de segurança da informação, neste artigo propomos a utilização da metodologia DOTMLPI-I para a identificação dos elementos críticos a considerar na edificação desta capacidade. Começaremos por apresentar a metodologia DOTMLPI-I e o modo como as Forças Armadas a utilizam para a edificação de capacidades operacionais. No ponto seguinte iremos aplicar esta metodologia para a identificação dos elementos críticos a ter em consideração para a identificação da uma capacidade operacional de resposta a incidentes de segurança da informação. Finalmente apresentaremos as conclusões resultantes da utilização desta metodologia a este tema da Cibersegurança.

## 2.A METODOLOGIA DOTMLPI-I

O acrónimo DOTMLPI (Doutrina, Organização, Treino, Material, Liderança, Pessoal e Infraestruturas) refere-se aos componentes básicos da edificação de uma capacidade operacional, desenvolvido pelo Departamento da Defesa dos EUA (*Department of Defense – DoD*). É uma abordagem à implementação de capacidades operacionais, de modo a identificar lacunas na sua operacionalização[7]. A este modelo básico, o *DoD* viria a adicionar uma outra componente, as Políticas, com o objetivo de adicionar a esta abordagem a procura de procedimentos comuns entre os diversos utilizadores na utilização da nova capacidade. Este novo modelo é conhecido por DOTMLPI-P [8]. A OTAN adotou este modelo básico de implementação de novas capacidades fazendo apenas uma alteração, a troca do conceito de Políticas por um outro que lhe é bastante caro, a Interoperabilidade, nascendo assim o acrónimo DOTMLPI-I [9].

Antes de abordar cada um dos diferentes domínios que compõem esta metodologia DOTMLPI-I e a sua relevância para a edificação de uma capacidade operacional, seguindo uma perspetiva militar, importa definir este conceito de capacidade. De acordo com a definição da OTAN, uma capacidade operacional é a possibilidade de um comandante militar conseguir executar um conjunto específico de ações, identificando os efeitos necessários para atingir determinado objetivo [10]. Desta definição resulta que uma capacidade operacional é complexa e que não se resume a questões de material ou de procedimentos, no fundo é necessária uma abordagem holística como a que permite a DOTMLPI-I, para o sucesso do seu desenvolvimento e implementação.

### DOUTRINA

Numa perspetiva militar a Doutrina aparece ligada ao modo como são conduzidas as operações de combate, sejam manobras, campanhas ou outras, ou seja, os princípios fundamentais que permitem a utilização coordenada de uma ou mais forças militares para atingirem um objetivo comum. A Doutrina baseia-se em princípios comuns, construídos sobre as lições aprendidas durante as operações militares, através de treinos e exercícios. Considerando a sua caraterística imperativa para as Forças militares em campanha, esta está sempre sujeita às políticas comuns acordadas entre

as partes, aos tratados e a restrições de natureza legal, devendo ser sempre seguida, exceto se, de forma muito excecional, o comandante em exercício assim o entender.

## ORGANIZAÇÃO

A Organização diz respeito ao modo como os indivíduos se constituem como equipas, e estas em unidades operacionais, executando as funções que lhes são determinadas, de forma a contribuírem para o sucesso da missão. Estas unidades operacionais são suportadas numa estrutura que permite que funcionem de forma coordenada. Esta estrutura tem configurações diversas, de natureza diferenciada e multidisciplinar, conforme se destine às operações propriamente ditas ou a ações de suporte e manutenção. Do desempenho desta estrutura depende em grande parte o sucesso das missões como tal as ações de Treino assumem particular importância.

## TREINO

Como descrito no parágrafo anterior, o Treino das equipas é fundamental, sejam unidades individuais, de grupo ou mesmo alianças internacionais, de natureza operacional ou de suporte às várias estruturas que participam nas operações. Só o treino permite aos diversos intervenientes num teatro de operações a resposta pronta e capaz às necessidades estratégicas, operacionais e táticas do comando. Uma das formas de executar as ações de treino é através de exercícios que *incorporem os aspetos apropriados do ambiente operacional no cenário de treino, permitindo à audiência de treino a aprendizagem dos conceitos necessários às diversas capacidades, observando a execução do exercício* [8]. As lições aprendidas através do treino permitem a revisão ou mesmo o desenvolvimento de novos conceitos, com impacto direto no aperfeiçoamento das capacidades operacionais.

## MATERIAL

O Material refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais. Esta dimensão abrange desde os equipamentos, à tecnologia, às armas, ou as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão. Os problemas que surgem nesta área podem ter soluções de natureza material, adquirindo o artigo necessário para a sua resolução. Por outro lado também podem ser problemas que não sejam resolúveis através de qualquer aquisição, ou seja, terão de ter uma solução não-material, implicando assim soluções

que envolvam alterações nas outras dimensões, como por exemplo na doutrina, na organização ou no treino [11].

## LIDERANÇA

Nesta metodologia a Liderança surge diretamente ligada à Formação, preocupando-se essencialmente com a preparação das chefias para uma abordagem profissional da operação, ou seja ao desenvolvimento da competência profissional para comandar. É fundamental que o líder seja capaz de compreender o objetivo que lhe é apresentado e que conduza a ação para que este seja alcançado com sucesso. Tem de ter a capacidade de dirigir e motivar os membros da equipa, com profissionalismo, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo, as suas capacidades com vista ao sucesso da missão. Como refere *Cecília Bergamini*, *todas as organizações podem contar com bons líderes desde que lhes dispensem o treino adequado e promovam um ambiente favorável onde possam agir com eficácia* [12].

## PESSOAL

No referente ao Pessoal o mais importante é garantir que este possui as qualificações necessárias para o desempenho da missão, quer considerando as necessidades em tempo de paz, quer em tempo de crise. O fator humano e a componente social são determinantes, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e disponibilizarem-lhes a formação adequada. Por outro lado é preciso considerar que para algumas missões, o pessoal pode não ter as competências necessárias, sendo por isso necessário envolver pessoal externo ou parceiros civis, como sejam as empresas do setor tecnológico ou outras, para que se possa cumprir a missão. Quando identificadas lacunas na formação do pessoal, ou o surgimento da necessidade de novas competências relevantes para a missão, deve ser feita a ponderação de alteração do plano de formação previsto para os diferentes papéis que os elementos desempenham no seio da equipa ou a contratualização do serviço a entidades externas. Finalmente há que considerar um quadro de pessoal que garanta a disponibilidade dos recursos humanos necessários quer em tempo de paz quer em tempo de crise.

## INFRAESTRUTURAS

As Infraestruturas são tudo o que se refere com a disponibilização de instalações adequadas à preparação e condução das operações. Também aqui é importante garantir que as Infraestruturas existentes permitem responder de forma satisfatória aos requisitos de manutenção em tempo de paz e aos requisitos operacionais em tempo de crise. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, oficinas, armazéns, centros de dados, estradas, distribuição de energia elétrica e água, entre outras.

## INTEROPERABILIDADE

A estas sete dimensões básicas do modelo, o DoD dos EUA acrescentou as Políticas, mas a OTAN optou por estabelecer um conceito mais abrangente, a Interoperabilidade. Na verdade a diferença é quase inexistente e podemos mesmo considerar que os objetivos são idênticos. No fundo o que esta dimensão extra do modelo pretende é colocar em destaque a importância de existir uma abordagem comum entre as várias entidades ou equipas que participam nas operações. O estabelecimento desta abordagem comum implica que se utilize um conjunto de conceitos partilhados entre as partes, que todos entendam como válidos. Isto pode ser conseguido através de políticas que definam procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo. A OTAN define-a como “a capacidade de agir em conjunto de forma coerente, efetiva e eficazmente para atingir os objetivos táticos, operacionais e estratégicos da Aliança” [13]. De acordo com a missão, existe a necessidade de conduzir as operações num ambiente alargado de parcerias com os nossos aliados por isso a Interoperabilidade assume um papel de destaque na edificação de uma capacidade operacional.

## 3.CAPACIDADE DE RESPOSTA A INCIDENTES DE SEGURANÇA E O DOTMLPI-I

No ponto anterior foram apresentadas as várias dimensões do modelo DOTMLPI-I, fazendo uma análise básica de cada um dos seus componentes numa vertente de militar. Segue-se uma análise das mesmas dimensões, mas tendo agora por base os conceitos relacionados com a implementação específica de uma capacidade operacional de resposta incidentes no âmbito da Cibersegurança.

### DOUTRINA

A existência da Doutrina é fundamental na edificação de uma capacidade de Cibersegurança. Através dela são definidos os objetivos e o âmbito em que se inserem as ações a realizar, contextualizando a existência da capacidade em causa, no panorama global das outras instituições e organizações com responsabilidades idênticas e que têm necessariamente de interagir entre si. Dependendo do contexto em que a capacidade se insere, os documentos doutrinários são tipicamente as leis nacionais que regulam as atividades no Ciberespaço, as Estratégias Nacionais para a Cibersegurança, que definem os objetivos do Estado ou das Organizações e o seu âmbito de atuação no Ciberespaço, bem como os documentos doutrinários que definem as políticas de utilização do mesmo e o modo como interagir com os diferentes atores neste domínio. A ausência destas políticas provoca ambiguidades e reduzem a eficácia de uma efetiva capacidade de Cibersegurança. Ao nível nacional, Estratégia Nacional para a Cibersegurança do Ciberespaço apresenta-se como um importante documento doutrinário, não só pela definição dos objetivos estratégicos do país, mas vai mais longe ao apontar de forma inequívoca as orientações para a sua concretização.[4] Apresenta-se ainda como exemplo de documentos doutrinários a Lei do Cibercrime [14], que regula a utilização da informática e criminaliza as atividades ilícitas de natureza cibernética (em complemento a outros crimes já tipificados no Código do Penal), a publicação do Estado Maior General das Forças Armadas PEMGFA/CSI/301 que estabelece a estrutura orgânica, as normas e os procedimentos para garantir a Capacidade de Resposta a Incidentes de Segurança Informática das

[4]A estratégia nacional de segurança no ciberespaço apresenta como principais eixos de intervenção a "Estrutura de segurança do ciberespaço", o "Combate ao cibercrime", a "Proteção do ciberespaço e das infraestruturas", a "Educação, sensibilização e prevenção", a "Investigação e desenvolvimento" e a "Cooperação" [6].

Forças Armadas ou a sua equivalente PCA 16 sobre a Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha.

## ORGANIZAÇÃO

A Organização de uma capacidade de Cibersegurança, no seu sentido mais lato, não difere da organização de outras capacidades. Importa definir uma estrutura organizacional que suporte as diferentes atividades que se pretendem implementar e as respetivas relações e dependências hierárquicas e funcionais. Tipicamente existe um nível superior de decisão e coordenação geral, que poderá agregar as atividades que mais se afastam da sua natureza funcional em órgãos de apoio, como por exemplo a assessoria jurídica ou financeira e a gestão do pessoal. No caso de uma capacidade de Cibersegurança é natural que as diferentes valências técnicas e funcionais se organizem em departamentos com objetivos comuns. Como exemplo apresentamos a necessidade de existência de um departamento de operações no ciberespaço que inclua a gestão de incidentes, um departamento para a definição de políticas e normalização, com uma área de auditoria, que deverá ser independente de todas as outras, com a função de validar o cumprimento das normas, um departamento para a gestão da configuração e apoio técnico aos sistemas e às comunicações com um serviço de *helpdesk*.

## TREINO

O Treino é um domínio essencial do modelo para a manutenção e desenvolvimento de uma capacidade. No caso particular do nosso objeto de estudo, a capacidade de respostas a incidentes de segurança é apresentada com objetivos de treino muito concretos, os quais importa que as equipas e a própria organização atinjam, pois são determinantes para garantir esta capacidade. A capacidade de resposta a incidentes de segurança depende fortemente de equipas com a formação adequada e com processos de atuação perfeitamente interiorizados, pois em algumas situações de elevado risco, a garantia da qualidade da informação depende de uma ação pronta e eficiente. A OTAN organiza anualmente exercícios de natureza cibernética para treino das suas estruturas. Nos exercícios denominados *Cybercoalition*, a OTAN define como objetivos principais de treino a Capacidade de Decisão, a Coordenação, a Partilha de Informação e o treino das Capacidades Técnicas [15]. Desta forma assumem-se com principais objetivos de treino a

Capacidade de Decisão com base nas informações disponíveis, escolhendo as melhores ações a realizar perante a natureza do incidente, o que devido à grande variedade de ameaças e de fontes de informação disponíveis, requer um treino específico. Outro aspeto que é essencial treinar, é a Coordenação das equipas e dos vários atores que participam no processo de responder a um incidente. É normal o incidente ser detetado, por exemplo numa plataforma de segurança e que os mecanismos de resposta desencadeados com vista à resolução do incidente ou à mitigação da vulnerabilidade, envolvam entidades externas à equipa que está a gerir o incidente, como por exemplo a equipa de administração dos serviços ou comunicações, sendo fundamental que estas ações sejam bem coordenadas de modo a que atinjam o máximo de eficácia. Na sequência das atividades de coordenação apresentadas, surge como natural o objetivo de treinar a Partilha da Informação. Quando a resposta ao incidente tem de envolver entidades externas é expectável que surjam algumas dificuldades, relacionadas com a utilização de ferramentas e processos distintos, que não permitam uma ação coordenada. Estas dificuldades devem ser detetadas durante as ações de treino, levando à procura e desenvolvimento de processos de comunicação comuns ou pelo menos compatíveis, com vista a uma normalização de procedimentos e de taxonomia. Outro grande objetivo é o treino das Capacidades Técnicas dos vários elementos que compõem as equipas de resposta a incidentes. Para tal é importante que durante o treino sejam simuladas situações tão próximo quanto possível do real, que coloquem os elementos das equipas em situações imprevistas, que os obriguem a explorar completamente as ferramentas que utilizam diariamente, sendo assim possível identificar lacunas na sua formação ou inadequabilidade das ferramentas utilizadas em face da ameaça.

## MATERIAL

Como vimos anteriormente, no modelo DOTMLPI-I o Material refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais, desde os equipamentos, à tecnologia e às infraestruturas de comunicações. No caso específico da tecnologia utilizada numa capacidade de resposta a incidentes de segurança da informação, iremos considerar quatro categorias distintas, os equipamentos de

proteção e monitorização que geram a *informação em bruto*[5], os equipamentos que realizam a agregação e arquivo dessa informação e a correlacionam de modo a gerar informação com mais valor, os equipamentos ou tecnologias que permitem fazer a gestão da informação sobre os incidentes, e por ultimo, as tecnologias de análise que permitem a investigação do incidente, nomeadamente a investigação forense.

Na primeira categoria temos então os diferentes equipamentos e tecnologias que a organização utiliza, com o objetivo de proteger a informação e as comunicações, adotando estratégias de defesa em profundidade que passam também por estabelecer perímetros de segurança lógicos e físicos, segmentando a infraestrutura da informação em níveis de grau de segurança distintos. Para obter este efeito utilizam-se equipamentos de proteção do tipo *firewall* para controlar e filtrar o acesso aos fluxos de informação entre os diferentes níveis. A comunicação entre níveis é inevitável, bem como a disponibilização e o acesso de serviços de e para o exterior da organização, utilizando-se tecnologias que permitem a autenticação dos utilizadores, que definem diferentes graus de autorização, bem como o registo de toda a atividade realizada. Outra ferramenta que é indispensável na estrutura de segurança da organização, são os equipamentos de inspeção e prevenção do tipo IPS[6] que analisam todo o tráfego dados que circulam na rede, detetando padrões de comportamento potencialmente perigosos, podendo agir preventivamente através do bloqueio automático dessas comunicações. Consideramos ainda nesta categoria as tecnologias de anti *malware* como sejam os programas de antivírus de gestão centralizada ou as plataformas de proteção de correio eletrónico. A utilização destas ferramentas permite ter um conhecimento situacional do ciberespaço da organização, através da análise da informação disponibilizada através dos vários registos de atividade (*logs*) ou dos quadros informativos que disponibilizam.

O conjunto de equipamentos e tecnologias que protegem a informação da organização, abordados no parágrafo anterior, geram eventos de informação em tal quantidade que numa organização de média dimensão (cerca de 8000 utilizadores) pode chegar facilmente aos 1000 eventos por segundo, tornando impossível um tratamento eficaz da informação recebida, que permita realmente saber o que está a

[5] Por informação em bruto entendemos a informação tal como é gerada pelos equipamentos de segurança, ou seja, não foi alvo de qualquer tratamento prévio, servindo como exemplo os registos de atividade, de comunicações ou processamento de informação, normalmente designados por *logs*.
[6] IPS - Intrusion Prevention System

acontecer na infraestrutura de informação e comunicações da organização. Para solucionar estes problemas são utilizados os equipamentos da segunda categoria indicada anteriormente. As tecnologias de *Security Information and Events Management* (SIEM) permitem agregar toda a informação gerada nas várias plataformas de segurança, correlacioná-las entre si e com outras fontes de informação externa, como a análise de vulnerabilidades ou informações de inteligência.[7] Assim, os milhares de eventos são transformados em algumas poucas dezenas de potenciais incidentes. Caberá à equipa de resposta a incidentes analisá-los, classificá-los e reagir no caso de estarmos perante um verdadeiro incidente. Os equipamentos que implementam esta tecnologia têm também a capacidade de armazenar os vários registos que recebem, no seu formato original, servindo como fonte de evidências com valor legal, no caso de uma investigação para apuramento de responsabilidades.

A categoria de tecnologias que permitem fazer uma efetiva gestão do incidente está relacionada com a necessidade de existir uma plataforma única que permita seguir o incidente ao longo de todos o seu ciclo de vida, registando todas as ações com este relacionada, desde o relato dos eventos, as ações de triagem realizadas e que levaram à sua escalada para incidente. Nesta plataforma são igualmente registadas as várias ações e iterações efetuadas com vista à resolução do incidente pelos técnicos intervenientes no processo e finalmente as recomendações ou lições aprendidas. Toda esta informação é assim registada numa plataforma associada a uma base de dados, com um interface que permite registar todas as ações relativas à gestão do incidente[8]. Algumas plataformas deste tipo têm também associado um sistema de seguimento das várias ações realizadas, por quem as realizou, disponibilizando ainda um conjunto de ferramentas básicas de apoio à gestão do próprio incidente.[9]

Na última categoria consideramos os equipamentos ou tecnologias utilizados para a análise dos dados e informações disponíveis, com vista à investigação das causas e os efeitos, provocados pelo incidente. Para identificar todos os acontecimentos

[7] Estas informações de inteligência, conhecidas por Cyberfeeds, são informações recolhidas e divulgadas em tempo quase real sobre eventos de segurança, recolhidos em todo o mundo e pre-processados para as organizações subscritoras destes serviços [16].

[8] Devido à potencial importância da informação recolhida, relevamos a necessidade de existirem mecanismos de salvaguarda da informação armazenada, recorrendo a tecnologias de *backup* e a procedimentos de *disaster recovery*, que deverão ser testados periodicamente.

[9] O *Request Tracker for Incident Response* (RTIR) é uma das plataformas mais populares de gestão de incidentes, possuindo um sistema de seguimento das ações realizadas e por quem (*tickting)*, apresentando um *workflow* próprio para apoio à gestão de incidentes [17].

relacionados com um incidente, é necessário utilizar tecnologias que permitam capturar e analisar pacotes de dados, analisar as configurações base dos sistemas de informação, bem como detetar as alterações introduzidas nos sistemas de ficheiros ou nos registos de configuração dos sistemas operativos, no decorrer do incidente. As plataformas que implementam estas tecnologias têm de estar preparadas para lidar com enormes quantidades de dados, em diversos formatos, e ainda de recolher evidências sem introduzirem qualquer alteração à informação original, para não comprometer a utilização da informação recolhida, no âmbito de uma possível investigação legal.[10]Este material deve estar disponível no local principal de trabalho da equipa de resposta a incidentes, no entanto deve também de existir sob a forma de *Kit* de investigação forense, que seja transportável, para permitir a mobilidade dos técnicos da equipa, mantendo toda a sua operacionalidade ou seja, a capacidade de recolher e investigar evidências.[11]

## LIDERANÇA

Na edificação de qualquer capacidade, o fator Liderança apresenta-se sempre como um fator muito importante. No caso da Capacidade de Resposta a Incidentes de Segurança da Informação, existe como fator determinante a abrangência da ação da equipa de resposta, e o impacto das suas ações de forma transversal em toda a organização. Assim, é muito importante que a implementação desta capacidade tenha o apoio inequívoco dos líderes da própria organização. Por outro lado, esta é uma capacidade que está associada a uma forte componente tecnológica, como tal é fundamental a preparação das chefias das equipas para uma abordagem profissional das operações, ou seja, ao desenvolvimento da competência profissional para comandar, dirigindo e motivando os membros da equipa, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão. Nesta perspetiva, o líder da equipa é visto mais como um decisor que tem de possuir um conhecimento holístico da estrutura da organização e dos seus sistemas. A tomada de decisão ocorre

[10] O *Forensic ToolKit* (FTK) é uma das plataformas mais completas, incluindo funções muito variadas para a investigação forense, como por exemplo a recolha e análise do conteúdo de memória RAM, suporta a análise de todos os sistemas de ficheiros mais importantes, ferramentas de apoio à desencriptação de informação, cópia integral de discos entre outras [18].

[11] Devido à importância destas ferramentas para o sucesso da investigação, consideramos de particular importância mantê-las sempre atualizadas, quer do ponto de vista de segurança (eg atualizações do fabricante), quer do ponto de vista tecnológico.

muitas vezes em plena ação e desenvolvimento dos acontecimentos, sendo assim importante que o líder esteja preparado para lidar com a gestão de crises no seu ciberespaço organizacional, que conheça os fatores que afetam e irão ser afetados pela sua decisão, de maneira a que o habilite a tomar decisões prontas e fundamentadas. No apoio ao líder podem existir sistemas de apoio à decisão baseados em multicritérios que não serão abordados no âmbito deste trabalho.

Outro ponto que assume especial importância, na gestão da capacidade de resposta a incidentes de segurança, está relacionado com o posicionamento do líder e da sua equipa, na estrutura hierárquica da organização. Devido à abrangência das ações a realizar no âmbito da auditoria aos sistemas e análise de vulnerabilidades, transversal aos vários departamentos, parece-nos particularmente importante assegurar na estrutura da organização, a total separação entre a equipa responsável pela gestão de incidentes e as equipas responsáveis pela administração e configuração dos sistemas de segurança e de suporte aos serviços. Esta separação evita situações de conflito de interesse entre os membros das duas equipas e evita situações de "promiscuidade" técnica, como por exemplo o de um técnico ter de avaliar a vulnerabilidade de um sistema por si configurado. Finalmente, as ações e as recomendações relativas à segurança da informação, resultantes da análise de vulnerabilidades, da avaliação do risco e das lições aprendidas, devem ter um peso institucional elevado, devendo por isso o líder e a sua equipa estarem posicionados na dependência direta da Direção da organização.

## PESSOAL

Numa capacidade de resposta a incidentes de segurança, mesmo existindo todo o material necessário para a sua operacionalização, o Pessoal ou fator humano é determinante, pois tem sempre de existir uma fase muito importante de análise e decisão das ações a seguir. A organização deve disponibilizar os elementos mais capazes para o desempenho das tarefas a realizar, garantindo que estes são possuidores das qualificações técnicas necessárias para o desempenho da missão. Neste sentido é particularmente importante definir os diferentes papeis que cada membro da equipa terá de desempenhar, aprovar o percurso de formação necessário para o desempenho dessas funções e selecionar os elementos. Nas organizações em que existe implementado o conceito de rotatividade de pessoal, é importante garantir a

estabilidade dentro das equipas de resposta a incidentes, devido à especificidade das suas ações e da sua formação técnica.

O número e a especialização dos elementos da equipa está obviamente dependente, da estrutura definida para a capacidade que a organização pretende implementar. Uma estrutura exclusivamente interna à organização, com uma configuração centralizada, terá necessidades de pessoal diferentes, de outra de configuração distribuída ou então apoiada por entidades externas.[12]

Tomando como exemplo uma estrutura de resposta a incidentes interna à organização e centralizada, que será a que melhor se adapta à organização fortemente hierarquizada e centralizada da infraestrutura de Tecnologias da Informação e Comunicações (TIC) da Marinha Portuguesa, segundo *Killcrece et al* [19] a estrutura deverá ser composta por um gestor (garantindo um elemento alternativo para assumir as suas funções), um elemento administrativo e a equipa técnica com formação que lhe permita assegurar os serviços a que a equipa tem de responder, em numero suficiente para garantir a operacionalidade desejável de 24x7x365. São ainda apresentados exemplos de outros papéis a serem preenchidos como o de apoio jurídico, o de investigador ou de relações públicas que por não terem caracter permanente não são considerados como responsabilidade direta da equipa.

*Killcrece et al* [20] identifica como principais fatores para o pessoal, a variedade de competências. As equipas de maior sucesso caracterizam-se por serem dedicadas, inovadoras, flexíveis, analíticas, orientadas para a solução, bons comunicadores e capazes de trabalhar em situações de *stress*. *Killcrece* destaca ainda competências técnicas necessárias, ao nível de experiência na administração de redes e de sistemas, experiência em diferentes sistemas operativos, compreensão básica de protocolos de *Internet* e conhecimento básico sobre os ataques mais comuns a computadores e sobre vulnerabilidades. Na área mais específica da segurança, indica como fatores importantes, a experiência na gestão de incidentes e a capacidade de resolver os problemas.

[12] A universidade de Carnegie Mellon apresenta cinco modelos de organização diferentes para as equipas de resposta a incidentes de segurança, o modelo "equipa de segurança", o modelo interno distribuído, o interno centralizado, um modelo interno misto centralizado e distribuído, modelo coordenador [19].

## INFRAESTRUTURAS

Uma capacidade de resposta a incidentes de segurança da informação não é muito exigente ao nível das Infraestruturas requeridas. Atendendo a que a informação a proteger tem diferentes níveis de segurança, que implicam muitas vezes a segregação física ao nível da própria infraestrutura, é essencial que essa segregação se estenda até ao local onde a equipa de resposta a incidentes monitoriza e analisa os diversos eventos, bem como ao armazenamento da informação relativa aos incidentes de segurança. Assim, nesta dimensão consideramos como fator mais importante, a segurança física das instalações. O edifício onde está operar a equipa de resposta a incidentes, para além da necessária proteção elétrica que permita manter a operar os seus sistemas, mesmo em caso de corte de energia[13], e das condições ambientais, terá também de possuir comunicações redundantes, áreas de segurança para a operação dos sistemas, com os devidos mecanismos de controlo de acessos e de videovigilância.

