

O CONCEITO DE TRATAMENTO DE DADOS APÓS O CASO *GOOGLE SPAIN* E SUA INFLUÊNCIA NA SOCIEDADE BRASILEIRA

CÍNTIA ROSA PEREIRA DE LIMA

Pós-doutoranda na *Università degli Studi di Camerino* – Itália com bolsa CAPES (Proc. BEX 6189/14-8). Doutora em Direito Civil pela Faculdade de Direito da USP (2004 - 2009) com estágio na Universidade de Ottawa (Canadá) com bolsa CAPES - PDEE - Doutorado Sanduíche, Advogada, Professora de Direito Civil da Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo e na pós-graduação da Faculdade de Direito da USP - Largo São Francisco. Agradeço a Professora Maria Cristina Di Cicco pelo convite para realizar as pesquisas na UNICAM (Itália) e pela disponibilidade constante em debater e questionar os resultados desta pesquisa.

Resumo

A economia da informação coloca em xeque a tutela dos dados pessoais uma vez que esta representa um entrave aos interesses econômicos das grandes corporações que atuam neste setor. As empresas operadoras dos sites de busca, que antes somente obtinham lucros, enfrentam atualmente constantes batalhas para se adequarem às legislações. O caso conhecido como *Google Spain* deve ser considerado um marco neste processo, pois o Tribunal de Justiça europeu, ao interpretar a Diretiva 95/46/CE entendeu que as ferramentas de busca devem ser consideradas tratamento de dados pessoais, porque os dados inseridos na rede mundial de computadores são coletados, armazenados, disponibilizados aos usuários segundo uma ordem de classificação. De fato o tratamento de dados é definido em lei de forma ampla porque não se pode engessar uma lei que sofre grande impacto da evolução das novas tecnologias. O Direito Espanhol teve uma participação muito importante neste processo, inclusive mediante a *Agencia Española de Protección de Datos Personales* – AEPD, que desde 2007, concluiu que os motores de busca realizam atividades que devem ser caracterizadas como tratamento de dados. Tal entendimento foi corroborado um ano depois, pelo Grupo de Trabalho, WP 29 em sua opinião n. 148, adotada em 04 de abril de 2008, na qual se deixou claro que as atividades das ferramentas de busca na internet devem ser consideradas tratamento de dados. Este artigo pretende analisar os argumentos suscitados para a caracterização destas como tratamento de dados. Em assim sendo, os operadores destas ferramentas estão sujeitos à legislação de aplicação

de dados pessoais, que garante diversos direitos aos titulares dos dados, entre os quais o direito ao cancelamento ou à exclusão de suas informações. No Brasil, o Marco Civil da Internet tratou timidamente da proteção dos dados pessoais ao elencar no art. 7º, inc. VIII, IX e X alguns direitos, este último garante o direito à exclusão das informações, repetido no art. 10. Esta pesquisa tem por objetivo investigar se este pode ser considerado o fundamento legal do direito à desindexação afirmado pela Corte de Justiça europeia. Ao final, destaca-se a necessidade de harmonizar as leis sobre o tema para que seja garantida a proteção dos dados pessoais pouco importando onde os dados são tratados e onde os operadores dos motores de busca estão sediados, questão que, também, foi julgada neste importante precedente.

Palavras-chave

Autoridade Garantidora da Proteção dos Dados Pessoais; Ferramentas de busca; Direito à desindexação.

Abstract

The information economy challenges personal data protection because it represents an obstacle to the big corporations' economic interests within this market. The companies which operate the searching websites, that before had only profits, face nowadays legal battles in order not to be bound to personal data protection legislation. The leading case, known as *Google Spain* must be considered as a landmark in such process given the European Court of Justice's interpretation of the Directive 95/46/CE considering that the search engines shall be considered as personal data processing because the data which are inserted by the users are collected, stored, disclosed within certain classification order. As a matter of fact, personal data processing is stated by law in open terms due the fact that one cannot freeze the law that suffers constantly the impact of new technologies. The Spanish Law played an important role through its Supervisory Authority, named *Agencia Española de Protección de Datos Personales – AEPD*, that since 2007 had concluded that the search engines are activities that process personal data. Such findings were reaffirmed one year later by the Working Party, *WP 29* opinion n. 148 (April 4th 2008) in which it was clear that the searching websites shall to be considered personal data processing. This paper intends to analyze the statements raised within this subject. In other words if the search engines are data processing, the searching websites' operators must follow the personal data protection legislation that ensures rights to the data's subject such as the right to correct, cancel or delete his information. In Brazil, the Internet Civil Rights Framework, know as *Marco Civil da Internet*, has dealt with personal data protection superficially within article 7º, inc. VIII, IX and X, the last one states the right to cancel or delete personal information which is repeated at article 10. This research aims to investigate that

these legal statements could be considered the legal basis for the right to unindexation as it was affirmed by the European Court of Justice. To sum up, it points out the necessity of harmony among the laws to ensure an effective personal data protection worldwide no matter neither where the data are processed nor where the search engines' operators are established another question judged by this important precedent.

Key words

National Supervisory Authorities on Personal Data Protection; Search engines; Right not to be indexed.