## INTEROPERABILIDADE

A Interoperabilidade é fundamental no processo de responder aos incidentes de segurança da informação de modo eficaz e eficiente, de forma a não só resolver o incidente e recuperar a operacionalidade, mas também a mitigação das vulnerabilidades. É um processo complexo que muitas vezes envolve não só a própria organização mas também entidades externas, sejam elas prestadoras de serviços de comunicações, serviços de internet, ou mesmo entidades congéneres. Estas entidades externas naturalmente terão os seus processos próprios de operação, com procedimentos e taxonomias diversas das nossas. As ameaças cibernéticas à segurança da informação são globais e na maioria das vezes afetam todas as organizações, independentemente da sua natureza ou área de negócio. O estabelecimento de relações de confiança entre as várias entidades responsáveis por assegurar a resposta a incidentes de segurança, permite a partilha de informação e mesmo de apoio mútuo, na resolução de incidentes de natureza global, permitindo assim um conhecimento situacional do ciberespaço que vai para além do da própria organização. Para que estas partilhas de informação sejam possíveis, é necessário

[13] O edifício deverá apresentar duas linhas principais de energia elétrica, uma associada a sistemas de proteção do tipo U*ninterrupted Power Supply* (UPS), ao qual se associaram todos os sistemas críticos para a operação, e outra associada a um sistema de mecânico de geração de energia.

estabelecerem-se não só as já referidas relações de confiança mas também mecanismos que permitam a comunicação clara, com procedimentos e taxonomias comuns.[14]

## 4.CONCLUSÃO

A análise que realizámos das diferentes dimensões DOTMLPI-I com base os conceitos relacionados com a implementação de uma capacidade operacional de resposta incidentes no âmbito da Cibersegurança permitiu identificar alguns dos aspetos essenciais à implementação de uma capacidade desta natureza. Da Doutrina é relevada a importância de estarem definidos os princípios legislativos, que irão enquadrar a ação da equipa de resposta a incidentes relativamente aos seus objetivos e o âmbito da sua ação. A Organização é muito importante nomeadamente na articulação e comunicação da capacidade dentro da própria organização. Do Treino sobressai como mais importante a realização de exercícios à escala nacional e internacional que permitam testar e desenvolver competências ao nível da capacidade de decisão, coordenação, partilha de informação e capacidades técnicas. O Material na capacidade de resposta a incidentes assume relevância no sentido que devem de existir os meios necessários que permitam a monitorização do ciberespaço com mecanismos de deteção e registos de eventos, que eventualmente escalarão para incidentes, assegurando os meios para os acompanhar ao longo do seu ciclo de vida. Da Liderança destaca-se a importância de os níveis superiores de chefia da organização estarem envolvidos em todo o processo de edificação da capacidade, apoiando o seu desenvolvimento, motivados pela sua necessidade operacional, dotando-a dos recursos humanos e materiais necessários. Para que esta capacidade seja efetiva, os recursos ao nível do Pessoal devem possuir a formação e o treino que permitam alcançar com sucesso os objetivos elencados na Doutrina, sendo muito importante conseguir garantir a estabilidade das equipas. A Interoperabilidade assume-se como vital na construção da Capacidade de Resposta a Incidentes de

[14] Como exemplo do esforço de criação de uma verdadeira interoperabilidade a nível nacional, temos o exemplo da Rede Nacional de CSIRT que possui mais de vinte membros efetivos, abrangendo um vasto leque de entidades, que inclui o Centro Nacional de Cibersegurança, as Forças Armadas, vários operadores públicos de telecomunicações, Bancos e instituições universitárias. A Rede assume-se como "fórum de cooperação entre equipas de resposta a incidentes de segurança informática (CSIRT)" tendo acordado entre os seus membros os "termos de referência" que permitirão garantir as condições para uma verdadeira Interoperabilidade [21].

Segurança. A complexidade de muitos dos ataques cibernéticos faz com que apenas uma ação concertada de várias entidades permita a sua mitigação. Por outro lado, a partilha de informação e conhecimentos é determinante na construção de um conhecimento situacional do Ciberespaço. A verdadeira Interoperabilidade apenas se concretiza se estiverem considerados dois elementos chave: a existência de relações sólidas de confiança entre os diversos atores que contribuem para a Cibersegurança e os mecanismos de comunicação compatíveis (plataforma de comunicação segura, taxonomia, comum, entre outros).

A metodologia DOTMLPI-I, desenvolvida para a identificação dos elementos críticos de uma capacidade operacional de natureza militar, mostra-se assim igualmente eficaz quando aplicada à Cibersegurança, nomeadamente na edificação de uma resposta a incidentes de segurança da informação.

## REFERÊNCIAS


[1] NATO. (2014). NATO Cyber Defence Taxonomy and Definitions. Norfolk: Consultation, Command and Control Board (C3B).

[2] Bravo, R. & Matias, A. (18 de 10 de 2014). Geopolítica, geoestratégia e ciberespaço: Notas introdutórias. Obtido de academia.edu: http://www.academia.edu/ 5543845/Geopolitica_geoestrategia_e_ciberespaco Notas_introdutorias.

[3] IDN, I. d. (2013). Estratégia da Informação e Segurança no Ciberespaço. Obtido de idn.gov.pt: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

[4] EC, E. C. (2013). Cybersecurity Strategy of European Union: An Open, Safe and Secure Cyberspace. Bruxelas.

[5] DR, D. d. (2014). Instalação do Centro Nacional Cibersegurança, DR, 1.ª série - N.º 89 - 9 de maio de 2014. Lisboa: Assembleia da República.

[6] DR, D. d. (2015). Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015. Lisboa: Assembleia da República.

[7] ACQuipedia. (30 de junho de 2005). DOTMLPF.P Analysis. Obtido em 29 de outubro de 2014, de ACQuipedia: https://dap.dau.mil/acquipedia/Pages/ ArticleDetails.aspx?aid= d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2.

[8] DoD, D. o. (2013). Guidance for development and implementation of joint concepts. Chairman of the Joint Chiefs of Staff.

[9] NATO. (2010). NATO Concept Development and Experimentation (CD&E) Process MCM-0056/2010. NATO.

[10] NATO. (2009). Policy for NATO concept development and experimentation MC 0583. NATO.

[11] E-Maps. (22 de agosto de 2013). DOTMLPF-P. Obtido em 03 de novembro de 2014, de e-mapsys: http://www.e-mapsys.com/ DOTMLPFP(3).pdf.

[12] Bergamini, C. (maio/junho de 1994). Liderança: A administração do sentido. Revista de Administração de Empresas, pp. 102-114.

[13] NATO. (2014). AAP-6 NATO Glossary of Terms and Definitions. NATO.

[14] DR, D. d. (2009). Lei do Cibercrime, Lei nº 109/2009 de 15 de Setembro. Lisboa: Assembleia da República.

[15] NATO. (2014). Cyber Coalition CC14 Training Objectives. NCIA.

[16] Anubisnetworks. (2015). Cyberfeed. Obtido em 17 de janeiro de 2015, de anubisnetworks.com: https://www.anubisnetworks.com/products/threat-

intelligence/cyberfeed.

[17] JANET. (s.d.). RTIR incident handling work-flow. Obtido em 17 de janeiro de 2015, de bestpractical.com: https://www.bestpractical.com/static/rtir/janet-workflow.pdf.

[18] Accessdata. (2015). Forensic Tool Kit. Obtido em 17 de janeiro de 2015, de accessdata.com: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk.

[19] Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). Pittsburg: Carnegie Mellon.

[20] Killcrece, G., & Ruefle, R. (2008). Creating and Managing Computer Incident Response Capability (CSIRTs). Pittsburg: Carnegie Mellon University.

[21] RCTS. (2015). Serviço de Resposta a Incidentes de Segurança da RCTS - objetivos. Obtido em 18 de janeiro de 2015, de cert.rcts.pt: http://www.cert.rcts.pt/ index.php/rede-nacional-csirt/objectivos.

CYBERLAW by CIJIC

# CONSTITUIÇÃO E CIBERESPAÇO: ARGUMENTOS PARA UM *"DIREITO CONSTITUCIONAL DO INIMIGO"?*

# *CONSTITUTION AND CYBERSPACE: ARGUMENTS FOR A "CONSTITUTIONAL LAW OF THE ENEMY"?*

**RAQUEL A. BRIZÍDA CASTRO** [1]

[1] Doutora em Direito, Ciências Jurídico-políticas, na Faculdade de Direito da Universidade de Lisboa; Professora Auxiliar na Faculdade de Direito da Universidade de Lisboa; Investigadora do Centro de Investigação em Direito Público do Instituto de Ciências Jurídico-políticas da Faculdade de Direito de Lisboa; Membro da Comissão para a Doutrina do Cibersegurança, junto da Autoridade Nacional de Segurança; Vogal do Conselho Regulador da Entidade Reguladora para a Comunicação Social (ERC). Correio eletrónico: Raquelcastro@fd.ul.pt

**SUMÁRIO:** *INTRODUÇÃO; PARTE I. REFLEXÕES PARA UMA INTERPRETAÇÃO CONSTITUCIONAL TECNOLOGICAMENTE NEUTRA; 1. CONSTITUIÇÃO E CIBERESPAÇO: "CONTRADICTIO IN TERMINIS"?; 2. DA EXACERBAÇÃO DAS CONDIÇÕES DA CONCRETIZAÇÃO CONSTITUCIONAL: A PRÉ-COMPREENSÃO DO INTÉRPRETE ENTRE O ESPARTILHO TEXTUAL E A SUBVERSÃO DO PROGRAMA NORMATIVO-CONSTITUCIONAL; 3. DO IMPACTO DOS FACTOS DAS NOVAS TECNOLOGIAS NO DOMÍNIO NORMATIVO E VERTENTE DINÂMICA DA INTERPRETAÇÃO CONSTITUCIONAL; 4. DA INSUBSTITUIBILIDADE DO PAPEL DA JUSTIÇA CONSTITUCIONAL NO CONTROLO DE CONSTITUCIONALIDADE DA REGULAÇÃO DO CIBERESPAÇO: PARTE II. CONSTITUIÇÃO E REGULAÇÃO DO CIBERESPAÇO; 5. DA RELEVÂNCIA CONSTITUCIONAL DO IMPACTO EFETIVAMENTE RESTRITIVO DAS NOVAS TECNOLOGIAS NO PERÍMETRO PROTETIVO DOS DIREITOS CONSTITUCIONALMENTE PROTEGIDOS; 6. INFRAESTRUTURAS CRÍTICAS, DEVER DE REPORTE E AS OMISSÕES JURÍDICO-CONSTITUCIONALMENTE RELEVANTES NA ESTRATÉGIA DA SEGURANÇA NO CIBERESPAÇO; 7. A INDEFINIÇÃO REGULATÓRIA DO CIBERESPAÇO NÃO LEGITIMA NEM CARECE DE UM "DIREITO CONSTITUCIONAL DO INIMIGO"*

## RESUMO

Os novos problemas do ciberespaço têm impacto na interpretação constitucional e na justiça constitucional. O eventual excesso de interpretativismo pode resultar da exacerbação das condições de concretização, através da sobrevalorização do impacto dos dados reais e do problema concreto a resolver, no domínio normativo. Uma interpretação tecnologicamente neutra que deve garantir a tradução dos valores constitucionais positivados, explícita ou implicitamente, nas normas constitucionais, para a atual realidade tecnológica, salvando a identidade constitucional, no limite do texto constitucional. Perante um domínio normativo onde o ritmo de intervenção legislativa e correspetiva densidade são, particularmente, problemáticos, torna-se crucial garantir que o expetável incremento de ativismo judicial, designadamente através da criação de normas *"ad casum",* possa ser sujeito ao escrutínio da justiça constitucional. Os novos desafios reclamam uma refundação regulatória, focada na atividade efetivamente desenvolvida e no impacto efetivo das intervenções restritivas. A atual indefinição regulatória do ciberespaço não legitima estados de exceção constitucional, não previstos, ou um *"Direito Constitucional do Inimigo".*



**Palavras-Chave:** Regulação Constitucional do Ciberespaço; Interpretação Constitucional Tecnologicamente Neutra; Justiça Constitucional; Modelos Regulatórios; "Direito Constitucional do Inimigo"

## ABSTRACT

*Issues newly raised by cyberspace have an impact on constitutional justice and interpretation. At one normative level, one possible interpretativism surplus may result from one exaggeration of the legal conditions fulfillment - through overvaluing the impact of concrete data and the specific problem to solve. One technologically neutral constitutional interpretation for the current technological reality should ensure the consecration of positivized constitutional values - explicitly or implicitly - in the constitutional provisions, saving the constitutional identity on the constitutional text limit. It is then critical to ensure that the expected increase of judicially activism - inter alia, by setting "ad casum" norms - may be subjected to the scrutiny of constitutional justice, given this regulatory domain where the pace of legislative intervention and its consequent legal density are particularly problematic. These new cyberspace challenges call for a refoundation of the regulatory framework focused on the activity actually developed and on the concrete impact of restrictive interventions. The present indefinition of the regulatory framework of cyberspace cannot justify constitutional states of emergency, unforeseen, or even a "Constitutional Law of the Enemy.".*

**Keywords:** *Constitutional Cyberspace regulation; Technologically Neutral Constitutional interpretation; Constitutional justice; Regulatory models; "Constitutional Law of the Enemy"*

## INTRODUÇÃO

Perante as novas tecnologias, apenas uma interpretação constitucional tecnologicamente neutra[1] pode garantir que as regras e os princípios estruturantes, os valores vertidos nas disposições constitucionais, as categorias e institutos jurídico-constitucionais aplicáveis, mantêm toda a sua efetividade. Não obstante, a relevância da dogmatização de uma interpretação constitucional tecnologicamente neutra pressupõe o reconhecimento prévio do impacto específico dos factos tecnológicos e dos seus problemas concretos na interpretação constitucional e na Justiça Constitucional. Este constituirá o desiderato da primeira parte (I) da presente reflexão.

Na segunda parte (II), procuraremos, a partir de pistas recentes, demonstrar a dificuldade de categorização prévia de modelos regulatórios aplicáveis ao ciberespaço e problematizar, para efeitos de delimitação do perímetro protetivo dos direitos e liberdades, a relevância da atividade efetivamente desenvolvida e do impacto efetivo dessa intervenção restritiva. No desfecho da reflexão, respigando o argumentário expendido ao longo do artigo, procuraremos ser incisivos na conclusão de que os eventuais ciberdesafios não podem legitimar uma interpretação constitucional amiga de um *Direito Constitucional do Inimigo*[2].

[1] O conceito de interpretação constitucional tecnologicamente neutra foi, por nós, dogmatizado, na nossa Dissertação de Doutoramento. V*ide* - CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 91 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 84 e segs.

[2] Inspiramo-nos no conceito de *"Direito Penal do Inimigo"*, dogmatizado por JAKOBS, adaptando-o aos novos desafios constitucionais, gerados pelo Ciberespaço. – JAKOBS, Günther/MELIÁ, Manuel Cancio (2003) *Derecho penal del Enemigo*, Civitas, Madrid.

## *PARTE I - Algumas Reflexões para uma Interpretação Constitucional Tecnologicamente Neutra*

Uma interpretação constitucional tecnologicamente neutra requer um ajustamento às novas questões suscitadas pelas novas tecnologias[3]. Apesar de alguma doutrina questionar, em termos gerais, as estruturas tradicionais do direito público[4], uma análise perfunctória do Direito Constitucional do ciberespaço[5] leva-nos a sufragar as teses, segundo as quais, a sua constitucionalização é não apenas uma possibilidade, mas desde logo uma necessidade[6]. O ciberespaço não pode ser um espaço livre de direito, ainda que integrado numa sociedade da informação, global ou transnacional[7], não obstante a consciência de que a sua constitucionalização[8] é uma tarefa do futuro[9]. A Constituição não deve ser acolhida, apenas, como ditadora de limites, numa dimensão puramente negativa, como deve ver reforçada a sua vertente positiva, esperando-se que ela participe no desenho de uma opção de fundo da ordem normativa, expressa no catálogo dos direitos fundamentais. Daí a necessidade, pertinência e oportunidade de elaboração de uma Carta de Direitos para a Internet *("Bill of Rights").*

---

[3] Sobre o direito de acesso *à internet*, como um direito fundamental, mesmo oponível ao Estado – SEGURA-SERRANO, Antonio (2006) "*Internet* Regulation and the role of International Law", *in Max Planck UNYB*, 10; p. 265.

[4] Para TRACHTMAN, o ciberespaço não vai destruir o Estado, podendo tanto fortalecê-lo como enfraquece-lo. Exige, porém, uma revisão dos conceitos de jurisdição e de soberania. - TRACHTMAN, Joel (1998) "Cyberspace, Sovereignity, Jurisdiction and Modernism*", in Indiana Journal of Global Legal Studies:* Vol. 5, Issue 2, Article 10; pp. 561 e segs.

[5] Conforme nota WÜRTENBERGER, as duas últimas décadas estão marcadas por duas revoluções silenciosas: a revolução técnica da *internet* e a revolução do conhecimento na sociedade de informação. - WÜRTENBERGER, Thomas (2008) "La Transformación del Derecho en la Sociedade de la Información", *in Dignidad de La Persona, Derechos Fundamentales, Justicia Constitucional*, Coord. Francisco Fernández Segado, Dykinson-Constitucional; p. 1041.

[6] PEREIRA, Alexandre Libório Dias (2012), "Direito Ciberespacial: "*soft law*" ou "*hard law*"? *in Estudos em Homenagem ao Professor Doutor José Joaquim Gomes Canotilho*, BFDC, Coimbra Editora: Coimbra; p. 695.

[7] WÜRTENBERGER, Thomas (2008) "La Transformatióm del Derecho en la Sociedade de la Información", *in Dignidad de La Persona, Derechos Fundamentales, Justicia Constitucional*, Coord. Francisco Fernández Segado, Dykinson-Constitucional; p. 1060.

[8] Sobre o Transconstitucionalismo nas suas múltiplas vertentes. – NEVES, Marcelo (2012) "Transconstitucionalismo: breves considerações com especial referência à experiência latino-americana", *in Estudos em Homenagem ao Professor Doutor José Joaquim Gomes Canotilho, Vol. III*, Coimbra Editora: Coimbra; pp.615-652.

[9] WÜRTENBERGER, Thomas (2008) "La Transformatióm del Derecho en la Sociedade de la Información", *in Dignidad de La Persona, Derechos Fundamentales, Justicia Constitucional*, Coord. Francisco Fernández Segado, Dykinson-Constitucional; p. 1059.

## 1.CONSTITUIÇÃO E CIBERESPAÇO: "CONTRADICTIO IN TERMINIS"?

1.1.Problemático é, não obstante, o conceito de Constituição para a doutrina constitucional do ciberespaço, teoricamente mais próximo de um sistema de *common law*[10], baseado em precedentes e no costume, do que num ordenamento jurídico-constitucional como o português, fundado numa Lei Fundamental hiper-rígida[11], dotada de limites formais, temporais, circunstanciais e materiais de revisão constitucional. Mesmo a própria Constituição dos EUA,*"subsidiariamente consuetudinária e predominantemente instrumental"* [12], os princípios e regras costumeiras, nela integrados, *"não têm o mesmo peso dos costumes constitucionais britânicos, convertidos em "Common Law" mediante decisão dos tribunais superiores*"[13]. Será então o conceito de Constituição rígida, em sentido instrumental, compatível com o ciberespaço? Ou terá de render-se à provisoriedade do *living Constitutionalism*[14]? A eventual contradição nos termos, sublinhada no presente título, surge agravada com a afirmação dogmática da existência de uma relação determinista entre os conceitos de Constituição e de Estado: *"onde houver Constituição existirá Estado",* ou, menos restritivamente, *"onde houver Estado de Direito haverá Constituição*"[15], aparentando ser uma questão de poder constituinte, nas suas *"intermitentes revelações atípicas e difusas, sem povo e sem vontade*

[10] LESSIG sustenta que: "*if we understand a Constitution as a set of relatively unplastic constraints – understandings or ways of living, practices or inbuilt institutions – then cyberspace has a Constitution"*. Trata-se, para o autor de uma espécie de Constituição não escrita, uma *"architecture"* e uma *"architecture that regulates*". – LESSIG, Lawrence (2000) "Cyberspace's Constitution, Draft 1.1.", *Lecture given at the American Academy*, Berlin: Germany; pp. 1-3; No mesmo sentido, PERRIT Jr. sustenta que a Constituição da *internet* não existe de um ponto de vista instrumental, como a Constituição britânica. – PERRIT Jr., Henri H. (2012) "The *Internet* at 20: Evolution of a Constitution for Cyberspace", *in William &Mary Bill of Rights Journal*, Vol. 20:000; p.2.

[11] MORAIS, Carlos Blanco (2006) Justiça Constitucional, Tomo I, 2.ª Edição, Coimbra Editora: Coimbra; pp. 59 e segs..

[12] MORAIS, Carlos (2014) *Curso de Direito Constitucional, Tomo II*, Coimbra Editora: Coimbra; p. 46.

[13] Como ensina Blanco de MORAIS, *"a "Common Law" norte-americana é distinta da britânica e não se afirma como uma fonte própria de Direito Constitucional, pois os tribunais só podem criar direito, por via interpretativa, a partir da Constituição escrita".* - MORAIS, Carlos (2014) *Curso de Direito Constitucional, Tomo II*, Coimbra Editora: Coimbra; p. 93.

[14] Conforme já vimos, segundo STRAUSS, uma Constituição baseada na *"common law"* é um *"Living Constitution",* mas que também que pode proteger princípios fundamentais, apesar da transitoriedade da opinião pública. – STRAUSS, David (2010) "The *Living Constitution*", *in Oxford University Press*; p. 3.

[15] MORAIS, Carlos (2014) *Curso de Direito Constitucional, Tomo II*, Coimbra Editora: Coimbra; p. 303.

*democrática legitimadora*"[16]. Não obstante, se as questões do ciberespaço integram hoje a rotina dos cidadãos, os valores a proteger deverão ser decantados do núcleo identitário constitucional.

A erosão dos conceitos tradicionais do Direito Público pelas questões emergentes do ciberespaço é uma questão emergente e, embora, recorrente, localiza-se ainda na pré-história da sua dogmatização científica. Sem prescindir de um aprofundamento futuro, não pretendemos, porém, no presente artigo, trilhar um caminho sem saída. Diremos, fundados em evidências empírico-científicas, que o mais provável é que o conceito de Constituição, tal como o conhecemos, seja mesmo incompatível com o ciberespaço, porquanto o mesmo pressupõe a existência de um Estado, conforme a doutrina do direito público sempre vaticinou. Logicamente, nenhum Estado pode reclamar a sua soberania perante um recurso global que é a *internet*, ou o espaço comum do ciberespaço. O reconhecimento da dificuldade, ou mesmo impossibilidade, do sonho de um Tratado global, conforme aos parâmetros tradicionais, não é, todavia, o fim do mundo nem da Constituição.

1.2. Numa perspetiva jusinternacional, alguns autores propõem, o que consideram ser, uma alternativa mais realista, focada na elaboração de um conjunto de "*cyber-confidence measures*"[17], baseadas na proteção da confiança de que os Estados irão agir e adotar normas num determinado sentido[18]. Entre outros, cabe destacar que é com base, precisamente, no princípio da soberania territorial que se admite que um Estado possa regular, para o seu território, as suas próprias atividades da *internet* ou aquelas que os estrangeiros possam desenvolver nos seus países, mas que tenham efeitos no seu território [19] [20]. Efetivamente, como alguns autores já notaram, a

[16] MORAIS, Carlos (2014) *Curso de Direito Constitucional, Tomo II*, Coimbra Editora: Coimbra; p. 266.
[17] *Confidence Building Measures for Cyberspace – Legal Implications* (2013), CCDCOE – NATO Cooperative Cyber Defence Centre of Excelence, Tallinn.
[18] *Cyber-security: The Vexed Question for Global Rules. An Independent Report on Cyber-Preparedness around the World*, (2012) – SDA, Security And Defence Agenda. p.27.
[19] Do mesmo princípio decorre, nos termos do Direito Internacional, o dever de não causar danos aos direitos dos outros Estados. Acrescem o princípio da boa vizinhança e o princípio *sic utere tuo principle*, dos quais decorre que um Estado não pode danificar os componentes técnicos da *Internet*, localizados no território de outos estados, ou causar outros efeitos danosos à segurança nacional desses mesmos Estados. - *Confidence Building Measures for Cyberspace – Legal Implications* (2013), CCDCOE – NATO Cooperative Cyber Defence Centre of Excelence, Tallinn; p. 90.
[20] Com base nos princípios de não-agressão, boa vizinhança e *sic utere tuo principle*, os Estados têm a obrigação de prevenir ciberatividades maliciosas que possam afetar os direitos dos outros estados. Nesse sentido, devem garantir: i) A instalação de sensores nos ISPs nacionais que recolham informação no *"net flow"* (permitindo detetar ciberataques); ii) A instalação de sistemas de deteção e prevenção de intrusão nas suas portas de transmissão de dados internacionais, através de um filtro *deep package* (que

soberania é nuclear no conceito de Estado e, concomitantemente, um princípio axiomático onde se baseia o direito internacional. É então possível fazer derivar do princípio da igualdade dos Estados um conjunto de direitos e obrigações, bem como de princípios aplicáveis aos conflitos entre direitos soberanos na comunidade internacional[21]. Não pode ser esta uma alternativa pragmática ao caos? Da intimidade dos conceitos de Estado e Constituição resulta que as doutrinas conducentes ao fortalecimento dos Estados, neste domínio normativo, podem contribuir, lateralmente, para a revivescência da pujança constitucional na regulação das questões especialíssimas do ciberespaço, cada vez mais intrigantes. Estamos, não obstante, conscientes da sua teimosa insuficiência para uma resposta global.

## 2. DA EXACERBAÇÃO DAS CONDIÇÕES DA CONCRETIZAÇÃO CONSTITUCIONAL: A PRÉ-COMPREENSÃO DO INTÉRPRETE ENTRE O ESPARTILHO TEXTUAL E A SUBVERSÃO DO PROGRAMA NORMATIVO-CONSTITUCIONAL

2.1. Sendo a interpretação constitucional concretização[22], a interpretação assume caráter criativo: o conteúdo da norma interpretada só fica completo com a sua interpretação, ainda que a atividade interpretativa continue vinculada à norma. A concretização pressupõe a compreensão do conteúdo da norma[23], não podendo desligar-se nem da pré-compreensão do intérprete, em função da sua localização singular, nem do problema concreto a resolver, enquanto condições da interpretação[24].

---

permita o reconhecimento de *software* malicioso); iii) Um sistema de reporte a uma entidade governamental - CERT nacional ou governamental;

[21] *Confidence Building Measures for Cyberspace – Legal Implications* (2013), CCDCOE – NATO Cooperative Cyber Defence Centre of Excelence, Tallinn; p. 90.

[22] HESSE, Konrad (1991) "Concepto y Cualidad de la Constitución", *Escritos de Derecho Constitucional*, Fundación Coloquio Juridico Europeo, Centro de Estudios Politicos y Constitucionales: Madrid; p. 63.

[23] HESSE, Konrad (1991) "Concepto y Cualidad de la Constitución", *Escritos de Derecho Constitucional*, Fundación Coloquio Juridico Europeo, Centro de Estudios Politicos y Constitucionales: Madrid; pp. 33 – 57.

[24] HESSE, Konrad (1991) "Concepto y Cualidad de la Constitución", *Escritos de Derecho Constitucional*, Fundación Coloquio Juridico Europeo, Centro de Estudios Politicos y Constitucionales: Madrid; p. 65.

Na senda da hermenêutica filosófica, o que não é unívoco deve ser determinado mediante a inclusão da realidade a regular[25].

O sobredito modelo teórico hermenêutico evidencia, porém, a identificação possível de diferentes graus interpretativos, oscilantes entre a mera subsunção e a concretização, a que correspondem distintos níveis de complexidade, jurídica e fáctica[26]. Nos casos difíceis, é mesmo suscetível de remeter a atividade concretizadora para um campo de generosa criatividade jurídica, legitimando excessos de interpretativismo, eventualmente intoleráveis. Os exageros podem resultar de uma exacerbação das condições de concretização, através da sobrevalorização de uma pré-compreensão do intérprete, dissociada da norma e dos seus enunciados linguísticos, ou do impacto dos dados reais e do problema concreto a resolver. Note-se o especial peso do domínio normativo na interpretação constitucional, incontornável perante a voracidade dos factos técnicos e tecnológicos, eventualmente responsável por desvios interpretativos, na ausência de tempero, que apenas uma interpretação constitucional tecnologicamente neutra pode propiciar. Concretização *"não é uma apreensão pragmática de vários sentidos possíveis"*[27], seguida da seleção positiva do que for politicamente mais conveniente ou consensual, mas sim *"o trânsito do abstrato para o concreto"* [28], permitindo-se o desenvolvimento (atualização, evolução) do *"programa constitucional",* sem ultrapassar os limites de uma tarefa interpretativa[29].

---

[25] ALEXANDRINO, José Melo (2011), "Hermenêutica dos Direitos Humanos", *Texto revisto da conferência proferida no Curso "tutela de Direitos Humanos e Fundamentais",* organizado pela FDL. Disponível em: http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Alexandrino-Jose-de-Melo-Hermeneutica-dos-Direitos-Humanos.pdf; p. 9.

[26] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação), p. 58.

[27] MORAIS, Carlos Blanco de (1998) *As Leis Reforçadas. As Leis Reforçadas pelo Procedimento no Âmbito dos Critérios Estruturantes das Relações entre Atos Legislativos*, Coimbra Editora: Coimbra; p. 596.

[28] MORAIS, Carlos Blanco de (1998) *As Leis Reforçadas. As Leis Reforçadas pelo Procedimento no Âmbito dos Critérios Estruturantes das Relações entre Atos Legislativos*, Coimbra Editora: Coimbra; p. 597.

[29] *"Entre um objetivismo histórico, que conduza a uma absoluta rigidificação do texto constitucional, e um objetivismo atualista extremo, legitimador de uma estratégia política de subversão ou de transformação constitucional*", impõe-se a "*proibição de ruturas, mutações constitucionais silenciosas e de revisões apócrifas".* - CANOTILHO, J.J. Gomes (2003) *Direito Constitucional e Teoria da Constituição*, 6.ª Edição; pp. 1196. Sobre o tema das mutações – MORAIS, Carlos Blanco de (2013) "As Mutações Constitucionais implícitas e os seus limites jurídicos: autópsia de um Acórdão controverso*", Jurismat*; JELLINEK, Georg (1906) "Constitutional Amendment and Constitutional Transformation", *in Weimar: a Jurisprudence of Crisis*, coord. Arthur Jacobson and Bernard Schlink, translated by Belinda Cooperwith Peter C. Caldwell, Stephen Cloyd, David Dyzenhaus, Stephan Hemetsberger, Arthur J. Jacobson, and Bernhard Schlink, University of California Press, (2000); pp. 54 e segs.

2.2. No processo de concretização, ou vertente dinâmica da interpretação, cabe explicitar as premissas básicas da metódica estruturante, proposta por HESSE[30], fundadas na distinção prévia entre norma e enunciado (disposição), sendo esta uma formulação textual e a norma o sentido adscrito a qualquer disposição. Norma constitucional é um modelo de ordenação, juridicamente vinculante, positivado na Constituição, orientado para uma concretização material e constituído por: i) programa normativo – medida de ordenação expressa através de enunciados linguísticos; ii) domínio normativo – constelação de dados reais. Estando o programa normativo, essencialmente, contido no texto da norma, relevam os critérios de interpretação tradicionais para a sua compreensão. Caso se revelem insuficientes, cumpre indagar os *topoi* fornecidos pelo domínio normativo, ou seja, pela realidade da vida, objeto de ordenação.

Desse procedimento resultará a coordenação material entre os *topoi* que resultam do texto e programa normativo e os que derivam da observação dos âmbitos da realidade. Sem prescindir, o ponto de partida da interpretação não pode, todavia, deixar de ser as regras de interpretação tradicionais, uma vez que a apreensão da vontade constituinte não pode senão ser *"sujeita a uma objetivação, na base do seu teor literal e do seu contexto histórico, sistemático e teleológico*"[31]. Nem o resultado pode, nos casos mais problemáticos, deixar de ser modelado por uma interpretação tecnologicamente neutra, mediante a atribuição da relevância devida ao domínio normativo e aos factos tecnológicos, garantindo o desiderato da respetiva integração no ambiente constitucional do intérprete.

2.3. No que concerne à hiperbolização da pré-compreensão do intérprete constitucional, esses riscos espraiam-se por uma escala gradativa, inerente ao *iter* interpretativo, que começa no texto e se estende até à subversão do programa normativo-constitucional. Na senda da sugestiva lição norte-americana[32], a propósito

[30] CANOTILHO, J.J. Gomes (2003) Direito Constitucional e Teoria da Constituição, 6.ª Edição, p. 1202; ALEXANDRINO, José de Melo (2011) "Como ler a Constituição: algumas coordenadas", *in* José Melo Alexandrino, *Elementos de Direito Público Lusófono*, Coimbra Editora: Coimbra; p. 3.
[31] MORAIS, Carlos Blanco de (1998) *As Leis Reforçadas. As Leis Reforçadas pelo Procedimento no Âmbito dos Critérios Estruturantes das Relações entre Atos Legislativos*, Coimbra Editora: Coimbra; p. 596.
[32] ALEXANDRINO, José de Melo (2011) "Como ler a Constituição: algumas coordenadas", *in* José Melo Alexandrino, *Elementos de Direito Público Lusófono*, Coimbra Editora, Coimbra; p. 6.

de *"ways not to read the Constitution"*[33], cabe identificar dois tipos de resultados interpretativos indesejáveis: a *"des-integração"*, que constitui uma forma de interpretação que ignora o facto de as suas partes se encontrarem integradas num todo, tratando-se, efetivamente, de uma Constituição e não de simples conjuntos de cláusulas e preceitos separados, com histórias distintas; a *"hiperintegração"*[34], que consiste numa abordagem que ignora que o todo integra partes distintas, parcelas que foram introduzidas em momentos distintos da história constitucional, apoiadas e refutadas por diferentes grupos, refletindo posições diferentes e, nalguns casos, mesmo opostas[35].

A eventual sobrevalorização da pré-compreensão do intérprete [36] constitui, indubitavelmente, o principal risco de conceções suprapositivas do ordenamento jurídico [37], designadamente no contexto de uma leitura *hiperintegrada* da Constituição. Os preconceitos do intérprete contaminam o produto da interpretação constitucional, inflacionando as objeções conducentes à fragilização do papel do juiz constitucional[38]. Daí a importância de condicionar a atuação do intérprete, através do espartilho propiciado pela vinculação ao programa normativo, aliado à privação de relevância jurídica dos seus anteprojetos interpretativos, eventualmente arbitrários e desprovidos de base normativa. Em conformidade, rejeitamos expressões artificiais *hiperintegradoras*, como a hiperbolização pluralista *häberliana*[39], a diluição moral

[33] TRIBE/Lawrence H./DORF/ Michael C. (1991) *On Reading The Constitution*, Harvard University Press, p. 20; TRIBE, Lawrence H. (1986) "On Reading the Constitution", *The Tanner Lectures on Human Values*, Delivered at the University of Utah, November 17 and 18; pp. 19 e segs.

[34] "(…) *the fallacy of treating the Constitution as a kind of seamless web, a "brooding omnipresence" that speaks to us with a single, simple, sacred voice expressing a unitary vision of an ideal political society*". - TRIBE/Lawrence H./DORF/ Michael C. (1991) *On Reading The Constitution*, Harvard University Press; p. 24.

[35] TRIBE, Lawrence H. (1986) "On Reading the Constitution", *The Tanner Lectures on Human Values*, Delivered at the University of Utah, November 17 and 18; p. 20.

[36] Essa sobrevalorização equivale à superlativização dos fatores principológicos e axiológicos que são, na opinião de Blanco de MORAIS, *"fator de inversão do sentido normativo, de fratura do império da lei, de depreciação do modelo democrático e do seu modelo representativo, bem como de insegurança jurídica*". – MORAIS, Carlos Blanco de (1998) *As Leis Reforçadas. As Leis Reforçadas pelo Procedimento no Âmbito dos Critérios Estruturantes das Relações entre Atos Legislativos*, Coimbra Editora: Coimbra; p. 595.

[37] MORAIS, Carlos Blanco de (2012) *Curso de Direito Constitucional, Tomo I, 2.ª Ed.*, Coimbra Editora: Coimbra; pp. 143 a 149 e 172 a 182.

[38] SANCHIS, Luis Prieto (2000) "Tribunal Constitucional y Positivismo Jurídico", *in DOXA*, n.º 23; p. 162.

[39] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 67 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 60 e segs.

*Dworkiniana*[40], ou as teses refundadoras de uma rematerialização e revolução constitucionais, a nosso ver, portadoras de novos argumentos para excessos interpretativos[41]. No presente domínio material, o relevo especialíssimo dos factos das novas tecnologias e do domínio normativo na interpretação constitucional impõe, com especial acuidade, a sobriedade desta viagem hermenêutica, em detrimento de conceções que indicam não como o direito é, mas sim como o direito deve ser[42], ou seja uma ideologia[43].

2.4. Não sendo este o *locus* adequado ao aprofundamento da questão[44], cabe, não obstante, sufragar a lucidez das críticas a estas aceções suprapositivas de Constituição, contida na afirmação de que nem tudo o que pode ser considerado moralmente errado é inconstitucional e ilícito[45], porquanto a atribuição de relevância a certos juízos morais não implica, necessariamente, o acolhimento da respetiva juridicidade. O inverso favorece e alimenta, precisamente, a conceptualização de uma indesejável Constituição não escrita, não oficial, que vai silenciando a efetividade e normatividade da Constituição escrita e oficial[46]. Não se trata de uma opção

[40] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 67 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 63 e segs.

[41] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 77 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 79 e segs.

[42] POZOLO, Susanna/DUARTE, Écio Oto Ramos (2006) O *Neoconstitucionalismo e Positivismo Jurídica*, São Paulo: Landy Editora; p. 78.

[43] SANCHIS reconhece que, para além do modelo institucional de uma certa forma de organização política e uma teoria do direito, o neoconstitucionalismo é também uma ideologia. Como ideologia, identifica-se com a filosofia política que considera que o Estado Constitucional de Direito representa a melhor e a mais justa forma de organização política: "*Em ternos metodológicos, se é assim, onde ele existe terá de sustentar uma vinculação necessária entre a moral e o direito e postular alguma forma de obrigação de obediência ao direito."* - SANCHIS, Luis Prieto (2001), "Neoconstitucionalismo e Ponderación Judicial", *AFDUAM, 5*; pp. 201 e 202.

[44] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 77 e segs.

[45] Esse foi, alias, um dos principais problemas apontados a TRIBE por SEGALL, a propósito da sua *"Invisible Constitution".* SEGALL atribui as perplexidades expressas por TRIBE, sobre o Direito Constitucional norte-americano, à constante subjetividade e incoerência das decisões jurisprudenciais do Supremo Tribunal – " *The differences between the results in Bowers and Lawrence, Usery and Garcia, Garcia and Printz, and Roe, Casey, Stenberg, and Gonzales v. Carhart have little to do with texto, history and structure, or precedent, and everything to do with Justice Blackmun changing his mind in Garcia, Justice Kennedy's personal agenda to overturn Bowers, and the substitution on the Court of Justice Alito for Justice O'Connor."* - SEGALL, Eric. J. (2009) "Lost in Space: Lawrence Tribe's *Invisible Constitution*", *Northwestern University Law Review*, Vol. 103; p. 447.

[46] OTERO, Paulo (2010) *Direito Constitucional Português: Organização do Poder Político*, Vol. II, Almedina: Coimbra; pp. 135 e segs; PETTYS, Todd E. (2009) "The Myth of the Written Constitution", *Notre Dame Law Review*, Vol. 84; pp. 991 e segs.

comodista[47], pois a ideia de uma Constituição não oficial que vai gerando a sua própria normatividade informal, a par da Constituição escrita oficial, não é suficiente para gerar um novo parâmetro de invalidade, suscetível de fundar um juízo de inconstitucionalidade [48], enquanto expressão de uma desconformidade face à normatividade integrante da Constituição não-oficial[49]. O entendimento inverso, propiciado pela adoção de uma conceção suprapositiva axiológica de Constituição, implicaria que a formulação de um juízo de inconstitucionalidade "*envolvesse uma prévia indagação sobre a normatividade constitucional efectivamente vigente*"[50], convocando dois tipos de normatividade potencialmente aplicáveis e, reflexamente, potencialmente inválida, com graves danos para a segurança e certeza jurídica. Para além de uma *Invisible Living Constitution*, contendo alegados novos parâmetros de invalidade constitucional, teríamos de contar com uma *Invisible Dead Constitution*, traduzida num aglomerado apócrifo de enunciados linguísticos constitucionais moribundos, produto da ação dessa ordem suprapositiva sobre as normas da Constituição escrita, oficial.

[47] PETTYS sustenta que *"the myth's claims are far too tightly interwoven with American's fundamental commitments to be easily discarded. By serving their insistence upon endorsing popular sovereignity, acknowledging human beings´ moral fallibility, embracing judicial supremacy, and preserving a sense of nationhood, the myth of the written constitution goes a long way toward legitimating and stabilizing the legal regime that many Americans desire. Those who argue that the myth´s claims should be openly rejected are, thus, doomed for disappointment unless they carry either of two weighty burdens: they must demonstrate either that the objetives at wich the myth's claims are aimed are not sufficiently important to warrant indulging those fictions, or that there are more desirable means by wich those objetives may be achieved*."- PETTYS, Todd E. (2009) "The Myth of the Written Constitution", *Notre Dame Law Review*, Vol. 84; pp. 1049 e 1050.

[48] Obviamente, alerta STERN, a Constituição só pode ser a lei fundamental do Estado constitucional, se aquelas expressões da autoridade governamental que a contrariam, não adquiram efetividade. Mas *Quis custodiet ipsos custodes?*- STERN, Klaus (2008) "El Constitucionalismo. Génesis, Evolución y Universalidad", in *Dignidad de La Persona, Derechos Fundamentales, Justicia Constitucional*, Coord. Francisco Fernández Segado, Dykinson-Constitucional; p. 65.

[49] OTERO, Paulo (2010) *Direito Constitucional Português: Organização do Poder Político*, Vol. II, Almedina: Coimbra; p. 142.

[50] OTERO, Paulo (2010) *Direito Constitucional Português: Organização do Poder Político*, Vol. II, Almedina: Coimbra; p. 143.

## 3. DO IMPACTO DOS FACTOS DAS NOVAS TECNOLOGIAS NO DOMÍNIO NORMATIVO E VERTENTE DINÂMICA DA INTERPRETAÇÃO CONSTITUCIONAL

3.1. A reflexão sobre a relevância específica dos factos das inovações tecnológicas e dos problemas concretos na interpretação constitucional, no esboço de uma interpretação constitucional tecnologicamente neutra[51], obriga a elucidar: i) a distinção dos factos gerados pelas novas tecnologias, pela especificidade do seu impacto, através do domínio normativo, na concretização constitucional; ii) a relevância particular de uma interpretação constitucional tecnologicamente neutra e respetiva expressão no processo dinâmico interpretativo. Em termos análogos a uma abordagem dogmática da Constituição no tempo, cumpre sublinhar que ela só pode cumprir as suas tarefas se conseguir preservar a sua força normativa, apesar das constantes mudanças, assegurando a sua continuidade, sem prejuízo das transformações históricas, no pressuposto da conservação da sua identidade. Nem a Constituição, nem as suas normas concretas podem ser concebidas como letra morta ou algo estático e rígido[52].

Efetivamente, quando se atende ao domínio normativo e aos dados reais, relevantes para a vertente dinâmica da interpretação, constata-se que os factos suscetíveis de influenciar a interpretação constitucional podem revestir diversas naturezas, ter diferentes incidências na norma constitucional e gerar, ou mesmo justificar, operações interpretativas de recorte e intensidade diversas. Os factos, com impacto na interpretação constitucional, podem assumir natureza social, política ou ideológica, sendo responsáveis pela configuração de alterações quase impercetíveis no programa normativo-constitucional, as quais, todavia, não podem ser negligenciadas, sob pena de legitimarem o desenvolvimento de mutações constitucionais impuras, inconstitucionais e indesejáveis[53]. Uma mutação pura,

[51] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 96 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 84 e segs.

[52] HESSE, Conrado (2001) "Constitución y Derecho Constitucional", *in Manual de Derecho Constitucional – Benda, Maihofer, Vogel, Hesse, Heyde*, 2. ª Ed., Madrid; p. 9.

[53] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 96 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o*

enquanto ainda produto genuíno de uma operação interpretativa, postula que esta não se separe da norma interpretada, devendo fidelidade ao seu programa normativo, compreendido através do método jurídico[54]. Regra geral, porém, tais mudanças reclamam largos períodos de tempo para se manifestarem e ganharem raízes no *acquis* constitucional, até o correspetivo resultado normativo se encontrar pronto a ser desvelado em sede de interpretação. Neste contexto, as mudanças interpretativas diluem-se no tempo e raramente suscitam choques jurídico-constitucionalmente relevantes.

Pelo contrário, os factos gerados pela evolução da técnica e das tecnologias são muito rápidos, mesmo mais velozes do que a mais tecnológica comunidade jurídica, imbuídos de um tempo diferente do tempo do legislador constituinte., sendo a densidade do legislador ordinário um problema, dogmatizado, especificamente, à luz do ciberespaço[55]. Perante Constituições detalhadas, como a nossa, a evolução tecnológica revela-se, particularmente, rápida, sendo essa velocidade proporcional ao risco de nominalização constitucional. O grau de erosão do programa normativo, contido na disposição constitucional, é especialmente voraz, revelando-se mesmo na desintegração do enunciado textual.

3.2. Nesta senda, cabe questionar se a interpretação da Constituição perante as novas tecnologias assume um caráter de especialidade ou nos deve *levar a olhar mais de perto os valores que procura preserva*r[56], porquanto o medo do desconhecido, facilmente, pode levar-nos a descurar a guarda constitucional[57]. Como ponto de partida, todavia, adotamos dois dos impressivos axiomas formulados precocemente por TRIBE, há mais de duas décadas, a propósito da Constituição no Ciberespaço e

---

*Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 84 e segs.

[54] Como nota Blanco de MORAIS, *"como é enfatizado por BOCKENFÖRD, por HESSE e pelo próprio MÜLLER"*. - BLANCO DE MORAIS, Carlos (2013) "As Mutações Constitucionais implícitas e os seus limites jurídicos: autópsia de um Acórdão controverso*", Jurismat*; Portimão, n.º 3, pp. 55-90. ISSN: 2182-6900; p. 83.

[55] REED, Chris (2010) "How to make Bad Law: Lessons from Cyberspace", *in The Modern Law Review, Vol 73;* p. 912; FULLER, Lon L. (2000), "Eight Ways to Fail do Make Law", *in Philosophy of Law*, Feinberg &Coleman, eds. USA, pp. 91 e segs.

[56] TRIBE, Lawrence H. (1991) "The Constitution in Cyberspace: Law and Liberty beyond The Electronic Frontier", *The Humanist*, Set-Oct; p. 1.

[57] Recorrendo à sugestiva comparação de Carla GOMES*, "a gestão do risco tecnológico e do risco social revelam algumas afinidades: têm ambas vocação universal, como ideias puras geram um capital político que se alimenta dos temores mais básicos dos cidadãos; em versão extremada promovem dinâmicas de alienação da liberdade*". – GOMES, Carla Amado (2011), "Estado Social de Direito e concretização de direitos fundamentais na era tecnológica: algumas verdades inconvenientes", *Textos Dispersos de Direito Constitucional*, AAFDL: Lisboa; pp. 75 e segs.

respectiva interpretação: apesar das novas tecnologias: i) o governo não pode controlar o conteúdo da informação e ii) os princípios constitucionais mantêm-se[58]. Referindo-se à Constituição dos EUA, o constitucionalista norte-americano alerta que os juízes, ao interpretarem uma Constituição do final do século XVIII, tendem a esquecer que, se as disposições constitucionais não forem lidas numa perspetiva atualista e dinâmica, os seus valores arriscam-se a perder a proteção de que já beneficiaram[59]. Não é, efetivamente, admissível que as mudanças tecnológicas impliquem alterações da Constituição[60], à margem do processo formal de revisão, e esse é um limite interpretativo, implícito e intransponível.

Uma tese que não ofereça devida resistência à enorme pressão interpretativa, exercida pelo problema concreto, no contexto do domínio normativo, obstando à tradução de contextos, partilha afinidades com as conceções que conferem demasiada relevância à pré-compreensão do intérprete, em detrimento do direito positivo, quanto ao risco de excessos de interpretativismo, conducentes a normatividades apócrifas, paralelas ou sobrepostas à Constituição oficial: i) ambas resultam da hipervalorização de algumas das *supra* referidas condições básicas de concretização constitucional, inerentes à opção por uma metódica estruturante enquanto modelo interpretativo; ii) ambas reclamam a necessidade de estabelecer limites interpretativos. Substituir o peso específico de certos problemas concretos, excluindo-os de uma tradução dos valores constitucionais para o atual contexto tecnológico, pelos preconceitos filosóficos, políticos ou morais do intérprete, carreados livremente, para certas conceções, para a interpretação constitucional, conduz-nos exatamente ao mesmo resultado. Não obstante: enquanto no caso das aceções suprapositivas, será, porventura, uma atuação mais construtivista do intérprete suscetível de gerar essas interrogações adicionais, no

[58] TRIBE, Lawrence H. (1991) "The Constitution in Cyberspace: Law and Liberty beyond The Electronic Frontier", *The Humanist*, Set-Oct; p. 11 e p. 13.

[59] No caso *Olmstead v. United States*, a questão era a de saber se as escutas telefónicas eram proibidas pela Quarta Emenda. O Tribunal sustentou que não, uma vez que, quando a Constituição foi promulgada *(Chief Justice Taft)* a Quarta Emenda pretendia evitar a invasão de propriedade, no sentido físico. Contudo o Juiz BRANDEIS sustentou uma posição diferente, considerando que a invasão de propriedade era a única forma do Estado invadir interesses pessoais e privados, não devendo a Constituição deixar os cidadãos desprotegidos perante as mudanças de tecnologias de vigilância e de comunicação. O que a Constituição protegia, deve continuar a proteger após as mudanças tecnológicas. - LESSIG, Lawrence, (1996) "Reading the Constitution in Cyberspace", *45 Emory*, L. J., number 3: p. 4.

[60] LESSIG considera que esta posição do juiz BRANDEIS merece o aplauso e o reconhecimento do mundo cibernético, "*devendo tornar-se num modelo dos ativistas do ciberespaço e o primeiro capítulo na luta pela proteção do ciberespaço"*. - LESSIG, Lawrence, (1996) "Reading the Constitution in Cyberspace", *45 Emory*, L. J., number 3: p. 4.

sentido de aceder a uma ordem suprapositiva que satisfaça aos seus preconceitos; uma interpretação tecnologicamente neutra sugere, precisamente, o juízo inverso, porquanto será a inércia do intérprete, rendida à voracidade destruidora das novas tecnologias, que obstaculizará uma interpretação restituidora da efetividade das normas constitucionais.