1. Introdução

A proteção dos dados pessoais não é um tema recente. A Convenção n. 108, isto é, a *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (conhecida como *Convenção de Estrasburgo sobre Proteção de Dados Pessoais*), realizada em 28 de janeiro de 1981, já elencava a matéria como relevante e que deveria ser tratada com muita seriedade pelos países signatários.¹

Na *Exposição de Motivos* deste documento, destacou-se que somente a legislação não seria suficiente para a efetiva tutela dos dados pessoais, *in verbis*:

39. The “measures within its domestic law” can take different forms, depending on the legal and constitutional system of the State concerned: apart from laws they may be regulations, administrative guidelines, etc. Such binding measures may usefully be reinforced by measures of voluntary regulation in the field of data processing, such as codes of good practice or codes for professional conduct. However, such voluntary measures are not by themselves sufficient to ensure full compliance with the convention.

Além da legislação e de códigos de boas condutas, destacou-se a necessidade de um órgão que auxiliasse os indivíduos e o governo a fim de que fosse garantida a eficácia da norma. É justamente esta a novidade do tema, isto é, a atuação das denominadas *Supervisory Authorities* na proteção dos dados pessoais. Em outras palavras, em 1981, já foi sinalizada a necessidade de uma atuação deste órgão, modelo que foi adotado na Diretiva 95/46 CE sobre proteção de dados.

Em 24/10/1995, quando foi aprovada a Diretiva 46 do Parlamento e do Conselho Europeu, o quadro jurídico de proteção de dados pessoais foi estabelecido tendo em vista

¹ COLOMBO, Matteo. *Regolamento UE sulla Privacy: principi generali e ruolo del data protection officer*. Milão: Associazione Data Protection Officer, 2015. p. 08.

um contexto tecnológico bem diverso do que existe hoje. Assim, após a aprovação desta diretiva, a *web* trouxe e traz desafios constantes.

O modelo de proteção de dados da União Europeia sofreu algumas mudanças tendo em vista o avanço tecnológico, notadamente pelas Diretivas 2002/58/CE e a que a substituiu, a Diretiva 2009/136/CE, sobre direitos dos usuários no que tange às comunicações eletrônicas e serviços de redes sociais. As mudanças da legislação comunitária de proteção de dados pessoais continuam através da proposta de uma nova Diretiva sobre Proteção de Dados para modernizar o panorama atual estabelecido pelas Diretivas 95/46/CE e 2009/136/CE, notadamente quanto aos desafios relacionados com a coleta e compartilhamento de dados no contexto das novas tecnologias de comunicação, e. g. redes sociais e ferramentas de busca.²

Na década de 90, a rede mundial de computadores era identificada como *web 1.0*³, caracterizada sobretudo por ser uma ferramenta de leitura (*“the mostly read-only web”*). A partir do final da década seguinte, 2006 em diante, a rede trouxe várias aplicações e a possibilidade de geração de conteúdo de forma colaborativa.⁴

Em outras palavras, na primeira fase da *web (1.0)*, a internet era utilizada basicamente como fonte de informação e como meio de comunicação (*emails*). Na fase seguinte, *web 2.0*, a internet é utilizada, além das maneiras antes citadas, como ferramenta potente de gerar conteúdo de maneira colaborativa⁵ e divulgá-lo, permitindo inclusive que outras pessoas continuem a trabalhar com a ideia, *curtindo, compartilhando, blogando, retuitando* etc. Desta forma, os dados que passaram a ser inseridos na rede mundial de computadores

2 EC, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), Brussels, 25 January 2012. Disponível em: <<http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf>>, acessado em 04/01/2014.

3 DEAN, Tami R; CIELOCHA, Kristin M; HANDSFIELD, Lara J. Becoming Critical Consumers and Producers of Text: Teaching Literacy with Web 1.0 and Web 2.0. *Reading Teacher*, 2009, Vol.63 (1), p. 40 - 50.

4 TAPSCOTT, Don; WILLIAMS, Anthony D. *Wikinomics: how mass collaboration changes everything*. New York: Penguin Group, 2006. P. 10 – 11: “Today the tables are turning. The growing accessibility of information technologies puts the tools required to collaborate, create value, and compete at everybody’s fingertips. This liberates people to participate in innovation and wealth creation within every sector of the economy. Millions of people already join forces in self-organized collaborations that produce dynamic new goods and services that rival those of the world’s largest and best-financed enterprises. This new mode of innovation and value creation is called ‘peer production’, or peering – which describes what happens when masses of people and firms collaborate openly to drive innovation and growth in their industries.”

5 ZITRAIN, Jonathan. *The future of the internet and how to stop it*. Virginia: Yale University Press, 2008. p. 20: o autor resume este processo de criação de conteúdo com a possibilidade de participação alheia de conhecimento *generative*.

alcançaram quantidades inimagináveis, sendo que em 2013, de acordo com a Cisco, a quantidade de tráfego de informações na internet alcançou 667 exabytes.⁶

Tal fato não passou despercebido pelos gerenciadores destas informações que, em posse destes dados, começaram a desenvolver outras aplicações, tais como as “ferramentas de busca” (*search engines*), *big data*, *cloud computing*, entre outras. Desta forma, as ofertas de serviços de *email*, de criação e manutenção de perfis em redes sociais passaram a serem feitas sem custo direto, ou seja, para estimular a inserção de mais e mais dados, estas empresas oferecem serviços “equivocadamente” denominados como gratuitos.

Isto porque o preço que o usuário paga são os próprios dados que inserem, viabilizando práticas