3.3. O desiderato particular de uma interpretação constitucional tecnologicamente neutra é, precisamente, o de salvar a identidade constitucional, perante as mudanças tecnológicas, garantindo que o limite interpretativo seja, efetivamente, o texto constitucional [61] . O sobredito desígnio hermenêutico reclama flexibilidade na interpretação textual ou literal[62], uma tradução fiel dos valores constitucionais para a realidade do ciberespaço[63], paralela a uma incontornável interpretação atualista e evolutiva[64], atendendo ao elevado risco de enfraquecimento ou perda de efetividade de certas regras ou princípios constitucionais:

i) É, efetivamente, impossível, *"constituindo mesmo um puro autismo, conceber o ordenamento clausurado nos contrafortes delineados pela autopoiesis*"[65] e ignorar essa dimensão factual, informal, que integra as normas jurídicas num dado contexto social, porquanto *"as normas são veículos de comunicação entre o hemisfério da realidade factual existente na sociedade e o hemisfério formal do sistema jurídico-positivo*"[66]. A estabilidade constitucional não pode ser totalmente inflexível, pois uma Constituição também deve ser idónea para o futuro e modificada, caso se distancie da vontade geral [67] . Uma interpretação constitucional tecnologicamente neutra, baseada numa revolução do processo comunicativo, que

[61] A propósito da influencia do tempo na Constituição - HESSE, Konrad (2001) "Constitución y Derecho Constitucional", *in Manual de Derecho Constitucional – Benda, Maihofer, Vogel, Hesse, Heyde*, 2. ª Ed., Madrid; p. 10.
[62] TRIBE, Lawrence H. (1991) "The Constitution in Cyberspace: Law and Liberty beyond The Electronic Frontier", *The Humanist*, Set-Oct; p. 15.
[63] Ao contrário dos originalistas, que acreditavam que a fidelidade à Constituição requeria fazer o que os constituintes teriam feito *(one-step originalism),* a tradução implica o entendimento de que para "*to preserve meaning across contexts, one must change readings across contexts" (two-steps originalism).* - LESSIG, Lawrence, (1996) "Reading the Constitution in Cyberspace", *45 Emory*, L. J., number 3: p. 5. Contudo, LESSIG é considerado por alguma doutrina como um *broad originalist.*
[64] OTERO, Paulo (2010) *Direito Constitucional Português: Organização do Poder Político,* Vol. II, Almedina: Coimbra; p. 159.
[65] MORAIS, Carlos Blanco (2012) *Curso de Direito Constitucional, Tomo I, 2.ª Ed.*, Coimbra Editora: Coimbra; pp. 212 e 213.
[66] OTERO, Paulo (2010) *Direito Constitucional Português: Organização do Poder Político,* Vol II, Almedina: Coimbra; p. 159.
[67] STERN, Klaus (2008) "Desarrollo Constitucional Universal y Nuevas Constituciones", in *Dignidad de La Persona, Derechos Fundamentales, Justicia Constitucional*, Coord. Francisco Fernández Segado, Dykinson-Constitucional; p. 78.

vem questionar, diariamente, a legitimidade dos institutos jurídicos tradicionais[68], "*não pode prescindir da consciência dessa comunicabilidade entre hemisférios, atento o facto de a positividade do direito ser determinada pela sua ligação ao mundo dos factos sociais e atos humanos"*[69]. Acresce o risco da ambiguidade e da incerteza do cidadão, pois uma Constituição só é autêntica e completa se define com clareza a posição do indivíduo face ao Estado[70]. Se as questões fundamentais para os cidadãos deixam de ser tratadas no contexto constitucional, a Constituição perde a sua força normativa;

ii) Não obstante, o incontornável peso do domínio normativo e dos factos das novas tecnologias na interpretação constitucional, e as inerentes limitações do legislador, a afirmação de que a regulação da *internet* pode ou deve assumir uma intensidade *sui generis*, diretamente proporcional à gravidade, extensão e indeterminação de eventuais danos, não pode nem deve impressionar. Impõe-se, precisamente, a definição de limites da interpretação constitucional, que obstem à legitimação de um ativismo judicial ou regulatório, desenfreado ou indesejado ou, simetricamente, a um suspeito amorfismo regulatório, fundando-se ambos os excessos em atitudes temerárias. LESSIG advertia que uma cultura constitucional pouco ativista dificulta a dogmatização das questões do ciberespaço[71]. Mas o reconhecimento de que, no mínimo, os novos problemas requerem uma interpretação constitucional mais criativa e intensa, para que os valores constitucionais possam ser objeto de uma adequada tradução para o atual contexto tecnológico, não implica a exacerbação da dimensão factual, integrante do hemisfério da realidade, em detrimento do sistema jurídico positivo, ou do programa normativo.

iii) Uma interpretação constitucional tecnologicamente neutra, baseada na consideração dos *topoi* fornecidos pelo texto e programa normativo, cuja vontade

---

[68] Como descreve Blanco de MORAIS, *"as variantes mais destacadas de inputs oriundos do sistema social manifestam-se através de exigências e apoios; enquanto as primeiras se concretizam em "cargas", "problemas" e "dilemas" carecidos de solução, as segundas consistem em manifestações de suporte ao sistema em geral, às suas autoridades e às decisões por estas tomadas".* - MORAIS, Carlos Blanco (2012) *Curso de Direito Constitucional, Tomo I, 2.ª Ed.*, Coimbra Editora: Coimbra; p. 212.

[69] MORAIS, Carlos Blanco (2012) *Curso de Direito Constitucional, Tomo I, 2.ª Ed.*, Coimbra Editora: Coimbra; p. 213.

[70] STERN, Klaus (2008 "Desarrollo Constitucional Universal y Nuevas Constituciones", in *Dignidad de La Persona, Derechos Fundamentales, Justicia Constitucional*, Coord. Francisco Fernández Segado, Dykinson-Constitucional; p. 74.

[71] LESSIG, Lawrence, (1996) "Reading the Constitution in Cyberspace", *45 Emory*, L. J., number 3: p. 2.

constituinte seja objetivada na base do seu teor literal e no seu contexto sistemático, teleológico e histórico, pode garantir, a nosso ver, esse resultado mínimo. No entanto, caso se revele insuficiente, obstando a uma tradução de contextos, cabe indagar os *inputs* do hemisfério factual, e garantir a coordenação material entre os *topoi* desvelados, podendo, eventual e excecionalmente, conduzir o intérprete e aplicador do direito à legitimação de alguma deferência judicial, e mesmo regulatória, *in casu*.

O importante é garantir que o que a Constituição protegia continuará a proteger, apesar das mudanças[72] geradas pelas novas tecnologias, salvo se o fundamento da proteção tiver deixado de fazer sentido. Neste caso, em conformidade com uma leitura constitucional tecnologicamente neutra, a manutenção ou depreciação de uma determinada posição jurídica ou regulação só é justificável caso, perante uma mudança tecnológica, exista fundamento para uma atualização/manutenção do regime aplicável ao bem protegido, em conformidade com essa precisa evolução.

## 4. DA INSUBSTITUIBILIDADE DO PAPEL DA JUSTIÇA CONSTITUCIONAL NO CONTROLO DE CONSTITUCIONALIDADE DA REGULAÇÃO DO CIBERESPAÇO

4.1. Em conformidade, o papel da Justiça Constitucional no controlo da constitucionalidade da normatividade vigente e, efetivamente, aplicada na regulação das questões do ciberespaço, reclamante de cuidados especiais atinentes à segurança jurídica, assume cada vez maior importância, no contexto de uma interpretação constitucional tecnologicamente neutra. O impacto dos factos das novas tecnologias no direito positivo suscita problemas sérios de interpretação e integração, podendo, nalguns casos, como vimos, justificar uma atividade judicial mais criativa, como forma de evitar a perda de efetividade ou mesmo deturpação dos programas normativo-constitucionais. Revela-se, neste conspecto, particularmente problemático o impacto das novas tecnologias, por exemplo, sobre os axiomas fundamentais da Legalidade Penal e na reação jurisprudencial às incertezas geradas pelas questões

[72] Como lembra HESSE, na perspetiva de uma Constituição no tempo, a Constituição só pode cumprir as suas tarefas se conseguir preservar a sua força normativa, apesar das constantes mudanças, ou seja, onde assegurar a sua continuidade, sem prejuízo das transformações históricas, o que pressupõe a conservação da sua identidade. - HESSE, Conrado (2001) "Constitución y Derecho Constitucional", *in Manual de Derecho Constitucional – Benda, Maihofer, Vogel, Hesse, Heyde*, 2. ª Ed., Madrid; p. 9.

especialíssimas do ciberespaço, não contempladas pelo legislador. Não obstante os riscos, se atentarmos na jurisprudência constitucional portuguesa sobre esta matéria, podemos verificar que o sentido interpretativo que os juízes constitucionais têm conferido às garantias inerentes ao direito sancionatório público continua a ser relativamente exigente no seu escrutínio e generoso na sua abrangência e apresentação genérica [73] , em plena conformidade com uma interpretação constitucional tecnologicamente neutra. Apenas quando o processo hermenêutico gera uma norma não reconduzível *"à moldura semântica do texto"*[74], um sentido que, não tendo na letra da lei *"um mínimo de correspondência verbal",* extravasava o domínio da mera interpretação jurídica, é que somos reconduzidos ao domínio da analogia e – *in casu* – da analogia (constitucionalmente) proibida nos domínios penal e processual penal[75].

Não obstante os constrangimentos jurídico-processuais, inerentes ao nosso sistema de fiscalização concreta da constitucionalidade, restrito ao controlo de normas, não poderem deixar de inquinar o nosso otimismo, atente-se nas vantagens do recente alargamento funcional do conceito de norma pela jurisprudência constitucional portuguesa. É, atualmente, consensual que o objeto dos processos de fiscalização pode incluir atos normativos, desprovidos da forma de lei, que contenham comandos jurídicos gerais e abstratos[76], incluindo certas interpretações normativas ou o seu critério normativo de decisão, autonomizável da atividade judicial subsuntiva que o origina[77]. Entre estas interpretações normativas, suscetíveis de integrarem o objeto do recurso de fiscalização concreta da constitucionalidade, incluem-se, precisamente, as normas extraídas da integração de lacunas[78], pelo recurso à analogia.

[73] CASTRO, Nuno Teixeira (2015) *Reflexões Quanto ao Impacto das Novas Tecnologias sobre a Legalidade Penal*, Relatório de Mestrado da disciplina de Cibercrime (inédito), do Mestrado em Segurança da Informação e Direito do Ciberespaço, numa organização conjunta entre o IST, FDUL e Escola Naval; pp. 18 e segs.
[74] Cfr. Acórdão n.º 186/2013 do TC.
[75] CASTRO, Nuno Teixeira (2015) *Reflexões Quanto ao Impacto das Novas Tecnologias sobre a Legalidade Penal*, Relatório de Mestrado da disciplina de Cibercrime (inédito), do Mestrado em Segurança da Informação e Direito do Ciberespaço, numa organização conjunta entre o IST, FDUL e Escola Naval; pp. 18 e segs.
[76] MORAIS, Carlos Blanco (2012) *Curso de Direito Constitucional, Tomo I, 2.ª Ed.* Coimbra Editora: Coimbra; pp. 93 e 94.
[77] REGO, Carlos Lopes do (2004) "As interpretações normativas sindicáveis pelo TC", in *Jurisprudência Constitucional*, N.º 3, AATRIC: Lisboa; p. 7.
[78] MORAIS, Carlos Blanco de (2012) *Curso de Direito Constitucional, Tomo I, 2.ª Ed.,* Coimbra Editora: Coimbra; p. 94.

Perante a positivação constitucional expressa do princípio da legalidade criminal, e atendendo à correspetiva proibição de aplicação analógica de normas incriminadoras, os juízes constitucionais advogam que *"uma interpretação sistemática do texto constitucional aconselha a que esse momento hermenêutico "se converta num "pedaço" de normatividade integrante do objeto de controlo*"[79]. Não se trata de legitimar o escrutínio do processo hermenêutico, mas antes de verificar se foram ultrapassados os limites constitucionais a que esse *iter* está sujeito em matéria penal, concretamente, a proibição da analogia *in malam partem*. O entendimento contrário implicaria que um importante e sensível *"pedaço de normatividade*" vigente ficasse à margem da Justiça Constitucional[80]. Perante um domínio normativo, onde o ritmo de intervenção legislativa e correspetiva densidade são particularmente problemáticos, torna-se crucial garantir que o expetável incremento de ativismo judicial, designadamente através da criação de normas *"ad casum",* constitucionalmente devidas, possa ser sujeito ao escrutínio da justiça constitucional.

4.2. Acresce que essa evolução subjectivizante do conceito de norma, para efeitos do objeto dos recursos de constitucionalidade, revela-se especialmente inspiradora nos casos de discordância entre o tempo dos factos gerados pelas novas tecnologias e o tempo do legislador, daí resultando uma omissão normativa lesiva de direitos, liberdades e garantias[81], reclamante da atividade criadora jurisdicional *in casu*. Nesse contexto, se o titular de um direito, liberdade ou garantia ou direito constitucionalmente análogo, lesado por uma omissão normativa inconstitucional goza de uma posição jurídica de vantagem, digna de tutela jurídico-constitucional, então a esse direito há-de corresponder o reconhecimento de um meio processual adequado em sede de justiça constitucional, com vista à obtenção da norma *"ad casum,"* constitucionalmente devida. Não podem os espartilhos processuais, meramente conjunturais, obstaculizar a plena eficácia das normas constitucionais de direitos fundamentais, enfraquecendo a sua posição jusfundamental. Antes pelo

[79] Cfr. Acórdão n.º 79/2015 do TC.
[80] CASTRO, Nuno Teixeira (2015) *Reflexões Quanto ao Impacto das Novas Tecnologias sobre a Legalidade Penal,* Relatório de Mestrado da disciplina de Cibercrime (inédito), do Mestrado em Segurança da Informação e Direito do Ciberespaço, numa organização conjunta entre o IST, FDUL e Escola Naval; p. 25.
[81] CASTRO, Raquel Alexandra Brízida (2015) "Normas implícitas e Normas Constitucionalmente Devidas *"ad casum"* e a Pretensa Quadratura do Círculo Processual Constitucional: Recapitulação, Desmistificação e Tentativa de Reconstrução", in *Obra de Homenagem a Rui Machete*, Almedina: Coimbra; pp. 851-881.

contrário, o direito adjetivo não pode deixar de ser lido em conformidade com a Constituição.

Em termos análogos ao problema da quadratura do círculo, propusemos a difícil tarefa de configuração de um controlo concreto das omissões normativas inconstitucionais, a partir de um sistema concebido para a fiscalização da inconstitucionalidade por ação, numa perspetiva *de jure condito* [82], problema que, neste contexto normativo, reveste particular importância. Partindo da admissibilidade do conceito de normas implícitas inconstitucionais, como ficção jurídica constitucionalmente devida, para efeitos processuais, no contexto da fiscalização concreta de omissões inconstitucionais, acreditamos que é possível descobrir normas implícitas geradas por silêncios normativos lesivos, cuja invalidação, para efeitos de acesso ao TC, abre caminho ao controlo concreto e respetiva reparação jurisdicional, pelo menos, das omissões normativas lesivas de direitos, liberdades e garantias ou direitos análogos. A norma implícita apresenta-se como uma ficção jurídica, sindicável pela Justiça Constitucional na medida da sua normatividade imaterial ou virtual, devendo a sua rejeição jurisdicional ou dos correspetivos efeitos jurídicos dar lugar à criação de uma norma constitucionalmente devida *"ad casum",* no quadro de uma sentença constitucionalmente obrigatória[83].

4.3. Em suma, na esteira de TRIBE, os princípios constitucionais mantêm-se, apesar das novas tecnologias, deslegitimando qualquer tentativa de mutação informal da Constituição, gerada pelo medo ou mera conveniência da indefinição, encorajadora de interpretações arrojadas ou, simetricamente, demasiado contidas. Os Princípios fundamentais estruturantes de um Estado de Direito Democrático não podem ser desprezados na voragem de uma qualquer pretensão regulatória ou de reparação judicial. O que deve reforçar a atitude de vigilância do legislador, mesmo penal, perante as novas realidades, de forma a tornar claras as condutas que são realmente

[82] Conforme tentámos demonstrar, mesmo no plano *de jure condito*: a) A autoria da norma - pelo legislador ou pelo juiz - não é fator decisivo para a definição da idoneidade do objeto do recurso de constitucionalidade; b) A distinção entre inconstitucionalidade por ação ou por omissão, para efeitos de suscitação da questão de inconstitucionalidade, no quadro dos recursos de decisões negativas de inconstitucionalidade, em sede de fiscalização concreta, pode ser considerada irrelevante. - CASTRO, Raquel Alexandra Brízida (2015) "Normas implícitas e Normas Constitucionalmente Devidas *"ad casum"* e a Pretensa Quadratura do Círculo Processual Constitucional: Recapitulação, Desmistificação e Tentativa de Reconstrução", *in Obra de Homenagem a Rui Machete*, Almedina: Coimbra; p. 867.

[83] CASTRO, Raquel Alexandra Brízida (2015) "Normas implícitas e Normas Constitucionalmente Devidas *"ad casum"* e a Pretensa Quadratura do Círculo Processual Constitucional: Recapitulação, Desmistificação e Tentativa de Reconstrução", *in Obra de Homenagem a Rui Machete*, Almedina; Coimbra; pp. 872 e segs.

proibidas e as que são permitidas, na estrita medida do jurídico-tecnologicamente possível. O próprio regime constitucional de proteção dos direitos fundamentais e, em última instância, de garantia da própria Constituição, não pode deixar de ser aplicável, nas suas dimensões orgânico-formais e materiais, em benefício de alegados estados de exceção legal ou constitucional, fundados na complexidade das inovações tecnológicas. Como veremos, tal como a rigidez constitucional, o imperativo de proteção dos direitos, liberdades e garantias mantém-se, através da sua aplicabilidade direta, reserva de lei ou exigência de reserva de densificação total, assim como as novas tecnologias não os isenta de ponderações, para resolver limitações e restrições, como todos os outros. Esse deve ser o princípio.

## PARTE II - CONSTITUIÇÃO E REGULAÇÃO DO CIBERESPAÇO

É, efetivamente, problemática, no atual estado da arte, a elaboração genérica, prévia e abstrata, de critérios distintivos para a regulação da *internet*, ou a afirmação da relevância dos mesmos para a justificação da opção por uma ou outra resposta constitucional. Não obstante, os sinais existentes reclamam, gritantemente, uma mudança de enfoque regulatório[1], atendendo à crescente indefinição dos perímetros protetivos dos direitos e liberdades fundamentais e, consequente alargamento dos elencos de condutas e agentes, eventualmente responsáveis por intervenções desvantajosas sobre essas posições jurídicas fundamentais.

### 5. DA RELEVÂNCIA CONSTITUCIONAL DO IMPACTO EFETIVAMENTE RESTRITIVO DAS NOVAS TECNOLOGIAS NO PERÍMETRO PROTETIVO DOS DIREITOS CONSTITUCIONALMENTE PROTEGIDOS

5.1. Esta lição resulta também do debate sobre o "*internet exceptionalism",* particularmente vivo no contexto constitucional norte-americano. Para TUSHNET, a verdadeira questão não se coloca na opção entre *"internet exceptionalism" ou Primeira Emenda com ajustamentos"*, mas antes entre *"internet exceptionalism" ou Primeira Emenda com ajustamentos",* por referência a um específico regime, aplicável a um problema específico….[2]. O debate em torno do designado *"internet excepcionalism"* da Primeira Emenda[3] incide sobre o problema de saber se as características tecnológicas da *internet* (mais genericamente, as tecnologias de

[1] Perante as novas tecnologias e os desafios do ciberespaço, especificamente no contexto mediático, defendemos a adoção de um modelo regulatório integrado dos Media, abrangendo Conteúdos, Comunicações e Concorrência. - CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 426 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 352 e segs e 401 e segs.

[2] TUSNHET, Mark (2015) "*Internet Exceptionalism: An Overview from General Constitutional Law*", 56 *Wm. & Mary L. Rev.* 1637 (2015), p. 1672. – disponível em http://scholarship.law.wm.edu/wmlr/vol56/iss4/15 e http://www.cijic.org/cyberlawbycijic/.

[3] WU, Tim (2010) "Is Internet Exceptionalism Dead?", in *THE NEXT DIGITAL DECADE - ESSAYS ON THE FUTURE OF THE INTERNET*, p. 179, Berin Szoka, Adam Marcus, eds., TechFreedom, Washington, D.C., 2010. Available at SSRN: http://ssrn.com/abstract=1752415 - última visita em junho de 2015

informação do século XXI) justificam uma regulação da informação, divulgada através da *internet*, diferente da propugnada, durante os séculos XIX e XX, para os *media* tradicionais.

No relato de TUSHNET, é possível detetar duas estratégias de desenvolvimento de uma *"law of the internet unto itself",* controvertida nos EUA. Na primeira, permite-se um período inicial experimental do legislador, porquanto nem ele nem o tribunal dispõem de especiais conhecimentos sobre a resposta constitucional apropriada à mais recente inovação tecnológica. O que aconselha a opção por uma deferência judicial relativamente a processos decisórios democráticos, para permitir a acumulação de experiência. A partir de dado momento, todavia, considera-se que os juízes se encontram em melhor posição para implementar os valores constitucionais, de forma mais esclarecida, criando-se as condições legitimadoras de uma doutrina judicial mais restritiva em relação à intervenção legislativa. Esta estratégia conduz, portanto, a uma forma transitória de *internet excepcionalism*, pois à medida que a experiência se vai acumulando, os juízes passarão a estar numa posição de assimilar a regulação dessas *não-tão-novas tecnologias* na doutrina geral da Primeira Emenda, talvez com alguns ajustamentos, para poder lidar com particularidades tecnológicas, verdadeiramente distintivas[4]. Para a segunda estratégia, perante uma ameaça à liberdade de expressão gerada por uma tecnologia emergente, o caso deve ser analisado por referência a princípios já elaborados, a partir da Primeira Emenda. Essa disciplina funda-se em toda a experiência que a primeira estratégia permitiu acumular. Ora, se o padrão comum acerca dos *media* tradicionais é o *supra* referido - deferência inicial dos juízes seguida da aplicação da doutrina da Primeira Emenda; e o resultado, mais do que provável, é sempre o mesmo, questiona-se a necessidade de a sociedade incorrer nos custos subjacentes a uma regulação que, mais tarde ou mais cedo, vai revelar-se inconstitucional.

Note-se que ambas as estratégias se baseiam na experiência: a primeira atende à experiência acumulada, relativamente a cada tecnologia, *"within technologies";* ii) a segunda deduz inferências *"across technologies*". No alerta de TUSHNET, essa escolha acaba, não obstante, por ser determinada pelas pré-compreensões do intérprete, porquanto os adeptos da Primeira Emenda vão sempre procurar *"across*

[4] TUSNHET, Mark (2015) "*Internet Exceptionalism: An Overview from General Constitutional Law*", 56 *Wm. & Mary L. Rev.* 1637 (2015), p. 1643. - disponível em http://scholarship.law.wm.edu/wmlr/vol56/iss4/15 e http://www.cijic.org/cyberlawbycijic/

*technologies",* enquanto os céticos – em relação a decisões judiciais agressivas de controlo dos legisladores democráticos competentes – vão procurar *"within technologies"*. Essa escolha, em seu entendimento, vai depender da regulação específica sobre o problema concreto que estiver em análise.

5.2. Pela nossa parte, como vimos, insistimos na lição precoce de TRIBE[5], segundo a qual, apesar das novas tecnologias, os princípios constitucionais devem manter a sua efetividade e o Estado/Governo não deve interferir nos conteúdos, independentemente do meio através do qual a informação é divulgada. O que significa que, pelo menos no ordenamento jurídico-constitucional português, sem prejuízo da sua liberdade de conformação, na sua precisa medida constitucional, como veremos: i) o legislador encontra-se vinculado ao respeito dos direitos, liberdade e garantias e respetivo regime de proteção e ii) ao juiz compete julgar, desaplicar normas inconstitucionais[6], resolver conflitos de direitos ou omissões lesivas de direitos, procedendo a ponderações e criar normas *"ad casum",* constitucionalmente devidas, através de sentenças constitucionalmente obrigatórias. E esta repartição de tarefas, com respaldo constitucional, não pode acolher desvios em função de alegados estados de exceção tecnológicos. De resto, num contexto de vinculação estreita do legislador, o recurso cuidado a um conjunto de regras categóricas ou a testes de ponderação pode conduzir-nos a resultados semelhantes: um elenco bem delimitado de regras categóricas permite-nos identificar um conjunto de características que correspondem aquelas que são, necessariamente, consideradas pela ponderação, às quais conferirá o devido peso, nos resultados que produzir[7]. São, portanto, questões correntes de interpretação de uma determinada Constituição.

Pelo exposto, na esteira de TUSHNET, não deixa de ser falaciosa a defesa, *a priori* e em abstrato, de regras especiais para a *internet*, ou de um *"internet exceptionalism",* premissa que se revela particularmente sugestiva no contexto mediático, tendo por referência comparativa a regulação dos *media* tradicionais, sendo esta uma distinção, tradicionalmente, baseada na plataforma e modelo de negócio na *internet* e mesmo na natureza pública ou privada das restrições. Para

[5] TRIBE, Lawrence H. (1991) "The Constitution in Cyberspace: Law and Liberty beyond de Electronic Frontier", *The Humanist*, Set-Oct; p. 11 e p. 13.
[6] Cfr. Artigo 204.º da CRP.
[7] TUSNHET, Mark (2015) "*Internet Exceptionalism: An Overview from General Constitutional Law*", 56 *Wm. & Mary L. Rev.* 1637 (2015), p. 1641. – disponível em http://scholarship.law.wm.edu/wmlr/vol56/iss4/15 e http://www.cijic.org/cyberlawbycijic/.

efeitos de delimitação do perímetro protetivo dos direitos e liberdades, positivados constitucionalmente, estes fatores são, perante a realidade do ciberespaço, jurídico-constitucionalmente irrelevantes. Ao invés, para a garantia do perímetro protetivo dos direitos fundamentais, assume cada vez maior relevância jurídica: i) a atividade efetivamente desenvolvida, para efeitos de escolha do modelo regulatório aplicável[8]; ii) o impacto efetivamente restritivo das intervenções desvantajosas [9] . Independentemente da sua forma, o que importa é o impacto efetivo dessa intervenção restritiva[10].

Neste contexto, a renovação do debate conceptual sobre a censura, por exemplo, fornece pistas para a consolidação de um conceito amplo, que destaca importantes restrições à liberdade de expressão, que nem sempre assumem essa natureza, embora sejam *"funcionalmente equivalentes"* à censura prévia tradicional[11]. Nessa medida, todas essas restrições, em sentido amplo, serão obrigatoriamente confrontadas com os pertinentes requisitos formais e materiais, fundados na Constituição, tornando irrelevante a diferente natureza de meios e agentes ou no que concerne ao momento da intervenção desvantajosa:

i) No Direito Constitucional alemão, por exemplo, o conceito de censura abrange, para além das intervenções tradicionais, aquelas medidas de facto similares a essas intervenções, sendo, por exemplo, um mecanismo fáctico de controlo considerado um equivalente funcional à censura formal*[12];*

ii) A proibição de censura dirigia-se, tradicionalmente, ao Estado, mas a essência programática da liberdade de comunicação obriga o legislador a estender essa proibição a outras instâncias de controlo, designadamente, a outros *"potenciais*

[8] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 459 e segs.

[9] Vide a relevância dos novos problemas trazidos pelo Ciberespaço para uma problematização constitucional da adoção de um modelo principiológico ponderativo, aliado a conceções amplas da previsão normativa e das restrições a direitos fundamentais. - CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 117 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 104 e segs,

[10] MACHADO, Jónatas (2002), *Liberdade de Expressão: Dimensões Constitucionais da Esfera Pública Social*, Coimbra Editora: Coimbra; pp. 486 e segs.

[11] MACHADO, Jónatas (2002), *Liberdade de Expressão: Dimensões Constitucionais da Esfera Pública Social*, Coimbra Editora: Coimbra; pp. 486 e segs.

[12] Veja-se, por exemplo, o caso de um controlo de facto, estabelecido em função de uma perspetiva de benefício patrimonial, com a difusão de certos conteúdos. - HOFFMANN-RIEN, Wolfgang (2001) "Libertad de Comunicación y de Medios", i*n Manual de Derecho Constitucional, Benda/Maihofer/Vogel/Hesse/Heyde*, 2.ª Ed., Marcial Pons: Madrid; p. 175.

*controladores privados"* poderosos, na medida em que se aproveitem do seu poder social ou económico para controlar os *media*[13];

iii) É possível considerar, materialmente, censórias muitas das restrições *ex post facto* à liberdade de expressão e, em contrapartida, admitir em abstrato que uma determinação prévia[14], de natureza administrativa ou judicial[15], possa vir a ser menos gravosa para o direito ou liberdade, do que um processo de condenação posterior à publicação[16].

As inquietações elencadas agravam-se no mundo digital. Atente-se, por exemplo, no regime português do *notice and take down*, que habilita dois órgãos administrativos Reguladores, com natureza de entidades administrativas independentes, a procederem a uma verdadeira censura material de informações difundidas por meios de comunicação social *online*, que contenham dados que estas entidades considerem sensíveis e, em conformidade, insuscetíveis de serem divulgados, por violarem ou poderem violar outros bens, como o direito à reserva da intimidade da vida privada[17] ou a segurança pública. Serão tais procedimentos

[13] HOFFMANN-RIEN, Wolfgang (2001) "Libertad de Comunicación y de Medios", i*n Manual de Derecho Constitucional, Benda/Maihofer/Vogel/Hesse/Heyde*, 2.ª Ed., Marcial Pons: Madrid; p. 175.

[14] No que concerne ao seu impacto nas liberdades de expressão e de imprensa, as diferenças entre medidas judiciais prévias e sentenças judiciais condenatórias, civis ou penais, não são substanciais. - TOLLER, Fernando M. (2011), *El formalism en la libertad de expresión: Critica de la distinción absoluta entre restricciones previas y responsabilidades ulteriores*, Marcial Pons: Buenos Aires, pp. 47 e segs.

[15] CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 204 e segs; (2014) *Constituição, Lei de Regulação dos Media: Contributo para o Estudo da Constituição Portuguesa da Comunicação*, Dissertação de Doutoramento (Inédita), Faculdade de Direito da Universidade de Lisboa; pp. 196 e segs.

[16] A propósito da dificuldade de, por vezes, distinguir o que é uma restrição prévia ou responsabilidade posterior, veja-se o seguinte exemplo: em Cincinnati, o *city Council*, cansado do comportamento de um determinado indivíduo que, invariavelmente, causava distúrbios nas audiências públicas, aprovou um regulamento que excluía a assistência a essas audiências, durante um período de 60 dias, de todos aqueles que se comportassem de forma a afetar a ordem das sessões. - TOLLER, Fernando M. (2011), *El formalism en la libertad de expresión: Critica de la distinción absoluta entre restricciones previas y responsabilidades ulteriores*, Marcial Pons: Buenos Aires, p. 41.

[17] Veja-se o caso *do notice and take down* obrigatório:

a) No caso da CNPD (Comissão Nacional de Proteção de Dados), o artigo 20.º, número 1, alínea b) do Decreto-Lei n.º 67/98, o sujeito pode solicitar à CNPD que bloqueie ou mande destruir dados pessoais recolhidos ou divulgados;

b) No caso da ERC, de acordo com o artigo 24.º, número 3, alínea e), dos seus Estatutos, o sujeito pode solicitar a restrição da circulação de serviços da sociedade da informação que contenham conteúdos submetidos a tratamento editorial e que, "lesem ou ameacem gravemente" os valores previstos no artigo 7.º, número 1, do Decreto-Lei n.º 7/2004, de 7 de janeiro. O artigo 7.º refere-se às medidas restritivas que podem ser adotadas contra um prestador de serviços "na medida em que possa lesar ou ameaçar gravemente:
b) Saúde pública; c) A segurança pública, nomeadamente na vertente da segurança e defesa nacionais; d) Os consumidores, incluindo os investidores. Este Decreto-lei foi aprovado no uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de maio, e transpõe para a ordem jurídica nacional a

subsumíveis ao conceito de censura, em termos constitucionalmente *ilícitos*? Este procedimento, a cargo eventualmente de privados (operadores de infraestruturas críticas), aliado à designada norte-americana *"Good Samaritan provision"*[18], é considerado um bom exemplo de novo modelo de *governance* que caracteriza a globalização[19], e implica, no caso norte-americano, uma mudança de uma regulação, de substancial para procedimental, e de uma regulação estatal para uma corregulação global. Pode, porém, adicionar o problema da eventual legitimação de critérios não oficiais, politica e economicamente corretos, constitutivos de um mecanismo informal, mas eficaz, de censura privada de conteúdos[20]. Trata-se, indubitavelmente, de um procedimento deveras paradigmático: i) perante a doutrina tradicional das restrições prévias, seria reconduzido liminarmente a uma censura ilegítima, pois implica uma atuação prévia de entidade administrativa em conteúdos sujeitos a tratamento editorial; ii) cabe porém admiti-lo como censura *prima facie*, cuja legitimidade pode resultar da ponderação constitucional com os bens colidentes; iii) alarga o universo de potenciais atores censórios, a ter em consideração num conceito amplo de censura.

Note-se o perigo adicional da aplicação de regras, suscetíveis de gerar efeitos danosos, quando incidem sobre os intermediários da *internet*, referindo-se, também a este propósito um *"chilling effect*", gerado por uma *"censorship by proxy"*[21]. São conceitos, especialmente, problematizados no contexto da regulação do ciberespaço, em especial perante as estratégias dos Estados em matéria de Cibersegurança. Revelam claramente os perigos que podem advir da indefinição de alguns conceitos e da natureza da intervenção dos privados em áreas especialmente delicadas, como a que nos ocupa, em prol da segurança, questão que abordaremos no ponto seguinte (Ponto 6).

---

Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno

[18] *"No provider (...) of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider (...) considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.*"- CDA 47 U.S.C. § 230 (c) (2) (A) http://www4.law.cornell.edu/uscode/47/230. html.

[19] FRYDMAN, Benoît/RORIVE, Isabelle (2002) "Regulating Internet Content through Intermediaries in Europe and the USA", in *Zeitschrift für Rechtssoziologie* 23, Heft 1, S. 41-59, p. 54.

[20] FRYDMAN, Benoît/RORIVE, Isabelle (2002) "Regulating Internet Content through Intermediaries in Europe and the USA", in *Zeitschrift für Rechtssoziologie* 23, Heft 1, S. 41-59, p. 54.

[21] KREIMER, Seth F. (2006) "Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of The Weakest Link", *in University og Pennsylvania Law Review*, Vol 155.;

5.3. Concorrendo para a atual indefinição e desestabilização regulatória, atente-se no Acórdão do TJ de 13 de maio de 2014[22] e nas *FCC's Open Internet rules*, adotadas em fevereiro de 2015[23], fatores que, a nosso ver, assumem relevância incontornável na elucidação das diferentes matizes do problema:

5.3.1. No Acórdão *sub judicio*[24], tratava-se de saber se: a) A Diretiva[25] deve ser interpretada no sentido de que a atividade de um motor de busca, como fornecedor de conteúdos[26], pode ser qualificada de *"tratamento de dados pessoais",* para efeitos de aplicabilidade daquela mesma disposição, quando essas informações contenham dados pessoais; b) Em caso afirmativo, se o operador de um motor de busca deve ser considerado responsável pelo referido tratamento de dados pessoais, na aceção dessa mesma disposição.

O Tribunal não se mostrou convencido pela argumentação aduzida pela *Google Spain* e a *Google Inc*., segundo a qual, *"limitam-se a tratar as informações acessíveis na Internet, no seu conjunto, sem fazer uma seleção entre dados pessoais e outras informações".* Acabou por soçobrar vitória a tese de que a atividade de um motor de busca *"é suscetível de afetar, significativamente e por acréscimo à atividade dos editores de sítios web, os direitos fundamentais à vida privada e à proteção dos dados pessoais"*. Para o Tribunal, o operador desse motor, como pessoa que determina as finalidades e os meios dessa atividade, *"deve assegurar, no âmbito das suas responsabilidades, competências e possibilidades, que essa atividade satisfaça as exigências da Diretiva".* Em suma, o que se pensava inicialmente ser uma

[22] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5d175fdbfddfd4cd89013bdda104ae9a3.e34KaxiLc3eQc40LaxqMbN4OaNmNe0?text=&docid=152065&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=401734 .

[23] https://www.fcc.gov/openinternet - última visita em julho de 2015. Segundo a FCC, estas regras *"are grounded in the strongest possible legal foundation by relying on multiple sources of authority, including: Title II of the Communications Act and Section 706 of the Telecommunications Act of 1996. As part of this decision, the Commission also refrains (or "forbears") from enforcing provisions of Title II that are not relevant to modern broadband service. Together Title II and Section 706 support clear rules of the road, providing the certainty needed for innovators and investors, and the competitive choices and freedom demanded by consumers*."

[24] Sem prescindir da relevância conferida ao direito ao esquecimento, enquanto corolário da consolidação de um direito fundamental à autodeterminação informacional. - CASTRO, Raquel Alexandra Brízida (2015) *Constituição, Lei e Regulação dos Media* (em processo de publicação); pp. 459 e segs.

[25] Cfr. Artigo 2.°, alínea b), da Diretiva 95/46.

[26] " *(...) que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexa-las automaticamente, armazena-las temporariamente e, por ultimo, pô-las à disposição dos internautas por determinada ordem de preferência (...)".*

atividade puramente instrumental, constitucionalmente inócua, pode, afinal, transformar-se num dragão de direitos e liberdades fundamentais.

5.3.2.Pelo contrário, a FCC adotou, recentemente, regras para uma *"open internet"*[27], que advogam a sua neutralidade – *"net neutrality"*. A sua conformidade constitucional funda-se, na explicação do Regulador, precisamente no pressuposto inverso ao consolidado pelo Tribunal de Justiça: as regras não põem causa a liberdade de expressão dos fornecedores de *internet*, uma vez que não podem ser considerados *"speakers",* mas apenas condutores da expressão dos outros[28]: *"the manner in which broadband providers operate their networks does not rise to the level of speech protected by the First Amendment",* uma vez que, enquanto operadores de telecomunicações, envolvem, por definição, *"a transmition of network users' speech without change in form or content"*.

Não obstante, o Regulador norte-americano não deixa de admitir a possibilidade inversa, de os fornecedores da *internet* serem considerados *"speakers",* aduzindo a justificação de que as regras adotadas se ajustam a um importante interesse público – *"protecting and promoting the internet and the virtuous cycle of broadband development"* -, o qual é, em seu entendimento, suficiente para superar um *"intermediate scrutiny*" de constitucionalidade. As regras adotadas seriam *"content-neutral*" e não *"content-based*", porquanto, nesse escrutínio de constitucionalidade, a questão relevante é a de saber se o Estado pode regular conteúdos, em função da sua concordância ou discordância com a mensagem neles contidos. Pelo contrário, aduz a FCC que estas regras *"are structured to operate in a such way that no speaker's message is either favored or disfavored, i.e., content neutral".* Na verdade, o que estas regras pretendem garantir é, precisamente, a livre circulação dos conteúdos e que os fornecedores de *internet* não interfiram nos acessos aos conteúdos, através da criação propositada de obstáculos, com intuitos comerciais.

[27] Na descrição da FCC, são regras fortes que protegem os consumidores de Práticas passadas e futuras que amaçam uma *"open internet",* tais como: i*) No blocking; No Throttling; No Paid Prioritization - Report and Order on Remand, Declaratory Ruling, and Order, In the Matter of Protecting and Promoting the Open Internet,* Relatório adotado pela FCC, em fevereiro 26, 2015; p. 11.
[28] *Report and Order on Remand, Declaratory Ruling, and Order, In the Matter of Protecting and Promoting the Open Internet,* Relatório adotado pela FCC, em fevereiro 26, 2015; p. 268.

## 6. INFRAESTRUTURAS CRÍTICAS, DEVER DE REPORTE E AS OMISSÕES JURÍDICO-CONSTITUCIONALMENTE RELEVANTES NA ESTRATÉGIA DA SEGURANÇA NO CIBERESPAÇO

6.1. No caso do ordenamento jurídico-constitucional português, o desenvolvimento da Estratégia Nacional de Segurança no Ciberespaço[29] poderá trazer novas preocupações, pelo menos, na ausência de uma Lei do Ciberespaço. Na verdade, alguns dos pilares da Estratégia assentam, precisamente, na subsidiariedade, complementaridade e cooperação entre públicos e privados[30]. No que concerne, especificamente, à proteção do Ciberespaço e das Infraestruturas, prevê-se o reforço *"das capacidades de prevenção, deteção e reação a incidentes de segurança do ciberespaço",* através, inclusive, da previsão de um *"dever de reporte dos operadores de infraestruturas críticas de falhas e interferências de segurança do ciberespaço nos seus sistemas",* operadores esses que poderão ser agentes privados.

Através da opção política descrita na Resolução por um dever de colaboração dos operadores privados, traduzido em dever de reporte, no caso das Infraestruturas Críticas, a intensidade das intervenções desvantajosas sobre a privacidade e as liberdades dos cidadãos poderá ser significativa. Em conformidade, é fundamental concretizar, por lei, a natureza das informações partilhadas nas várias dimensões da Estratégia de Cibersegurança, em sentido amplo, entre entidades públicos e suas congéneres, entre públicos e privados e privados e privados. A positivação desta opção política numa mera Resolução do Conselho de Ministros assume-se, de resto, jurídico-constitucionalmente irrelevante, porquanto a clarificação da natureza da responsabilidade partilhada pelos privados, correspetiva configuração e consequente definição de princípios e obrigações, integra, indiscutivelmente, a reserva de lei.

Acresce, num plano conceptual, o perigo da indefinição de conceitos, agravando a urgência da clarificação do conceito de cibersegurança (ou de segurança do

[29] Cfr. Resolução do Conselho de Ministros n.º 36/2015 - https://dre.pt/application/conteudo/67468089 - última visita em Julho 2015.
[30] Prevê-se : i) "a criação de mecanismos de reporte de incidentes de cibersegurança para entidades públicas e para os operadores de infraestruturas críticas" e ii) uma base de conhecimento que reúna informação sobre ameaças e vulnerabilidades conhecidas, para servir as entidades públicas e os operadores de infraestruturas críticas.

ciberespaço), em sentido amplo ou *stricto sensu*, por razões pragmáticas e substantivas.

i) Em termos pragmáticos, cabe definir claramente a sua articulação com a Ciberdefesa, em tempo de paz e de guerra, para evitar sobreposições e duplicações nocivas que ponham em causa fatalmente a agilidade dos processos. A indefinição terá consequências inevitáveis no plano das estruturas de liderança e no quadro de governação do ciberespaço. Por sua vez, em tempo de paz, é preciso reiterar que a sua estratégia não pode deixar de estar sujeita aos mesmos constrangimentos e compromissos assumidos no âmbito de uma Estratégia Nacional de Cibersegurança, entendida em sentido amplo. Ou seja, deverá atuar no pleno respeito do Estado de Direito Democrático, dos seus princípios e instituições fundamentais e da proteção dos direitos, liberdades e garantias.

ii) Numa perspetiva substantiva, afirma-se como uma etapa prévia incontornável a definição e consolidação doutrinária do conceito de cibersegurança (ou de segurança no ciberespaço), através da identificação rigorosa do seu objeto e, consequentemente, do âmbito de aplicação do respetivo regime jurídico. Envolvendo, por excelência, a ponderação e correspetiva concordância prática entre direitos fundamentais e valores constitucionalmente protegidos, eventualmente colidentes, é através da consolidação de um conceito material de cibersegurança ou de segurança do ciberespaço que o legislador lhe confere a robustez e blindagem devidas, por referência às credenciais constitucionais que forem consideradas suficientes para servir de fundamento a intervenções desvantajosas sobre os direitos fundamentais.

6.2. Numa perspetiva rigorosa e técnica de Direito Constitucional, tendo como premissa a ideia de que uma Estratégia Nacional de Cibersegurança não se esgota numa mera definição organizatória, a reserva de lei é, no presente domínio, constitucionalmente incontornável, atenta a fundamentalidade das matérias, direta ou indiretamente, implicadas num conceito de cibersegurança, avessas a tratamento regulamentar, conforme entendimento praticamente unânime da doutrina constitucionalista. Procedem, neste caso, as razões que fundamentam a exclusividade da atribuição da competência normativa nesta temática ao órgão a quem a ordem jurídica confere o primado do exercício do poder legislativo, que é o Parlamento. Todavia, só a partir da definição do conceito de cibersegurança, dos valores que se pretende proteger e da sua especial incidência preventiva ou repressiva, é que se torna

possível identificar, rigorosamente, o âmbito da reserva constitucional de ato legislativo.

A cibersegurança envolve, por natureza, a ponderação entre valores eventualmente colidentes, de igual proteção constitucional. No mínimo, impõe-se o reconhecimento constitucional de que a execução desta Estratégia terá impacto, jurídico-constitucionalmente relevante, nos direitos, liberdades e garantias, matéria que integra a reserva relativa da competência legislativa parlamentar [31] , independentemente da natureza da intervenção legislativa[32], encontrando-se sujeita a um apurado regime de proteção constitucional, expressamente positivado na Constituição[33]. Note-se que esta Estratégia envolve, na sua regularidade, a adopção de comportamentos positivos por parte do Estado com vista à efetividade dos direitos, liberdades e garantias dos cidadãos, cuja execução acarreta, por sua vez, afetações desvantajosas das posições jurídicas desses mesmos cidadãos. Ao legislador caberá fazer a ponderação dos direitos fundamentais com as exigências subjacentes a bens supraindividuais, como a segurança do Estado, constitucionalmente protegidos. A restrição dos direitos fundamentais, por causa da cibersegurança ou da segurança do ciberespaço, e respetivos efeitos nos direitos fundamentais ou na Segurança do Estado, exige que o legislador defina o âmbito desse conceito, no estrito respeito do princípio da proporcionalidade, sem prejuízo do reconhecimento da impossibilidade de uma regulação intensiva, fatalmente reconhecida pela doutrina e jurisprudência constitucionais.

Adicionalmente, cabe observar que, apesar de a Constituição não prever expressamente a matéria que nos ocupa, ela interliga-se, na sua previsível mas, ainda, indefinida extensão, com aspetos cuja configuração legislativa é da exclusiva

[31] Cfr. Artigo 165.º, n.º 1, alínea b) da CRP.
[32] CANOTILHO e Vital MOREIRA consideram que *"essa reserva de competência legislativa parlamentar – e implicitamente reserva material de lei – estende-se a todos os aspetos do regime dos direitos, liberdades e garantias e não apenas no caso das restrições, pois a alínea b) do art.º 168.º, número 1 (atual 165.º/n.º 1, alínea b) não discrimina".* – CANOTILHO, Gomes/MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Anotação ao artigo 18.º, p. 154; No mesmo sentido, MIRANDA defende que *"a reserva abrange os direitos na sua integridade – e não somente as restrições que eles sofram – por não fazer sentido que respeitasse ao acessório ou ao excecional (restrição) e não à substância ou ao conteúdo essencial de cada direito"*. Por outro lado, *"abrange quer um regime eventualmente mais restritivo do que o preexistente quer um regime eventualmente ampliativo; não é o alcance da lei, mas a matéria sobre a qual incide que a define".* – MIRANDA, Jorge (2010) *Manual de Direito Constitucional, Volume V*, Coimbra Editora: Coimbra; p. 378.
[33] Cfr. Artigo 18.º da CRP.

competência da AR, a qual é, neste caso, indelegável e inderrogável[34]. Acresce o facto de algumas matérias[35] carecerem da forma especial de lei orgânica[36], assumindo essa lei a natureza de valor reforçado pelo procedimento. O que, em suma, realça exigências adicionais constitucionais específicas, em termos orgânicos e formais, a somar ao regime material de proteção dos direitos fundamentais.

Cabe ainda questionar, em termos dogmáticos, se o estado de exceção, regulado expressamente na Constituição, é adequado à natureza das novas ameaças, bem como se, em termos simétricos, o plano estratégico de cibersegurança ou segurança no ciberespaço não poderá reclamar, ele próprio, ajustamentos no período de normalidade constitucional. Desde logo, não seria relevante equacionar a constitucionalização das estruturas de liderança e de governação do ciberespaço, bem como dos Serviços de Informações[37]?

6.3. Num plano substantivo, íntimo da legitimação, consideramos oportuno formular os seguintes comentários adicionais:

i) Falta, nesta Resolução, a criação de um eixo adicional que contemple, em coerência com a assunção de um compromisso político de respeito pelos direitos, liberdades e garantias dos cidadãos, a previsão de ações concretas, expressamente com esse desígnio. Pensamos que esta dimensão garantística não pode deixar de estar presente *ab initio* na Estratégia de Cibersegurança, até como fator suplementar de legitimação de atuação do Estado e do dever de colaboração dos operadores privados das infraestruturas críticas, a vingar esta opção política. Neste plano, reiteramos a necessidade de elaboração de uma Carta de Direitos dos Cidadãos para a *Internet* – um terceiro *"Bill of Rights"*.

---

[34] Do exposto, decorre que, em tudo o que possa interferir com direitos, liberdades e garantias:

a) O Governo poderá legislar através de decreto-lei, desde que obtenha a autorização legislativa exigida constitucionalmente, sob pena de inconstitucionalidade orgânica;

b) A lei de autorização legislativa deverá conter os requisitos essenciais, definidos no artigo 165.º, n.º 2 da CRP, sob pena de inconstitucionalidade material, por desvio de poder;

c) A emissão de qualquer acto de natureza regulamentar que interfira com a matéria identificada padecerá igualmente de inconstitucionalidade.

[35] Cfr. Artigo 164.º, alíneas d) e q), em conjugação com artigo 166.º, n.º 2 da CRP – Defesa Nacional, Serviços de Informações, Segredo de Estado.

[36] Cfr. Artigo 166.º, n.º 2 da CRP.

[37] Como defendemos, aliás, na conferência que proferimos sobre "***"Informações, Media e Cidadania: Para uma Cultura das Informações",*** no Curso "Informações em Democracia", promovido pelo Instituto de Defesa Nacional (IDN) em colaboração com o Sistema de Informações da República Portuguesa (SIRP).

ii) Prosseguindo no plano da Legitimação, cumpre elaborar um Estudo que retrate, com a maior fidedignidade e credibilidade tecnológica possíveis, os riscos potenciais que uma Estratégia do Ciberespaço pode importar sobre os direitos e as liberdades dos cidadãos[38]. Seria um sinal de transparência do Estado, sob reserva do tecnologicamente possível, que poderia contribuir para a própria eficácia da Estratégia de Cibersegurança, a qual não pode prescindir da colaboração de todos os agentes envolvidos.

iii) A previsão expressa das ações concretas na sobredita Estratégia poderia revelar-se um contributo inestimável, em termos de comunicação, na sua divulgação pública global, bem como ajudaria a introduzir um factor de tranquilidade junto dos cidadãos, ao longo da sua execução.

Por último, pensamos que será necessário refletir-se sobre a questão da fiscalização da aplicação da Estratégia e respetivo acompanhamento por uma autoridade administrativa independente, cuja base reflita o nosso sistema de governo semipresidencialista[39], com especial incidência no respeito dos dados pessoais dos cidadãos e das liberdades de expressão e de comunicação.

## 7. A INDEFINIÇÃO REGULATÓRIA DO CIBERESPAÇO NÃO LEGITIMA NEM CARECE DE UM *"DIREITO CONSTITUCIONAL DO INIMIGO"*[40]

7.1. Pelo exposto, não obstante o indiscutível peso de argumentos pragmáticos, eventualmente aduzidos em matéria de segurança do ciberespaço e sua regulação, não nos parece prudente uma dogmatização das questões jurídicas relevantes, em clara contraposição a uma abordagem constitucional. Na verdade, as questões do ciberespaço não podem ser relegadas para alegados quadros de exceção constitucionais, não previstos, *ex professo,* na Constituição. Insistimos que os conflitos constitucionais, imagináveis neste contexto, são suscetíveis de ser enquadrados no ambiente constitucional e, por conseguinte, as suas soluções são

[38] http://www.dhs.gov/privacy-impact-assessments - última visita em Julho de 2015.
[39] O nosso sistema de governo agrega elementos dos sistemas Parlamentaristas e Presidencialistas.
[40] Inspiramo-nos no conceito de Direito Penal do Inimigo, elaborado por JAKOBS, tendo-o adaptado aos novos desafios constitucionais do ciberespaço. Trata-se, não obstante, de um conceito que pretendemos aprofundar. – JAKOBS, Günther/MELIÁ, Manuel Cancio (2003) *Derecho penal del Enemigo*, Civitas, Madrid.

tecnicamente decantáveis por mera interpretação jurídica. As ponderações exigíveis são, em conformidade, tarefa rotineira do intérprete e do legislador democrático, habituados à concordância prática dos direitos fundamentais com outros bens constitucionalmente protegidos, mesmo a Segurança do Estado. As questões da Cibersegurança e do Ciberespaço integram, atualmente, a rotina do Estado e dos cidadãos, devendo a respetiva regulação ser desenhada a partir de um contexto jurídico de regularidade, sem prejuízo da necessidade inelutável de pontuais enquadramentos excecionais, perante a ocorrência de episódios cuja caracterização legislativa fique naturalmente sujeita à reserva do jurídico- tecnologicamente possível.

7.2. Não obstante alguma incontornável flexibilidade regulatória e o apoio de uma interpretação constitucional tecnologicamente neutra, nos termos *supra* descritos, merece-nos total repulsa uma leitura dogmática das questões do ciberespaço, contaminada por um *Direito Constitucional do Inimigo*. Em termos análogos às críticas desferidas pela doutrina ao designado *Direito Penal do Inimigo*, afigura-se-nos perigosa a generalização da tese que circunscreve a globalização a uma escolha incontornável entre um modelo de *Direito Constitucional máximo* e outro de *Direito Constitucional mínimo*[41], porquanto a função racionalizadora do Estado, perante uma eventual exigência social de regulação intrusiva, pode dar lugar a um produto que seja funcional e, ao mesmo tempo, garantístico[42]. Adaptando o raciocínio desenvolvido em sede de Direito Penal, este suposto dilema legitimaria um Direito Constitucional a duas velocidades, onde: i) na primeira, estaria representado um direito constitucional mais lesivo dos direitos, liberdades e garantias, respeitando de forma rígida os princípios politico-constitucionais mais fundamentais e ii) na segunda velocidade, referente a intervenções desvantajosas sobre direitos fundamentais menos relevantes, onde tais princípios seriam sujeitos a uma flexibilização proporcional a uma menor intensidade intrusiva. A cultura do medo não pode legitimar uma *"terceira*

[41] SÁNCHEZ, Jesús Maria Silva (2001) *La Expansión del Derecho Penal: Aspectos de la politicia criminal en las sociedades postindustriales*, Civitas, Madrid.

[42] SÁNCHEZ alude a um dilema entre um Direito Penal mínimo e um Direito Penal máximo, fundador de um Direito Penal a duas velocidades, onde: i) na primeira, estaria representada o direito penal que envolve a aplicação de penas privativas da liberdade, na qual se garantiriam de forma rígida os princípios político-criminais básicos, regras de imputação e princípios processuais e ii) na segunda velocidade, referente a penas de privação de direitos ou pecuniárias, tais princípios seriam sujeitos a uma flexibilização proporcional a uma menor intensidade sancionatória. - SÁNCHEZ, Jesús Maria Silva (2001) *La Expansión del Derecho Penal: Aspectos de la politicia criminal en las sociedades postindustriales*, Civitas, Madrid; p. 160.

*velocidade"* do Direito Constitucional, que implique consideráveis agressões aos direitos, liberdades e garantias, supostamente legitimadas por uma ampla relativização das garantias constitucionais. Uma terceira velocidade do Direito Constitucional, com estreita ligação conceptual ao designado "*Direito Penal do Inimigo"*[43], justificável, alegadamente, em certos contextos extremos, como os do terrorismo. O "*Direito Constitucional do Inimigo"* consubstanciar-se-ia na expressão de uma espécie de Direito de guerra ou de emergência, mesmo em tempo de paz, fortemente excecional, capaz de fazer face a fenómenos extraordinariamente graves[44]. Em troca, levar-nos-ia todas as liberdades.

Note-se que a relevância de uma interpretação constitucional tecnologicamente neutra, esboçada no presente artigo, reside, precisamente, no desígnio de garantir que, apesar dos desenvolvimentos tecnológicos, a lei e os seus conteúdos devidos continuam a ser vinculados e limitados pela ideia de Direito vertida na Constituição, não podendo ser absorvidos por pretextos conjunturais, ao abrigo de inexistentes e não declarados estados de exceção constitucional, alegadamente justificativos do atropelo das regras constitucionais mais firmes, para permitir respostas e reações tecnológicas rápidas e mais eficazes. Desde logo, cabe concretizar que, não obstante o impacto dos factos tecnológicos e sua eminente potência destrutiva do programa normativo-constitucional, deve manter-se: i) A repartição das tarefas de legislar, administrar e julgar e a distribuição de competências entre a Assembleia da República e o Governo legislador, a Administração e os tribunais, sufragadas pela Constituição: ii) O regime de proteção dos direitos, liberdade e garantias, nas suas dimensões orgânica, formal e material.

Não obstante, estamos convictos de que não podemos cair no erro de tudo querer regular, porquanto a incerteza inerente ao risco tecnológico torna, nalguns casos, impossível a densificação de uma posição jurídica de vantagem, suscetível de tutela regulatória ou judicialmente sindicável[45]. E não podemos, igualmente, ceder perante

[43] JAKOBS, Günther/MELIÁ, Manuel Cancio (2003) *Derecho penal del Enemigo*, Civitas, Madrid; ALLER, German (2006) "El Derecho Penal del Enemigo y la Sociedade del Conflito, in *Co-responsabilidad social, Sociedade del Riesgo y Derecho Penal del Enemigo*, Montevideo, Carlos Álvarez- Editor; pp. 163-270.

[44] SÁNCHEZ, Jesús Maria Silva (2001) *La Expansión del Derecho Penal: Aspectos de la politicia criminal en las sociedades postindustriales*, Civitas, Madrid; p. 166.

[45] GOMES, Carla Amado (2011), "Estado Social de Direito e concretização de direitos fundamentais na era tecnológica: algumas verdades inconvenientes", *Textos Dispersos de Direito Constitucional*, AAFDL: Lisboa; pp. 75 e segs.

tendências abstratas de deferência regulatória, em geral, ou judicial, sobretudo, perante tentativas de intrusão estatal nos direitos fundamentais, alimentadas pelo medo e pelo desconhecimento[46]. A emergência de novos desafios pode, efetivamente, gerar a configuração de novos direitos, eventualmente, alguns deles sob reserva do tecnologicamente possível[47]. Não se trata de desistir da sua densificação, apenas se reclama a consciencialização de que nem sempre intensidade a regulação deve ser proporcional à emergência de novos problemas. Uma interpretação constitucionalmente tecnologicamente neutra pode ajudar a fornecer a medida entre liberdade e regulação.

Sem prescindir das potencialidades curativas e rejuvenescedoras de uma operação interpretativa, fiel ao programa normativo, que recorra ao método jurídico, e se contenha no perímetro de uma interpretação constitucional tecnologicamente neutra, é nosso dever concluir a presente reflexão com um alerta pragmático aos cultores do direito constitucional e, em última análise, ao legislador de revisão constitucional. Urge, efetivamente, fazer um *check-up* da Constituição, perante os desafios emergentes da regulação constitucional da *internet* e do ciberespaço. Em especial, perscrutar a eficácia dos meios anteriormente escolhidos para: i) conferir efetividade aos direitos e liberdades, suscetíveis de sofrerem maiores agressões; ii) garantir que os instrumentos constitucionais previstos para fazer face a situações de emergência se encontram ajustados aos novos desafios do ciberespaço. Urge conferir princípios e balizar novos métodos e modelos regulatórios, substantivos e institucionais. O importante é evitar que uma eventual Constituição tecnológica, invisível e não oficial, a breve trecho, neutralize a Constituição positiva e oficial dos Direitos, Liberdades e Garantias, com o pretexto da sua falta de efetividade. Desnecessariamente.

[46]LESSIG, Lawrence, (1996) "Reading the Constitution in Cyberspace", *45 Emory*, L. J., number 3: p. 6.

[47] GOMES, Carla Amado (2011), "Estado Social de Direito e concretização de direitos fundamentais na era tecnológica: algumas verdades inconvenientes", *Textos Dispersos de Direito Constitucional*, AAFDL: Lisboa; pp. 75 e segs.

CYBERLAW by CIJIC

# INTERNET EXCEPTIONALISM: AN OVERVIEW FROM GENERAL CONSTITUTIONAL LAW

**MARK TUSHNET** [1]

[1] *William Nelson Cromwell Professor of Law, Harvard Law School. I thank Rebecca Tushnet for comments on a draft of this Article, and Andrea Matthews for valuable research assistance.*

**Please note:** This article was first published by William & Mary Law Review, Volume 56, Issue 4, April 2015. Upon request made by the Editor of the scientific magazine, «*Cyberlaw by CIJIC*»- to Professor Mark Tushnet, this article was kindly provided by its author and by his publisher, to be object of republishing, within the scope of it, by «Cyberlaw by CIJIC». Either its «Abstract» and «Resumo» were, after, added to the original article. «Resumo» by Nuno Teixeira Castro and Mark Tushnet.

**SUMMARY: INTRODUCTION; 1. WHY—OR WHY NOT—INTERNET EXCEPTIONALISM: SOME PRELIMINARY OBSERVATIONS; 2. STRATEGIES FOR DEVELOPING A "LAW OF THE INTERNET UNTO ITSELF"; 3. THE INTERNET'S DISTINCTIVE "NATURES, VALUES,[AND]ABUSES"; 4. SOME ADDITIONAL QUALIFICATIONS;**

**5. CONCLUSION**

## RESUMO


A natureza, os valores e os *perigos* da Internet justificarão por si só o «*excecionalismo da Internet*»? Ou será que justificarão a aplicação da doutrina da Primeira Emenda com *apropriados* ajustes? Os argumentos em torno desta natureza distinta, dos valores e dos *perigos* da Internet comportam apenas premissas frágeis.

A deferência judicial sobre escolhas legislativas exigiria uma deferência própria a um regime legislativamente escolhido do «excepcionalismo da Internet». Porém, em reflexão, afirmar tal constituíria uma falácia, uma vez que a "deferência judicial" deverá ser erigida sobre a análise de uma regulação específica e não generalizada sobre toda a regulação.

Em vez de "Excepcionalismo da Internet ou doutrina geral da 1.ª Emenda ajustada?", deveríamos, em jeito de lição, colocar a questão nos seguintes moldes: "Excepcionalismo da Internet ou doutrina geral da 1.ª Emenda ajustada em relação a esta regulação específica deste problema em concreto?"



**Palavras-Chave:** 1.ª Emenda; Liberdade de expressão, «*Excecionalismo da Internet*»; Deferência jurisdicional; Regulação

## ABSTRACT

Do the Internet's nature, values and dangers justify Internet exceptionalism? Or do they justify only the application of standard First Amendment doctrine with appropriate tweaks? Arguments about the Internet's distinctive nature, values and dangers support only a rather weak conclusion.

Judicial deference to legislative choices would require deference to a legislatively chosen regime of Internet exceptionalism. On reflection, though, saying so would be mistaken because the "judicial deference" concern is built into the analysis of specific regulations and cannot be generalized across regulations.

One lesson to consider should be, to the question: "Internet exceptionalism or standard doctrine with tweaks?", instead we should pose: "Internet exceptionalism or standard doctrine with tweaks in connection with this specific regulation of this specific problem?"

**Keywords:** First ammendment; Freedom of expression; Internet exceptionalism; Judicial deference; Regulation;

## INTRODUCTION:

This Article considers First Amendment Internet exceptionalism. I use that term in what I think is a reasonably standard way to refer to the question of whether the technological characteristics of the Internet (and, more generally, twenty-first-century information technologies) justify treating regulation of information dissemination through the Internet differently from regulation of such dissemination through nineteenth- and twentieth-century media, such as print, radio, and television. My aim here is not to provide an answer to that question, but to identify several subquestions whose answers must be part of the larger answer.

I begin with a disclaimer. After thinking and writing about general constitutional law and theory for many years, I began to think about the First Amendment relatively recently, and about the implications of that Amendment for the Internet even more recently. With so much specialized writing about the Internet and the

First Amendment already produced, I should note that my reflections on the possibility of Internet exceptionalism might simply be reinventing the wheel—that is, discussing in quite summary form matters that have been discussed in more detail elsewhere[1]. The fact that the term "Internet exceptionalism" is well known in the field indicates that much has indeed been said about the questions I discuss here[2]. Still, I have not found a crisp statement presenting many of the matters I find of interest in a single place, so the Articlemay have some value as such a compilation even if it is not all that original.

Coming to the topic from general constitutional theory and law, I believe that I am somewhat more sensitive than most of those who write on the subject to the question that pervades the entire field. That is the question of the appropriate degree

[1] Further, in my discussions of doctrine in this Article, I offer rather summary versions of what I believe to be the best understanding of current doctrine, without dealing with a rather large number of qualifications that a more complete treatment would add to deal with a fair number of cases that do (in my view) little more than add some bells and whistles to the core doctrines.

[2] ALEXIS search for "Internet exceptionalism" conducted on September 10, 2014, recovered forty-nine items. *See, e.g.*, Mark McCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037, 1040 (2010) ("[I]nternet exceptionalism is still a widely held viewpoint."). Because this is a short Article, I do not address in detail the many good articles dealing with both discrete subissues that arise in connection with Internet exceptionalism, or those dealing expressly with Internet exceptionalism as such. My sense is that the issues I address here have typically been embedded in arguments focused on more detailed questions.

or form of judicial deference to legislative regulatory interventions, whether those interventions occur in the material economy or in the information economy. Not surprisingly, scholars who focus almost exclusively on the Internet and the First Amendment, to the exclusion of general constitutional theory and law, simply assume that relatively intrusive judicial supervision of regulatory decisions dealing with the information economy is appropriate[3]. To the extent that the scholarship adverts to the question of judicial deference, I believe that it tends to assume that the question is adequately answered by referring to Footnote Four of *United States v. Carolene Products*[4] and the scholarship of John Hart Ely[5]. My view is that such an assumption is not warranted. I defend this view only indirectly by attempting to identify why and how the question of judicial deference is a complex one[6].

After the description in Part I of some general questions about the structure of constitutional doctrine, Part II examines two strategies that courts have used to deal with technological innovations— one allowing legislative experimentation until experience accumulates, the other imposing existing (or what I call "standard") doctrine from the outset. Part III looks at some attributes that are said to distinguish the Internet from traditional media—norms, scope, cost, and anonymity—with the aim of mapping out how or when Internet exceptionalism might be justified. Part IV discusses several general qualifications to the preceding analysis, involving doctrinal structure yet again, the First Amendment's bearing on regulation of business models, and the state action doctrine. Finally in a brief conclusion, I suggest that framing the discussion as one about Internet exceptionalism in a broad sense is misleading.

[3] For a somewhat more extended version of this point, see Mark Tushnet, *Introduction: Reflections on the First Amendment and the Information Economy*, 127 HARV. L. REV. 2234, 2237 (2014). There I argue that most scholars who write about the First Amendment "like" the Amendment, meaning that they favor relatively broad limitations on legislative power dealing with speech. For myself, I neither like nor dislike the First Amendment in that sense.

[4] 304 U.S. 144, 152 n.4 (1938).

[5] *See, e.g.*, JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW (1980).

[6] A short general version of my position is this: Footnote Four and Ely are concerned with regulations that, in Ely's terms, threaten to block the channels of political change. *See id.* at 105 ("Clearing the Channels of Political Change"). But, not all regulation of information dissemination poses such a threat. A more disaggregated analysis of the targets of regulation, one that attends to the extent to which those targets do in fact have much, if anything, to do with enabling political change, is required. For an extended essay on this topic, see Mark Tushnet, *Art and the First Amendment*, 35 COLUM. J.L. & ARTS 169 (2012).

## 1. WHY—OR WHY NOT—INTERNET EXCEPTIONALISM: SOME PRELIMINARY OBSERVATIONS

Considering the use of sound amplifying equipment by trucks cruising city streets to disseminate a political message, Justice Robert Jackson wrote, "The moving picture screen, the radio, the newspaper, the handbill, the sound truck and the street corner orator have differing natures, values, abuses and dangers. Each, in my view, is a law unto itself.[7]" To that, we can now add the Internet. So, for example, the cost of distributing information, whatever its nature, over the Internet is much lower than the cost of doing so in other media, particularly when the distributor uses one of the various social networks as an intermediary. It is somewhat easier to distribute information "anonymously" over the Internet in the sense that the steps one must take to identify the speaker may be more complicated or "techy" than the steps one must take to identify the person responsible for a leaflet or television advertisement.

Justice Jackson's observation rests on a proposition about the form that First Amendment doctrine takes[8]. For him, the constitutionality of specific regulations depends upon an assessment of "values, abuses and dangers"—that is, on what his generation would have called a balancing of interests and what today might be called a determination of the regulation's proportionality[9]. Whether that form was the correct one was contested at the time, with Justice Hugo Black notably asserting that First Amendment doctrine should be more categorical[10], and is even more contested today[11]. My argument in this Part is that the alternative forms of regulation—categorical rules or balancing tests—can be indistinguishable in practice, at least

[7] Kovacs v. Cooper, 336 U.S. 77, 98 (1949) (Jackson, J., concurring).

[8] A note about originalist approaches to the interpretation of the First Amendment seems appropriate. To state the conclusion of a complex argument: originalists must deal with the issues of balancing versus categorical approaches as they pursue their inquiries, though the discourse of originalism has developed its own terms to refer to balancing and categorical approaches.

[9] The primary expositor of proportionality analysis, including in connection with the First Amendment, is Justice Stephen Breyer. For a discussion of Justice Breyer's First Amendment jurisprudence, see Mark Tushnet, *Justice Breyer and the Partial Dedoctrinalization of Free Speech Law*, 128 HARV. L. REV. 508 (2014).

[10] *See, e.g.*, Smith v. California, 361 U.S. 147, 157 (1959) (Black, J., concurring) ("I read 'No law ... abridging' to mean *no law abridging*.").

[11] *See* United States v. Stevens, 559 U.S. 460, 470 (2010) ("The Government thus proposes that a claim of categorical exclusion should be considered under a simple balancing test: 'Whether a given category of speech enjoys First Amendment protection depends upon a categorical balancing of the value of the speech against its societal costs.' As a free-floating test for First Amendment coverage, that sentence is startling and dangerous." (citations omitted)).

when each is done carefully. Essentially, a welldesigned set of categorical rules will identify a large range of characteristics whose presence in varying degrees triggers the application of discrete rules within the set, and well-performed balancing will take precisely those same characteristics into account and give them appropriate weights in generating outcomes.

For analytical clarity, we should pry apart the two elements Justice Jackson combined. We might want to develop separate rules for each medium of information dissemination, or we might apply a general balancing or proportionality test to every medium. We might call the rule-based approach one of Internet exceptionalism[12] and the balancing approach a unitary account of the First Amendment.

Balancing can produce the following outcome: a regulation that would be constitutionally impermissible if invoked against print media would be constitutionally permissible when invoked against Internet dissemination[13]. That might *look* like Internet exceptionalism on the level of outcomes, but it would result from a unified approach to First Amendment problems.

One might think that a rule-based analytic approach could not have similar distinct results. Professor Jim Chen provides a useful formulation, in his discussion of regulation of Internet intermediaries, which he calls conduits: "Conduit-based regulation of speech is a constitutional mirage....Conduit-based regulation raises precisely the same issues as all other decisions reviewable under the First Amendment[14]." *Reno v. ACLU* exemplified this approach by applying existing rule-based doctrines in a challenge to the constitutionality of the Communications Decency Act (CDA), which restricted the distribution of some sexually explicit but nonobscene materials via the Internet[15]. According to the Court, "the CDA is a content-based blanket restriction on speech, and, as such, cannot be 'properly analyzed as a form of time, place, and manner regulation.'[16]"

[12] Note that when transforming Justice Jackson's approach into a categorical one, we might develop—as indeed some suggest we have—"broadcast" exceptionalism, "movie" exceptionalism, and even "book" exceptionalism.
[13] And vice versa: a constitutionally permissible regulation of the print media might be constitutionally impermissible if applied to dissemination on the Internet.
[14] Jim Chen, *Conduit-Based Regulation of Speech*, 54 DUKE L.J. 1359, 1450 (2005).
[15] 521 U.S. 844 (1997)
[16] *Id.* at 868 (citations omitted).

Yet, as Chen observes immediately after stating the general point, "distinct conduits raise distinct regulatory concerns, ranging from strictly physical characteristics to economic predictions regarding markets that exploit that conduit. Persuasive free speech jurisprudence considers differences of this sort.[17]" So, we would apply existing, pre-Internet doctrine (no Internet exceptionalism), but with some adjustments, or "tweaks," to take account of the Internet's distinct characteristics (Internet exceptionalism)[18]. And, as I suggested at the outset, the choice of doctrinal structure need have no impact on the outcomes generated. Internet exceptionalism and standard doctrine with tweaks could produce the same "rules.[19]"

## 2. STRATEGIES FOR DEVELOPING A "LAW OF THE INTERNET UNTO ITSELF"

Here I identify two general strategies[20] for following Justice Jackson's advice to think about a law of the Internet unto itself.

### *A). Allowing a Period of Policy Experimentation*

*In Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, Justice John Paul Stevens wrote, "At this early stage in the regulation of this developing industry, Congress should not be put to an all-or-nothing choice.[21]". The thought here is that individual technological innovations implicate an array of dangers and constitutional values, and that neither legislatures nor courts have any special insights, relative to the other, about the constitutionally appropriate response when the innovations have just been introduced. This counsels in favor of deference to

[17] Chen, *supra* note 14, at 1450; *see also* Richard Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1006 (2000) ("[T]he advent of cyberspace may raise the stakes, but it hardly follows that it also changes the correct solutions.").

[18] I note that the possibility that balancing and rules-based approaches will in practice result in the same outcomes is a general characteristic of those approaches, not specific to the First Amendment. *See* MARK TUSHNET, ADVANCED INTRODUCTION TO COMPARATIVE CONSTITUTIONAL LAW 73 (2014) (arguing that proportionality and rules-based approaches can be extensionally equivalent).

[19] I use the scare quotes here to indicate that the formulation does not entail a commitment to a "categorical rules" structure.

[20] I distinguish between interpretive methods such as balancing or rules, and strategies for implementing either of those methods.

[21] 518 U.S. 727, 769 (1996) (Stevens, J., concurring).

democratically responsible decision making or, as Justice Stevens put it, deference to congressional choices. But, as experience with the innovation and with policy experiments accumulates, legislators and judges learn more about specific dangers and how regulatory responses implicate constitutional values. Our constitutional system assumes that at some point judges' comparative advantage in implementing constitutional values in an informed way kicks in, and restrictive judicial doctrine can develop[22].

The pattern of judicial deference to legislative choice followed after some time by the development of judicial constraints on experimentation is common[23]. In the early years of motion pictures, the Court held that movies were mere "spectacles" and, for that very reason, movies were fully regulable without regard to the First Amendment[24]. Decades later, after society had become accustomed to movies, the Court applied standard First Amendment doctrine to their regulation[25]. There were similar results with radio[26] and cable television[27]. Writing in 1996—relatively late in the development of cable television as a communications technology—Justice David Souter observed, "All of the relevant characteristics of cable are presently in a state of technological and regulatory flux.[28]" For him, that justified refraining from

[22] For a good overview of the historical development of First Amendment doctrine with respect to several media technologies, see Robert Corn-Revere, *The First Amendment and the Electronic Media*, FIRST AMENDMENT CTR. (Nov. 20, 2002), http://www.firstamendmentcenter.org/internet-first-amendment-overview [http://perma.cc/QNU3-CPUF].

[23] *Cf.* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) (noting that in a case involving pager technology and instant messages, "[t]he Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear," and referring to the Court's "own knowledge and experience" in developing doctrine).

[24] Mut. Film Co. v. Indus. Comm'n, 236 U.S. 230, 243-44 (1915).

[25] Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 502 (1952).

[26] *Compare* Turner Broad. Sys. v. FCC, 512 U.S. 622, 637-39 (1994) (discussing the evolution of First Amendment doctrine dealing with broadcasting), *with* Nat'l Broad. Co. v. United States, 319 U.S. 190, 227 (1943) ("The right of free speech does not include, however, the right to use the facilities of radio without a license.").

[27] *Compare Turner Broad. Sys.*, 512 U.S. at 660-61 (applying intermediate First Amendment scrutiny to some cable regulations), *with* FCC v. Midwest Video Co., 440 U.S. 689, 709 n.19 (1970) (finding it unnecessary to resolve the question of what First Amendment standard was applicable to a regulation of cable television).

[28] Denver Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727, 776 (1996) (Souter, J., concurring). Professor Christopher S. Yoo refers to *Denver Area* as "experiment[ing] with alternative rationales for subjecting cable operators to a lower level of First Amendment scrutiny." Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 750 (2010).

"announc[ing] a definitive categorical analysis" to deal with the problem at hand[29]. The Court is similarly new to the technologies associated with the Internet[30].

This strategy would direct one to a form of Internet exceptionalism, at least for some period. But, it is worth emphasizing that the strategy need not lead to a state of permanent exceptionalism. As experience accumulates, judges should be in a position to assimilate regulations of now not-so-new technologies to the general body of First Amendment doctrine, perhaps, as suggested earlier, with some tweaks to deal with truly distinctive features of the technology.

### ***B). Drawing Inferences from the History of First Amendment Treatment of Technological Innovations***

*In the same case about cable regulation in which Justice Souter* defended deference to regulatory experiments, Justice Anthony Kennedy saw the problem differently: "When confronted with a threat to free speech in the context of an emerging technology, we ought to have the discipline to analyze the case by reference to existing elaborations of constant First Amendment principles.[31]" That "discipline" arises from the very experience that the first strategy allows to accumulate.

The first strategy counsels deference to regulatory experimentation with each until experience accumulates about that particular technology, at which point the courts can be confident about imposing First Amendment constraints on further experimentation. The first strategy, that is, hopes for wisdom to emerge from the accumulation of experience *within* each technology. Proponents of the second doctrine argue that we can also accumulate experience *across* technologies. They observe the course of doctrinal development about movies, radio, television, and cable, and note that there is a thread running through each area: initial deference followed by the application of standard First Amendment doctrine[32]. Medium exceptionalism is regularly replaced by general First Amendment law. So, for

[29] *Denver Area*, 518 U.S. at 775 (Souter, J., concurring.)
[30] According to Judge M. Margaret McKeown, between 1996 and 2012, the Supreme Court mentioned the Internet in seventeen cases, and "only seven were actually about the Internet." M. Margaret McKeown, *The Internet and the Constitution: A Selective Retrospective*, 9 WASH. J.L. TECH. & ARTS 135, 152 (2014).
[31] *Denver Area*, 518 U.S. at 781 (Kennedy, J., concurring in part, concurring in the judgment in part, and dissenting in part).
[32] *See supra* Part II.A.

example, movies were first outside the First Amendment, then fully within it[33]; the standard for regulating cable television was first left undefined, then controversially became subject to intermediate scrutiny, with strong voices arguing for the application of the usual rules for content-based regulations[34]. So, for proponents of the second strategy, existing doctrine has resulted from considering each technology separately, and yet a uniform doctrine has emerged. They infer, from experience, that we would profit from short-circuiting the deference-to-standard-doctrine pathway whenever legislatures attempt to regulate a new communication medium. We are going to get to standard doctrine eventually, and, they ask, why should society incur the interim costs of regulations that, in retrospect, will seem unconstitutional?

I do not propose to offer any observations about which strategy makes more sense. I note, though, that both strategies rely on experience; the first within technologies, the second across them. That signals a more general issue in connection with drawing inferences from experience, which is that we have to decide what is the domain (or, as it is sometimes put, what is the "reference class") of the relevant experience. My sense is that the choice of domain is driven by the analyst's prior commitments: First Amendment "mavens" will look across technologies, First Amendment skeptics—meaning, those who are skeptical about aggressive judicial review of decisions by democratically responsible legislatures—will look within technologies[35]. If so, identifying the two strategies may help us understand the structure of debates about Internet exceptionalism, but will not help us come to a judgment about which side has the better case.

[33] *See supra* notes 25-26 and accompanying text.
[34] *See supra* notes 28-30 and accompanying text.
[35] In comments on a draft of this Article, Rebecca Tushnet suggested that First Amendment skeptics may also look across technologies, sometimes finding reasons *against* their skepticism in connection with the dissemination of some categories of material through one technology, but thinking those reasons unavailing in connection with dissemination through another. An example, though rejected by the Supreme Court, might be the thought that regulation of obscene *films* might be justified even though regulation of words-only obscenity would not be. For the Court's rejection of that proposition, see *Kaplan v. California*, 413 U.S. 115, 118-19 (1973).

## 3. THE INTERNET'S DISTINCTIVE "NATURES, VALUES, [AND] ABUSES"

What would Internet exceptionalism, either because of the Internet's distinctive characteristics, or standard doctrine with tweaks to take account of those characteristics, look like? Justice Jackson's suggestion is that we should examine how the Internet differs from traditional media with respect to its potential values and abuses[36]. But, the real question is somewhat different—not what the differences are in some ontological sense, but rather this: to what extent should courts in determining a regulation's constitutionality defer to a reasonable legislative judgment about those values and abuses? This is the real question because legislatures enact regulations predicated on their judgments that each regulation is a constitutionally appropriate response to what they understand to be the Internet's distinctive values and abuses[37].

Consider some possible regulation of cyberstalking[38]. Physical stalking is regulable because it induces fear in its victims and can induce them to take costly protective measures (and because physical stalking is not, in general, an expressive activity covered by the First Amendment or, at least, consists of action "brigaded with" words, to invert Justice Douglas's formulation)[39]. Cyberstalking takes the form of words and images that induce fear[40]. Existing doctrine deals with words that induce fear under the doctrinal heading of "threats," and the First Amendment allows punishment of such words only if they constitute a "true threat.[41]" One issue that arises in connection with true threats under standard doctrine is whether an utterance is a true threat only when the threatener subjectively intends to carry out the threat

[36] *See supra* note 8 and accompanying text.
[37] In framing the issue in this way, I begin with the assumption that we should be thinking in the first instance about regulations specifically targeted at the dissemination of information over the Internet, and not about the application of general regulations of speech to the Internet as well as other media. The issue of deference to legislative judgments arises most clearly in connection with such targeted regulations. I note, though, that the issue of deference to legislative judgment arises in only a slightly different form with respect to general regulations properly interpreted to apply to the Internet.
[38] In the discussion that follows I do not discuss any specific regulation, and in particular I do not discuss whether some such regulation might be unconstitutionally vague or unconstitutionally overbroad. I note, though, that the standard for determining acceptable unclarity or breadth might depend on a prior judgment about whether Internet exceptionalism (or a tweak to standard doctrine) is appropriate. My sense is that many invocations of vagueness or overbreadth doctrine in the context of Internet regulation rely without analysis on the proposition that what is vague or overbroad with respect to traditional media is necessarily vague or overbroad with respect to Internet regulation. However, that is precisely what is at issue.
[39] Brandenburg v. Ohio, 395 U.S. 444, 456 (1969) (Douglas, J., concurring).
[40] Nisha Ajmani, Comment, *Cyberstalking and Free Speech: Rethinking the* Rangel *Standard in the Age of the Internet*, 90 OR. L. REV. 303, 304 (2011).
[41] Watts v. United States, 394 U.S. 705, 707-08 (1969).

when the occasion for doing so arises, or whether an utterance is a true threat when a reasonable recipient would be put in fear[42]. When a legislature adopts a regulation of cyberstalking that goes beyond its general regulation of threats, it implicitly (or perhaps even explicitly) determines that the dissemination of threatening words to victims over the Internet is distinctively harmful—perhaps, for example, because it is easier to ensure that threatening words reach the victim via the Internet than via traditional media. It seems (to me—and so, I think, could reasonably seem to legislators) more likely that a victim will become aware of a threatening Facebook posting than of a classified advertisement. And, the cost of posting on Facebook is lower than the cost of mailing a threatening letter to the victim. In enacting the cyberstalking statute, the legislature has made a judgment about the relative ease of communicating a threat via the Internet. Assume that that judgment is a reasonable one. Should a judge say, though, that the greater ease is not "large enough" to justify distinctive regulation? The answer to that question depends in large part on one's account of the deference judges should give to legislative judgments[43].

With the issue of judicial deference in hand, I turn to several of the characteristics typically invoked in discussions of whether there should be Internet exceptionalism. I depart from what I think is the usual order of presentation, in which scope, cost, and anonymity are said to distinguish the Internet from other media, and begin with norms.

### ***A). Internet Norms Are Fluid or Nonexistent***

The fact that in practice anyone can use the Internet as a platform for distributing ideas and information means that it is nearly impossible to generate widely adhered-to norms of appropriate behavior[44]. The well-known cartoon with the caption, "On the Internet, nobody knows you're a dog" is a comment not only about the anonymity the Internet affords, but on the fact that nothing—name, reputation, or any other norm—vouches for what appears on the Internet[45]. The existence of

[42] The issue is pending before the Supreme Court in *Elonis v. United States*, No. 13-983 (U.S. argued Dec. 1, 2014), a case involving cyberstalking but prosecuted under a general threat statute. *See supra* note 38 (discussing the distinction between Internet-targeted and general regulations).

[43] My experience, for what it is worth, is that men tend to think that the greater ease of disseminating threats is not large enough, whereas (some) women think that it is.

[44] I qualify this observation later, in my discussion of the question of intermediaries'First Amendment rights.

[45] The implication is captured in the subtitle of a play by Alan David Perkins: "Nobody Knows I'm a Dog: Six People; *Six Lies*; One Internet." Alan David Perkins, *Nobody Knows I'm a Dog* (1995),

"comment trolls," and even the existence of a term for the phenomenon, shows that there are as yet no real constraining norms of Internet behavior, as does Godwin's Law[46].

Norms may arise within discrete communities, and some of those communities might be quite large. Yet, it is in the Internet's "nature," to use Justice Jackson's term, that material circulated within a community and conforming to its norms will leak into other communities with other, perhaps more restrictive norms[47]. So, for example, one can readily imagine a subcommunity on the Internet whose members regularly use, and are not offended by, extremely crude and sexually explicit language. Members of other subcommunities who come upon that language might be offended—or, in some cases, psychologically and even materially injured—by it.

More consequential is the question of treating bloggers as members of the news media. That question arises in connection with statutes creating reporters' privileges to conceal their sources from inquiry or to get access to locations closed to members of the general public[48]. Professor Sonja West, defending special rules for "the press," offers a definition that is in part implicitly norm based. For her, one component of the definition involves "[t]raining, [e]ducation, or [e]xperience" in the field[49]. Although she does not develop the justification in detail, it appears that training and experience matter because they are methods by which a person becomes acculturated to the field's norms[50].

Norms or their absence may matter for the issue of Internet exceptionalism because standard First Amendment doctrine may rest on a judgment that norms—of newspapers, broadcasters, and the like—have developed to restrict harmful actions to some significant degree. The New Zealand Court of Appeal noted the importance of

---

http://www.alandavidperkins.com/nkiad/ [http://perma.cc/3KV6-SXA8]; *see also* Michael Cavna, *"Nobody Knows You're a Dog": As Iconic Internet Cartoon Turns 20, Creator Peter Steiner Knows the Joke Rings as Relevant as Ever*, WASH. POST (July 31, 2013, 11:35 AM), http://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-asiconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-asever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html [http://perma.cc/3YZPBRBB] (discussing the continuing relevance of the cartoon).

[46] Godwin's Law asserts, "As an online discussion grows longer, the probability of a comparison involving Nazis or Hitler approaches one." Mike Godwin, *Meme, Counter-meme*, WIRED, (Oct. 1994), http://archive.wired.com/wired/archive/2.10/godwin.if.html [http://perma.cc/F6R9-U7YW].

[47] Kovacs v. Cooper, 336 U.S. 77, 97-98 (1949) (Jackson, J., concurring).

[48] For a recent discussion, see Sonja R. West, *Press Exceptionalism*, 127 HARV. L. REV. 2434 (2014).

[49] *Id.* at 2459.

[50] *Cf. id.* at 2460 (referring to "independent journalistic activity"in connection with these elements).

norms for developing the rules to be applied in cases involving false statements about public figures: "New Zealand has not encountered the worst excesses and irresponsibilities of the English national daily tabloids[51]." Because the New Zealand press was "responsible," imposing liability relatively unrestrictedly would not have had significant effects on how the New Zealand press disseminate information[52]. When norms operate to limit the damage done across a wide range of information distribution, only normative outliers will engage in harmful dissemination of information and ideas. And perhaps standard First Amendment doctrine assumes that these normative outliers will be few, in part because markets will constrain behavior because relatively few consumers would purchase what the outliers were selling, with the result that the harm they cause will be small. Finally, with few normative outliers, attempting to control their behavior by law (norms having failed) might have undesirable effects on those who generally adhere to appropriate norms[53].

Internet exceptionalists might suggest that a world without norms is different from the world in which standard First Amendment doctrine developed. By definition, there are no outliers, ready access to the Internet means that large numbers of "unsocialized" speakers will in fact distribute ideas and information, and the size of the market coupled with relatively low costs of dissemination means that (to overstate a bit) anyone can make a living by disseminating anything. The resulting harm might[54] be large enough to justify regulations of the normless Internet world that would be impermissible for the norm-pervaded world of traditional media.

Perhaps the Internet is now normless. But, things could change and norms could develop to regulate substantial amounts of the information distribution on the Internet informally, without legal intervention[55]. An Internet exceptionalist might rely on that observation to support the pursuit of the first regulatory strategy, allowing

[51] *Lange v Atkinson* [2000] 3 NZLR 385 (CA).
[52] Although the court was developing the common law in a system without judicially enforceable constitutional protection of free expression, the court clearly understood that the common law should be developed in ways responsive to the values of free expression.
[53] This is what motivates concern for the "chilling effect" of regulations: even those who comply with the regulations may fear that they will have to defend their actions at some cost and risk being held liable as a result of what are analytically mistaken applications of the regulations.
[54] The word "might" here flags once again the question of judicial deference to legislative judgments.
[55] Section 230 loosens legal regulation in part to encourage the development of norms by protecting intermediaries against state tort law liability for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." 47 U.S.C. § 230(c)(2)(A) (2012).

experimentation with regulation until experience accumulates about whether or the extent to which acceptable norms come to characterize behavior on the Internet[56]. One might wonder, though, about the possibility that norms could develop so that judges could eventually enforce constraints on legislative experimentation pursuant to the first strategy. The issues of scope and cost, discussed next, may be both part of the Internet's nature and important causes of normlessness on the Internet. If so, norms will never develop. An Internet exceptionalist might conclude that courts should never attempt to constrain legislative experimentation with Internet regulation, although that conclusion is in some tension with the rhetoric typically associated with the first strategy. And, once again in contrast, the proponent of applying standard First Amendment doctrine to the Internet might give permanent normlessness as the very reason for following the second strategy.

### ***B). The Internet Is a Bigger and Better System for Amplifying "Sound"***

*Consider the classic First Amendment case Debs v. United States*[57]. Eugene V. Debs, a powerful orator, made an antiwar speech and was prosecuted for interfering with the war effort[58]. The Court upheld his conviction[59], but under a doctrine it has since repudiated[60]. One reason—not the only one, I emphasize—is that the risk was relatively low that Debs's speech would actually lead to interference with the war effort. His audience was a small fraction of the national population, so even if he persuaded some listeners to act on what he said, not much damage to the war effort would occur. Give Debs a bigger bullhorn—that is, a means of disseminating his message much more widely—and the risk of actual harm increases[61]. As the Court put it in *Reno v. ACLU*, "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther *than it could from any soapbox.*[62]"

---

[56] *Cf.* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) ("[I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of *new* and available devices." (emphasis added)).
[57] 249 U.S. 211 (1919).
[58] *Id.* at 212-14.
[59] *Id.* at 216-17.
[60] Brandenburg v. Ohio, 395 U.S. 444, 449-50 (1969) (Black, J., concurring) ("[T]he 'clear and present danger' doctrine should have no place in the interpretation of the First Amendment.").
[61] *Cf.* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 13 (2006) (referring to "the exponential increase in the number of speakers with potential access to broad audiences").
[62] 521 U.S. 844, 870 (1997) (emphasis added); *see also* United States v. Am. Library Ass'n, 539 U.S. 194, 207 (2003) ("As Congress recognized, '[t]he Internet is simply another method for making

*United States v. White* presents a variant on the "bigger bullhorn" argument[63]. The defendant operated a white supremacist website, with many postings praising assassinations and other violent acts, and often identifying people who, White said, deserved to be killed[64]. He posted detailed information on his website, including the name, address, and phone numbers of the foreperson of a jury that convicted another white supremacist of soliciting harm to a federal judge (the judge's husband and mother had been murdered, though not by the defendant in the case over which she presided)[65]. White was charged with soliciting a violent crime against the juror[66]. The court of appeals held that White did not have a valid First Amendment defense: "Though the government did not present a specific "solicitee" it was unnecessary to do so given the very nature of the solicitation—an electronic broadcast which, a reasonable jury could conclude, was specifically designed to reach as many white supremacist readers as possible so that *someone* could kill or harm Juror A[67].

There are of course distinctions between *Debs* and *White*[68]. Yet, both involved a risk that someone would commit a crime as a result of listening to (or viewing) some words and images. The court of appeals's reference to "as many white supremacist readers as possible" suggests that imposing liability on White was constitutionally permissible because he had a particularly susceptible readership large enough to make the risk that violence would occur significant enough to support regulation[69].

Internet exceptionalism would allow legislatures to make the judgment that the substantially larger audience available for communications over the Internet increases otherwise acceptable levels of risk beyond a tolerable threshold. Proponents of applying standard First Amendment doctrine would disagree. They might argue, for example, that the concern in standard First Amendment doctrine is not with the size of risk, but the mechanisms by which risk is realized. *Brandenburg v. Ohio* holds that a person can be convicted of uttering words that increase the risk of violence only if—

---

information available in a school of library.' It is 'no more than a technological extension of the book stack.'" (citations omitted)).

[63] 698 F.3d 1005 (7th Cir. 2012).

[64] *Id.* at 1009.

[65] *Id.* at 1009-10.

[66] *Id.* at 1010.

[67] *Id.* at 1016.

[68] Primarily, that the crime in *Debs* was not a specific intent crime, whereas the crime in *White* was. *See id.* at 1012 (quoting the jury instruction requiring that the government must prove beyond a reasonable doubt "with strongly corroborative circumstances, that the defendant intended for another person to commit a violent federal crime").

[69] *See id.* at 1010.

among several other criteria—the words are words of "incitement.[70]". The theory is that such words bypass the listener's deliberative capacities, effectively turning the listener into a weapon in the speaker's hands rather than an autonomous decision maker. The broader First Amendment theory on which *Brandenburg* rests, according to one prominent account, is that the First Amendment bars liability for harm that results when a speaker persuades someone else to take unlawful action[71].

In addition, one might note that just as the risk of resulting harm increases, perhaps dramatically, as the size of the audience increases when material is distributed over the Internet, so does the harm caused by suppressing the distribution of that material. Shutting down White's website, for example, prevents the rest of us from learning about the positions being taken by real white supremacists. Which is the more important risk? Here too the general issue of deference to legislative judgments arises. Saying that judges should apply standard First Amendment doctrine implies that judges rather than legislatures should decide what the balance of risks should be.

### ***C). Disseminating Information over the Internet Is Dramatically Less Costly than Other Modes of Dissemination***

WikiLeaks and data-mining are standard examples of the fact that a combination of non-Internet technology and the Internet has made it substantially easier to assemble information and disseminate it[72]. As Neil Richards puts it, "a number of recent technological advances and cultural shifts have enabled the easier dissemination of [personal] information and the creation of larger, more detailed, and more useful data-bases.[73]". For any level of cost, the Internet user can compile and distribute a much larger amount of information than he or she could through other

[70] 395 U.S. 444, 447 (1969).
[71] *See, e.g.*, David A. Strauss, *Persuasion, Autonomy, and Freedom of Expression*, 91COLUM. L. REV. 334, 337-39 (1991).
[72] The computers used to compile information for data mining and the thumb drives used to download information from the Web are not necessarily linked to Internet technology—someone with two computers, neither of which are linked to the Internet, could use a thumb drive to transfer information from one to the other computer—but obviously the existence of the Internet makes those technologies much more useful.
[73] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1150 (2005).

technologies[74]. As Jack Balkin observes, "social media lower the costs of informing and organizing people quickly.[75]"

The cost of inflicting harm always constrains doing so: In a world in which libelous statements can be distributed only through a newspaper, there will be fewer such statements than in a world where they can be distributed via the Internet, simply because it is cheaper to log on to the Internet than to purchase a newspaper with its editorial offices and publishing plant. The same goes for all forms of regulable harms—invasions of privacy, copyright infringement[76], or damage to national security.

Lower cost means that constraints on inflicting harms (to national security or by invasion of privacy, for example) are weaker than they are in connection with traditional media. Standard constitutional doctrine deals with liability for *distributing* information that is both truthful and harmful in two branches. First, the First Amendment protects the distributor against liability if the information is produced without violating the law and the distributor acquires it without breaking the law. For example, in *Florida Star v. B.J.F.*, the Court held unconstitutional a statute prohibiting the publication, in a medium of "mass communication," the name of a victim of a sexual offense, in a case in which a reporter found the victim's name on a police report, which was available to anyone who walked in at the police department's press room[77]. The second branch of the doctrine deals with information that is "produced" illegally—as the Court put it, "[w]here the ... publisher of information has obtained the information ... in a manner lawful in itself but from a source who has obtained it unlawfully.[78]" In such cases, the Court balances the harm

[74] As an analytic matter, scope and cost are closely related (perhaps even the same), but distinguishing between them seems to me useful for expository purposes.
[75] Jack M. Balkin, *The First Amendment Is an Information Policy*, 41 HOFSTRA L. REV. 1, 11 (2012). Balkin uses the observation to identify some of the benefits of lower costs. For a judicial observation referring to possible drawbacks of lower costs, see *Blumenthal v. Drudge*, 992 F. Supp. 44, 49 (D.D.C. 1998) (blending cost and scope concerns, the Court referred to "[t]he near instantaneous possibilities for the dissemination of information by millions of different information providers around the world to those with access to computers").
[76] For an example of this reasoning in practice, see *Universal Studios v. Corley*, 273 F.3d 429, 453 (2d Cir. 2001) (upholding the constitutionality of an injunction issued under the Digital Millennium Copyright Act prohibiting the publication of a decryption code, and observing that "[t]he advent of the Internet creates the potential for instantaneous worldwide distribution of the [decrypted and] copied material").
[77] 491 U.S. 524, 527-28 (1989).
[78] Bartnicki v. Vopper, 532 U.S. 514, 528 (2001) (quoting Boehner v. McDermott, 191 F.3d 463, 484-85 (D.C. Cir. 1999) (Sentelle, J., dissenting)).

done by the disclosure against the public interest in providing access to the information[79].

Standard doctrine involves the traditional media—in the cases discussed above[80], a newspaper and a radio station—and perhaps it implicitly rests on an evaluation of the harms of suppression *given* likelihood of harm to other interests in light of the cost constraints associated with those media. What are those costs? First, there is the cost to the originator of acquiring the information. In *Bartnicki v. Vopper*, the information was gleaned from overhearing a cell phone conversation on a device that intercepted the conversation[81]. The cost is that of obtaining and using the interception technology, a cost that I will characterize as moderate rather than low. Sometimes, the cost to the originator will be low—for example, downloading information to a thumb drive in the Bradley Manning Wiki-Leaks case[82].

Second, there is the cost to the distributor of obtaining any specific piece of information. In *Florida Star*, that cost was having a reporter who had the time to go to the police station's press room to look at the police reports there[83], again what I will characterize as a moderate cost. In *Bartnicki*, in contrast, this cost was quite low, as the originator basically dropped the tape recording into the radio station's lap[84]. For the Internet, I suspect that this second cost is almost always going to be low.

Third, though, there is the cost of maintaining an organization that is in a position to get and use the information. There has to *be* a newspaper or radio station for the problems in *Florida Star* or *Bartnicki* to arise. Similarly, there has to be an organization like WikiLeaks to acquire information from Manning. I will assume that the cost of maintaining these organizations, whether traditional or Internet, is relatively large. But, it probably is worth noting that the costs of maintaining traditional media organizations include rather large costs of a relatively immobile physical plant, such as printing machines, whereas the costs of a physical plant for

[79] *Id.* at 534 ("In these cases, privacy concerns give way when balanced against the interest in publishing matters of public importance."). I assume for present purposes that the same approach would be taken with respect to harms to national security, though the balance might be struck differently.
[80] *See supra* notes 78-80 and accompanying text.
[81] *Bartnicki*, 532 U.S. at 518.
[82] *See* Marc Ambinder, *WikiLeaks: One Analyst, So Many Documents*, NAT'L J. (Nov. 29, 2010), http://www.nationaljournal.com/whitehouse/wikileaks-one-analyst-so-many-documents-20101129 [http://perma.cc/ZFB-882T].
[83] Florida Star v. B.J.F., 491 U.S. 524, 527-28 (1989).
[84] *See Bartnicki*, 532 U.S. at 519.

businesses that distribute information and ideas over the Internet are relatively low—computers that can be rather easily transported and office space that can be rented.

We also need to focus on what precisely the organization is—that is, on its business model. The business models in *Florida Star* and *Bartnicki* were ones in which the information distributor engaged in some screening of, or editorial judgment about, what it would disseminate. Internet distributors might have a similar model, in which case the cost of maintaining the Internet organization would be comparable to that of maintaining traditional media. An Internet distributor might have a different business model, though, as Wiki-Leaks reportedly does. The Internet distributor could simply take what it receives and send it out, leaving it to others to evaluate its content. Relative to traditional media, this is a low-cost business model (the cost of maintaining the organization aside)[85]. Other business models, of course, might depend on the use of additional screening mechanisms, the use of which might increase the cost to a moderate level.

I have provided this sketch of various costs because standard doctrine might have been developed with an implicit understanding of the costs associated with acquiring and disseminating information. Perhaps the Court assumed that overall, the costs were reasonably high. The Court might have implicitly considered that those costs would in themselves limit the amount of harmful information distributed by the traditional media. Then, the Court might have asked, "In light of what we think is the likely amount of harmful information these media can distribute consistent with their business models, what may legislatures add by law consistent with the First Amendment?" Were the costs lower, the amount of harmful information distributed would be different, and the Court's interpretation of the First Amendment might be different as well. The obvious pressure point is the balancing test in the second branch of standard doctrine, but even with respect to the first branch, the Court might come to think that a categorical rule was undesirable. Internet exceptionalism—or standard doctrine tweaked to deal with lower costs—might then develop.

[85] According to Julian Assange, WikiLeaks's founder, in 2010 the organization had five full time employees and relied on about 800 volunteers. Stefan May, *Leak-o-nomy: The Economy of WikiLeaks (Interview with Julian Assange)*, MEDIEN-ÖKONOMIE-BLOG (Jan. 4, 2010), http://stefanmey.wordpress.com/2010/01/04/leak-o-nomy-the-economy-of-wikileaks [http://perma.cc/K3M4-XNPX]. The *Florida Star*'s website identifies a staff numbering twentyeight. *The Florida Star Staff*, THE FLORIDA STAR (Aug. 11, 2014), http://www.thefloridastar.com/about-2 [http://perma.cc/Y74A-2SMS].

### ***D). The Putative Anonymity of the Internet***

Finally, I return to the "nobody knows you're a dog" meme. Holding the cost of acting constant, perhaps it is easier to operate anonymously on the Internet. For example, it might be more difficult to determine who is cyberstalking you than to determine who is physically doing so: the technology of detecting physical stalking can be relatively simple—just keep your eyes open [86]—whereas the technology of identifying a cyberstalker may require sophisticated techniques of tracking IP addresses, penetrating security walls, and the like[87].

The additional cost may sometimes matter. Consider threat liability again. Standard First Amendment doctrine allows the government to impose liability for making true threats[88]. The case law involves liability imposed through the criminal law[89], but a legislature could unquestionably create a civil cause of action by a victim against a person who sent her a true threat. If the cyberstalking cause of action imposes liability only on the cyberstalker himself, the anonymity afforded by the Internet is irrelevant: the victim can recover only if she identifies the cyberstalker. Or, put another way, a cyberstalker who remains anonymous is free from liability under such a cause of action.

As the *White* case shows, the government may have the resources to track down a person who threatens via the Internet[90]. Ordinary civil litigants, though, might not be able readily to identify their cyberstalkers. A legislature creating a civil cause of action for cyberstalking might take that fact into account in structuring liability. The obvious way to do so is to make Internet intermediaries liable for distributing true threats (or other material that can be regulated under standard First Amendment law). Alternatively, it can impose liability for refusing to turn over information that would enable the victim to determine who was issuing the threat—a refusal, I emphasize

[86] Of course there are more complex technologies, such as installing surveillance cameras, and some more expensive ones, such as hiring a private detective.
[87] *See* Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 434 (2009) ("Much speech on the Internet is anonymous, it may be difficult to find the person who is speaking.").
[88] Watts v. United States, 394 U.S. 705, 708 (1969).
[89] *See supra* note 42 and accompanying text.
[90] United States v. White, 698 F.3d 1005 (7th Cir. 2012). Though in *White* the defendant made no real efforts to conceal his identity on the Internet. *See id.* at 1011.

again, that would flow from the business model the intermediaries adopted[91]. Would that be permissible under the First Amendment?

Here I sketch a map of the possibilities. The starting point, perhaps oddly, is *New York Times Co. v. Sullivan*, which held that an intermediary can be held liable for publishing a false statement made by another person, if the intermediary transmitted the statement with knowledge of the statement's falsity or with reckless disregard for its truth or falsity[92]. There, a group of supporters of the civil rights movement drafted an advertisement and paid the newspaper to publish it[93]. The newspaper was simply an intermediary for the transmission of the advertisement's message. But, had standard First Amendment requirements of knowledge or reckless disregard been satisfied, the newspaper could have been held liable for publishing libelous statements[94]. *Sullivan* showed that an intermediary does not automatically have First Amendment protection for statements it transmits[95]. What matters is whether substantive First Amendment requirements are satisfied.

Satisfying such requirements is similarly necessary for establishing liability for threats[96]. Suppose that the substantive requirement for threat liability is that a reasonable person would take the utterance to be a true threat. With respect to that objective standard, and subject to a qualification I introduce in a moment, the threatener and any intermediary who transmits the threat are in the same position, each putting the victim in fear[97]. It might seem that the outcome should be different if the substantive standard requires a subjective intent to threaten. The threatener might have the requisite intent, but the intermediary would not. So, it might seem,

[91] Congress has immunized intermediaries from liability under the Communications Decency Act. 47 U.S.C. § 230 (2012). The question I consider in the text is whether, in the absence of statutory provision, intermediaries have a First Amendment immunity from liability.
[92] 376 U.S. 254, 279-80 (1964).
[93] *Id.* at 256-57.
[94] *Contra id.* at 279-80.
[95] *See id.*
[96] *See* Virginia v. Black, 558 U.S. 343 (2003).
[97] Importantly, the threatener and the intermediary are equally subject to "chilling effect" concerns. *See supra* note 53. The substantive standard is designed with those concerns in mind. *But cf.* Kreimer, *supra* note 61, at 27-28 (arguing that the risk of error is larger for intermediaries than for originators, in part because "intermediaries have a peculiarly fragile commitment to the speech that they facilitate"). Kreimer continues, "revenue from the marginal customer brings only a small payoff, a benefit that can easily be dwarfed by threatened penalties." *Id.* at 29. One response is the availability of insurance, the cost of which is taken into account in designing a business model. *See infra* note 104 and accompanying text.

intermediaries might have some First Amendment protections that cyberstalkers and the like might not, depending on the substantive First Amendment rules.

The analysis becomes slightly more complex when intermediaries object that as a practical matter they cannot check every message they transmit to determine (in the case of libel) whether it was false or (in the case of true threats) whether the message would put a reasonable recipient in fear. With respect to libel, the objection might prevail if the intermediary made some, possibly cursory, effort to check truth[98]. With respect to true threats under the objective standard, intermediaries can use algorithms to identify potentially threatening messages and then can inspect those messages to see if they are objectively true threats[99].

Internet intermediaries have argued that the First Amendment ought to bar the government from requiring that they use some method for inspecting the messages they transmit, on the ground that inspection would be too expensive and that users rely on assurances that whatever they originate will reach its destination[100]. That argument must be unpacked. What it asserts is that the intermediaries have adopted business models that are profitable only if victims of unprotected speech[101] bear costs that could in principle be shifted to the intermediaries. It is not clear that the First Amendment should be taken as a restriction on the government's ability to regulate business models[102]. That observation also suggests that threat liability might be imposed on intermediaries without violating the First Amendment even if the substantive standard for true threats is subjective. The reason is that intermediaries can, at least in principle, obtain insurance against liability. On this view, the First Amendment does not guarantee that intermediaries can choose whatever business

[98] For example, perhaps a statement in the intermediary's terms of service that those who originate statements warrant their truth would be sufficient to show that the intermediary did not act with reckless disregard for truth.

[99] For example, an algorithm could pull from the stream all messages with the words "I'd like to kill" (and more, of course). Some statements that are objectively true threats might not be caught by the algorithm, but one can imagine a First Amendment standard that would protect intermediaries who used reasonable algorithms to identify threatening messages.

[100] Denver Area Educ. Telecomms. Consortium v. FCC, 518 U.S. 727, 754, 830 (1996).

[101] These include people whose reputation is damaged by the dissemination of false statements about them or people who are put in fear and perhaps take costly protective measures after receiving true threats.

[102] *Cf.* Associated Press v. United States, 326 U.S. 1, 19-20 (1945) (rejecting the proposition that the First Amendment provided the Associated Press with a defense to an antitrust action). For a somewhat more extended discussion, see *infra* Part IV.B.

model they want, without regard to the harms produced by using one rather than another model[103].

Introducing the idea of business models helps us understand another argument against intermediary liability. The person who makes a true threat gets something—a sense of satisfaction, perhaps—out of making the threat; the intermediary who transmits it does not. No matter what the content, a rule imposing liability on the intermediary will induce the intermediary to suppress more speech than would the same rule applied to originators. This is because the intermediary, or so the argument goes, does not lose anything from "overcensoring" speech—that is, refusing to transmit speech in circumstances in which the originator is in fact protected by the First Amendment[104]. But, the argument fails to take into account the fact that the intermediaries do gain something from transmitting the message. It would not be the psychological satisfaction that the originator gets, of course, but the financial returns from adopting a business model in which they transmit whatever is presented to them. Intermediaries, that is, do lose something by overcensoring speech[105].

The argument so far is that intermediary liability, when properly constructed, is compatible with standard First Amendment doctrine with some tweaks. Subject only to those tweaks, originators of statements and those who transmit them can equally be held liable under the applicable substantive First Amendment standards[106]. And, I doubt that Internet exceptionalism for intermediary liability would be defensible

[103] I think the fact that, in principle, insurance is available for all forms of liability for disseminating harmful speech argues rather strongly against the proposition that the First Amendment restricts intermediary liability, at least if the First Amendment does not constrain government regulation of choice among business models. For a discussion of that proposition, see *infra* Part IV.B.

[104] For presentations of versions of this argument, see Kreimer, *supra* note 61, at 95-100, and Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293 (2011).

[105] Kreimer argues that intermediaries' financial losses are unlikely to be large enough to eliminate (or perhaps even reduce substantially) overcensorship, in part because users are unlikely to read or understand disclosures contained in terms of service. Kreimer, *supra* note 62, at 33-40. In addition, market structure might matter: intermediaries who have something close to a monopoly need not fear loss of business. But monopoly-like power is a traditional basis that justifies regulation, even in the context of the distribution of ideas and information. That bandwidth was limited, for example, was the rationale for finding regulation of broadcasting constitutionally permissible. *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) (referring to "the scarcity of radio frequencies").

[106] At this point, I think it appropriate to note once again that I am here considering whether judges would be justified in using the First Amendment to constrain legislative choices to impose liability, not whether such choices would be good ones. For example, in some settings, good policy might impose a regime of notice-and-takedown, though I doubt that such a policy would be adequate in the case of true threats.

because of the anonymity associated with the Internet[107]. Internet exceptionalism here would mean this: the First Amendment would protect a statement's originator but not the intermediary who transmitted it. I find such a rule difficult to understand or justify.

## 4. SOME ADDITIONAL QUALIFICATIONS

The preceding examination of the doctrinal terrain mapped out by claims for and against Internet exceptionalism has revealed that both the competing theses—exceptionalism and standard doctrine with tweaks—are defensible only when the claims are qualified in connection with specific sub-doctrines. This Part deals with some qualifications that are somewhat more pervasive: a question about the structure of constitutional doctrine, a question about the First Amendment's applicability to business models, and a question about state action that lurks in the discussion of intermediary liability.

### *A). Doctrinal Structure*

Part I argued that the idea of Internet exceptionalism makes sense only with a categorical doctrinal structure because a balancing structure can take account of everything that is said to make the Internet distinctive. There is, however, one complication: the possibility of categorical balancing. Categorical balancing has this structure: one identifies some relevant domain of speech—commercial speech, sexually explicit material, political speech—and initially conducts a balancing inquiry over all cases within that category[108]. One then examines the outcomes of that balancing and comes up with a categorical rule applicable to all cases within the domain, or with a set of rules and subrules that covers the domain.

[107] I insert the "because of anonymity" qualification because the argument about the broader scope of transmissions over the Internet, discussed above in Part II.B., might support intermediary liability when the originator might be protected by the First Amendment—for example, in cases where the originator did not intentionally use the Internet to broaden the audience for his or her message.

[108] "Initially" here can refer to a temporal sequence, as in the first, "experimentation" strategy for dealing with innovative speech technologies, or a purely analytic process in which one does the balancing in one's head.

As I observed in an analogous context in Part II, the critical step in categorical balancing is identifying the domain within which one is to do the balancing. Scholarship on Internet exceptionalism or new technologies of speech more generally offers two candidates for the relevant domain. For the moment, I will call the first one a traditional domain definition. We identify the domains by the characteristics of the regulations. We ask: Does the regulation deal with a specific subject matter for regulation, such as political speech, commercial speech, and the like? Then, within each subject-matter domain, does the regulation deal with the content of the speech, or the viewpoint it expresses? Alternatively, is the regulation neutral as to the speech's content or viewpoint?

I call this the "traditional" domain definition because we already know the outcome of the balancing within each category. It is what I have called standard First Amendment doctrine, with its requirements, with respect to some domains, of narrow tailoring, compelling governmental interest, and the like.

The second candidate for domain-definition is, as Justice Jackson might be taken to have suggested, based on the medium[109]. We examine proposed regulations dealing with the press, with broadcasting, and now the Internet, do the required balancing and come up with appropriate rules. Perhaps those rules will map quite precisely onto standard First Amendment doctrine, but there is no reason a priori to think that they will—that is, no reason to think from the outset that medium-based rules will use criteria like content-neutrality and the like[110]. Perhaps, for example, the distinction between content-based and content-neutral rules makes sense regarding dissemination of information and ideas through print, but makes less sense with respect to such dissemination via broadcasting or the Internet. One cannot know without going through the process of categorical balancing[111].

[109] *See* Kovacs v. Cooper, 336 U.S. 77, 98 (1949) (Jackson, J., concurring).

[110] Chen concludes that differences among media are not large enough for us to expect that categorical balancing done with media as the relevant domains will yield rules differentiated by medium. Chen, *supra* note 15. I take no position on that question.

[111] To the extent that categorical balancing is a process that extends over time, it might well be the way in which we pursue the first "experimentalist" strategy for dealing with innovative speech technologies, but I do not think that there is an analytic connection between categorical balancing and the experimentalist strategy.

### ***B). Business Models and the First Amendment***

Professor Rebecca Tushnet has observed that in *Sullivan*, the Supreme Court invoked the First Amendment to limit an intermediary's liability for actions taken consistent with its business model. As she pointed out, "What the actual malice standard protected was ... [the newspaper's] business model—accepting the speech of others with only limited fact-checking[112]". One might interpret the decision as constructing First Amendment doctrine with an eye to the newspaper's business model: given the fact that their business model is one in which they can do only limited fact checking[113], what should First Amendment doctrine be? An alternative, and I think better, reading is that the existence of limited fact checking showed that New York Times Co. did not act with reckless disregard for the truth. On that reading, *Sullivan* does not stand in the way of business-model regulations adopted for reasons other than the suppression of the dissemination of information, either generally or through specific business models.

As is widely understood, the adoption of one section of the Communications Decency Act—now 47 U.S.C. § 230—makes it unnecessary to consider (today) whether a legislature could impose intermediary liability for distributing harmful material originated by others[114]. Suppose, though, that § 230 were replaced by a regime requiring that intermediaries do something to limit the distribution of harmful material—that they adopt a different business model. The question is whether such business-model regulation would be constitutionally permissible, even though the regime might be described as one in which the regulation was adopted for the purpose of restricting the dissemination of harmful information.

In initially discussing intermediary liability, I assumed that the First Amendment placed few constraints on a legislature's power to prescribe or ban business models, even if the business is the dissemination of information and ideas. Clearly, however, the First Amendment must place *some* constraints on that power. For example, it would be unconstitutional for a legislature to require that newspapers

[112] Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1005 (2008).
[113] Here "can do" means that the cost of more extensive fact checking would make the business unprofitable in its current form.
[114] *See* Tushnet, *supra* note 112, at 1008 n.95 ("Before the CDA, the assumption in the law reviews tended to be that the *Sullivan* standard was the best to be hoped for as a *constitutional* matter."). Rebecca Tushnet also observes that it was "not much argued" that there was "a constitutional right to operate a search engine free of liability for the indexed content." *Id.* at 1008.

be "printed" by scribes using quill pens. It is less obvious that a legislature could not require that newspapers be printed on newsprint manufactured in the United States[115]. And that would be true even in the face of a newspaper's claim that its business model requires that it use non-U.S. manufactured paper—even if, that is, complying with the requirement would drive the newspaper out of business[116].

What is the difference between the two requirements[117]? Probably that the only imaginable reason for adopting the first statute is to limit the distribution of information by newspapers, whereas the second statute has or could have other purposes. Now consider a regulation whose purpose is to require that a business internalize the harms it inflicts on others. One example is ordinary tort liability for damages caused by negligent operation of the trucks used to distribute the business's products. I think it clear that a newspaper could not claim First Amendment protection against that regulation when its delivery trucks cause harmful accidents, and that would be true even if the newspaper claimed that its business model required that its trucks regularly operate at dangerous speeds[118]. Intermediary liability of the sort I have discussed has the same analytic structure: it imposes liability on a business for the harm the business helps cause[119]. In the absence of reasons to think that a

[115] At the state level, preemption questions aside.

[116] *But cf.* Grosjean v. Am. Press Co., 297 U.S. 233 (1936) (holding unconstitutional a state statute that imposed a sales tax on newspapers with large circulations). I believe that *Grosjean* is best understood as holding that a statute, general on its face, that is adopted for the purpose of suppressing an information-providing business (or, even more narrowly, that is targeted at such business because of the content of what they distribute) is unconstitutional: a legislature cannot escape the limits the First Amendment places on content-based or viewpoint-based regulation by "gerrymandering" a statute so that it affects only the disfavored content or viewpoint.

[117] For a discussion of the application of the First Amendment to methods of producing speech, see Ashutosh Bhagwat, *Producing Speech*, 56 WM. & MARY L. REV. 1029 (2015).

[118] *Cf. Pizza Chain Loses Lawsuit over Wreck*, KY. NEW ERA, Dec. 18, 1993, at 1D, *available at* http://perma.cc/Y45L-LFDM. The news story deals with pizza deliveries, but I seriously doubt that the result would differ were the business involved a newspaper.

[119] I note two qualifications. First, that the intermediary is only one of the causes of harm—the other being the originator—which seems to me irrelevant for purposes of assessing legislative power. At least in modern times, legislatures have the power to impose liability on "but for" causers of harm, not only on proximate causers. *Cf.* N.Y. Cent. Co. v. White, 243 U.S. 188 (1917) (upholding the constitutionality of a workers' compensation statute that imposed liability without fault on employers); Hymowitz v. Eli Lilly & Co., 539 N.E.2d 1069 (N.Y.1989) (imposing "market share" liability on a defendant who could show that the plaintiff had not used the defendant's product). Second, equally irrelevant would be the fact, were it to be true, that the legislature imposed "but for" liability only on Internet intermediaries. A legislature is entitled to address problems as they arise, and need not make what Justice Stevens called an "all or nothing-at-all" choice. Denver Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727, 769 (1995) (Stevens, J., concurring). *But compare* Leathers v. Medlock, 499 U.S. 439 (1991) (upholding as constitutional a general sales tax, which cable providers had to pay, but from which newspapers and magazines were exempted), *and* Williamson v. Lee Optical, 348 U.S. 483 (1955) (finding it constitutional for a legislature to proceed one step at a time in the context of nonspeech businesses), *with* Minneapolis Star & Tribune Co. v. Minn. Comm'r of

legislature required businesses engaged in speech activities to internalize harms they cause for the very purpose of driving them out of business, I find it difficult to see a valid First Amendment objection to a cost-internalization statute. I acknowledge, however, that the state of the law and of scholarly discussions of the issue limits my confidence in that conclusion.

Some of the cases hint at an additional concern, that businessmodel regulation would be a disguised method of content-based regulation[120]. As always in such situations, the courts have a choice between two strategies, parallel here to Internet exceptionalism and standard doctrine with tweaks. They can ask in each specific case whether there is substantial reason to think that a statute not framed in content-based terms was adopted for the purpose of regulating content and whether that purpose is reasonably likely to actualize in practice, that is, that content regulation will in fact occur. Or, they can adopt a prophylactic rule banning the use of some regulatory approaches. Such a rule would single out some characteristics of the regulatory approach to identify a class of regulations in which the risk of disguised content-control measures is high enough. At this point, and partly because of the effect of § 230 in blocking the development of Internet regulations, I think it difficult to say more—for example, to identify the characteristics that would be built into a prophylactic rule.

### ***C). The Lurking Problem of State Action***

So far this Article has considered the possibility of Internet exceptionalism in connection with regulatory rules that might impose liability on those who disseminate information over the Internet when the First Amendment precludes the imposition of liability for disseminating the same information through traditional media. It has paid some attention to the concern for "censorship by proxy[121]". Censorship by proxy occurs when regulatory rules that operate appropriately when applied to originators and traditional media, by creating an acceptable mix of information dissemination and resulting harm, have a greater chilling effect when applied to Internet

---

Revenue, 460 U.S. 575 (1983) (holding unconstitutional a state sales and use tax imposed on ink and paper used in producing newspapers and magazines, when small publishers were exempt from the tax).

[120] *See* Chen, *supra* note 15, at 1360, 1450-51 ("[C]ourts should remain wary of disguised efforts to control content.").

[121] Kreimer, *supra* note 62, at 17.

intermediaries[122]. My expository strategy has been to try to present some ideas in the simplest legal context—when the government acts as regulator of speech itself rather than as the regulator of the media transmitting speech[123].

There is, though, another area in which Internet exceptionalism (or standard doctrine with tweaks) has featured prominently. The discussion so far has not dealt with information and ideas that the intermediary *wants* to transmit, but those which the government seeks to suppress because of the harms they cause. Or, more precisely, the discussion so far has dealt with intermediaries whose business model rests on transmitting everything that originators want distributed.

But, of course, intermediaries might have a whole range of different business models. One business model might filter out messages of which the business owners disapprove, without regard to whether the government does— for example, sexually explicit but nonobscene images. Another business owner might inspect incoming messages and refuse to transmit those expressing "extreme" political views, as defined by the intermediary in its terms of service. Those and others might be viable business models. Can the government direct that intermediaries adopt a particular business model? Specifically, can the government require that intermediaries transmit everything they receive, preserving the government's power to punish the originators of speech whose regulation is consistent with the First Amendment[124]?

Here too I aim only to identify the lines of argument available about Internet exceptionalism and standard doctrine with tweaks. In general, the arguments fall into two closely related categories. First, some argue that the government has the power to treat intermediaries as common carriers. At common law, a common carrier, is an entity that is required to adopt an "all-comers" policy that does not discriminate

[122] *See id.* at 66 (discussing how internet intermediaries' typical prophylactic response to regulation may lead to users self-censoring protected speech).
[123] Particularly by focusing on legislative and judicial assumptions regarding the nature and unique aspects of the Internet, such as the exponential accessibility of broad audiences, Kreimer, *supra* note 61, at 13, and lower transaction costs in communicating, Balkin, *supra* note 76, at 13.
[124] Section 230(c) immunizes intermediaries whose business model is an "all comers" model from liability for disseminating information and ideas where the originator can be punished without violating the First Amendment, but it does not require any intermediary to adopt such a business model. 47 U.S.C. § 230(c) (2012).

("unjustly," in the usual formulation) among those who seek to use its service[125]. Railroads and hotels are classic common carriers.

Putting the common-carrier obligation in another way leads us to the second type of argument. The property rights that common carriers have are more limited than the property rights of other businesses, who are entitled (absent otherwise permissible statutory regulations) to refuse to serve whomever they choose. The state action doctrine is at its base about the limits the Constitution, rather than statutes, places on property rights. Consider the classic case of *Shelley v. Kraemer*, which found that judicial enforcement of a property right created by a racially restrictive covenant violated the Equal Protection Clause even though judicial enforceability is a defining characteristic of property rights[126].

Standard doctrine holds that the government cannot require that the print media act as common carriers[127]. Unreversed precedent, highly controversial and probably unlikely to be followed by the Supreme Court were the issue to be presented to it today, allows the government to treat the broadcast media differently[128]. The *Turner Broadcasting* decisions adopted intermediate scrutiny to assess whether certain government "must-carry" requirements for cable television were constitutionally permissible, and ultimately upheld the ones at issue [129] . The "must-carry" requirements treat cable systems as limited common carriers. Notably, the four dissenters in the first *Turner Broadcasting* case acknowledged, though I suspect without fully thinking the question through, that "if Congress may demand that telephone companies operate as common carriers, it can ask the same of cable companies[130]".

---

[125] See N.J. Steam Navigation Co. v. Merchs.' Bank, 47 U.S. (6 How.) 344, 382-83 (1848) (finding that a common carrier is in effect a sort of public office and is obligated to carry and transport all goods offered to it).

[126] 334 U.S. 1 (1948). The case is controversial, but, as I have argued in detail elsewhere, the controversy is ultimately not about whether there was state action but whether the standards usually relied upon in finding equal protection violations were satisfied. Mark Tushnet, Shelley v. Kraemer *and Theories of Equality*, 33 N.Y.L. SCH. L. REV. 383 (1988).

[127] *See* Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241 (1974) (holding unconstitutional a state statute requiring that newspapers publish replies to editorials that "assail" a political candidate's character).

[128] *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367 (1969) (holding that an FCC policy requiring that broadcasters make time available for replies to personal attacks did not violate the First Amendment).

[129] Turner Broad. Sys. v. FCC, 520 U.S. 180 (1997) (rejecting the constitutional challenge to the "must-carry" requirements); Turner Broad. Sys. v. FCC, 512 U.S. 622 (1994) (holding that the appropriate standard was intermediate scrutiny).

[130] 512 U.S. at 684 (O'Connor, J., dissenting).

If Congress can demand that cable companies operate as common carriers, can it ask the same of Internet intermediaries?[131] We might get some guidance from thinking about why legislatures cannot impose common-carrier obligations on newspapers but can do so on cable operators. The most obvious reason is that newspapers adopt what I call "high editorial intervention" business models—the business model is one in which the publisher supervises editorial content quite closely—whereas cable operators use a "moderate-to-low editorial intervention" business model. According to the Supreme Court in *Turner Broadcasting*, the must-carry requirements implicated the First Amendment because cable operators had a business model in which they exercised some editorial discretion in choosing which channels to include in their packages, but not a lot of discretion[132]. Whether Congress could impose common-carrier obligations on Internet intermediaries might then depend on the precise business model each intermediary adopted: the First Amendment would bar imposing those obligations on intermediaries that exercised high levels of editorial intervention, by extensive screening for example, and would permit doing so on intermediaries that exercised significantly lower levels[133].

Finally, if we pursue the pure state action route, we will almost certainly end up with Internet exceptionalism. The difference between common carrier regulation and regulation pursuant to the state action doctrine is that the former is legislatively optional—Congress can choose to treat intermediaries as common carriers—whereas the latter is constitutionally required. Under a state action approach, the First Amendment not only does not bar legislatures from regulating intermediaries as

[131] I believe that there is no threshold question under modern law of whether a business has some traditional characteristics associated with common carriers as identified at common law—those characteristics included that the business provide a socially important service and that competition in some geographic areas was likely to be limited, though not that the businesses have a monopoly in the area. Under modern law, legislatures are free to impose service obligations on any business subject only to the First Amendment and perhaps some other discrete constitutional limitations on legislative power. The foundational case on this is *Nebbia v. New York*. 291 U.S. 502, 552 (1934) (holding that the Constitution permitted the New York legislature to treat an ordinary business, there supplying milk, as a business "affected with a public interest," without regard to traditional definitions of the latter phrase).

[132] *Turner Broad. Sys*, 512 U.S. at 643-44 (noting that "the provisions interfere with cable operators' editorial discretion by compelling them to offer carriage to a certain minimum number of broadcast stations").

[133] I think the implication of *Turner Broadcasting* is probably that the relevant distinction is between high and low levels of editorial intervention, not between business models with high levels and those with no editorial intervention at all.

common carriers, it affirmatively requires that courts develop common-carrier-type regulations[134]. A state-action analysis would ask, "Is the rule of property that allows people to adopt the business model at issue consistent with the First Amendment?" Under standard First Amendment doctrine, the answer might well be, "Yes." The property rule is the content-neutral rule that private owners of resources have the right to choose any business model that does not involve systematic violations of other provisions of law. The tests used to determine whether a content-neutral rule is consistent with the First Amendment are usually quite tolerant of such approaches, to the point when one might fairly characterize the doctrine as finding constitutionally permissible any rule that is a rational method of allocating property rights[135]. Invoking the state action doctrine to impose common-carrier obligations on intermediaries would be a dramatic departure from standard First Amendment doctrine understood in this way.

But, as always, there is an alternative interpretation available. The first move would be to focus not on "private property" generally, but on the property law rules applicable to media enterprises or even more narrowly to Internet intermediaries[136]. With the property rule narrowed, we would look to standard doctrine. And, at least as a matter of formally stated doctrine, content-neutral regulations can be unconstitutional if they have a troublingly large disparate impact on those who have few private resources of their own to disseminate their message[137]. A rule of property law that allows intermediaries to choose whatever business model they like *might* have that kind of disparate impact[138]. If so, we would once again have a rule for the Internet that was standard doctrine with tweaks.

---

[134] Note that the state action route changes regulation from being optional to being required, and it also (subject to some wrinkles not worth exploring in this Article) changes the institution doing the regulating from the legislature to the courts.

[135] *See* Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469 (1989) (holding that government restrictions on commercial speech need not be by the least restrictive means, but only be a reasonable "fit" between the government's ends and means); Ward v. Rock Against Racism, 491 U.S. 781 (1989) (upholding the constitutionality of a municipal regulation designed to protect residents from excess noise by requiring performances in public band shell use city provided sound system and technician).

[136] This is another version of the question of identifying the relevant reference class, *see supra* note 36 and accompanying text, and as before there is no policy-independent way of identifying that class.

[137] The basic cases, which remain good law, are *Hague v. Comm. for Indus. Org.*, 307 U.S. 496 (1939), and *Schneider v. Town of Irvington*, 308 U.S. 147 (1939).

[138] Note that the analysis is on the level of the general property rule authorizing choice of business model, not on the level of asking whether a particular business model has a troublingly large disparate impact.

## 5. CONCLUSION

The foregoing set of arguments about the Internet's distinctive nature, values, and dangers supports only a rather weak conclusion. I doubt that we can say either that the Internet's nature, values, and dangers justify Internet exceptionalism or that they justify only the application of standard First Amendment doctrine with appropriate tweaks. My predisposition is to say that in such a situation, judicial deference to legislative choices would require deference to a legislatively chosen regime of Internet exceptionalism. On reflection, though, I think that saying so would be mistaken because the "judicial deference" concern is built into the analysis of specific regulations and cannot be generalized across regulations[139]. The lesson, I think, is that the question, "Internet exceptionalism or standard doctrine with tweaks?" may be badly posed. The real question is, "Internet exceptionalism or standard doctrine with tweaks in connection with this specific regulation of this specific problem?"

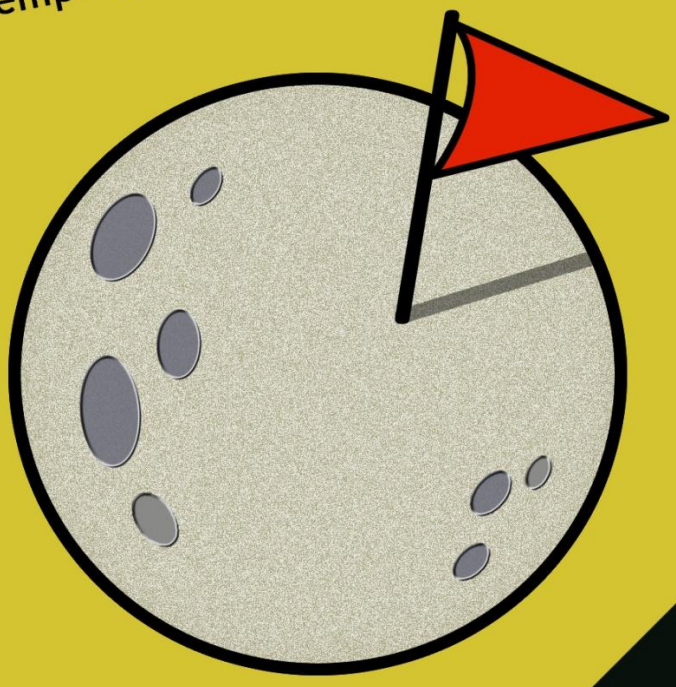
[139] For example, compare *Ashcroft v. Free Speech Coal.*, 535 U.S. 234 (2002), which illustrated the absence of judicial deference by holding unconstitutional the application of bans on child pornography to "virtual" child pornography, with *United States v. Williams*, 553 U.S. 285 (2008), which illustrated judicial deference by upholding the constitutionality of a prohibition on "pandering" child pornography when the defendant did not actually possess child pornography.

# CYBERLAW

by CIJIC

## DIREITO:
## A PENSAR TECNOLOGICAMENTE

Em pleno século XXI, o ciberespaço assume-se como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação e de informação ao serviço do Homem. A sociedade hodierna, inebriada por esta revolução tecnológica, numa quase-metamorfose híbrida, adapta-se a esta tecno-dependência. Mas, será que compreendemos, minimamente, o advento do ciberespaço e do tempo moderno em que vivemos?



CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA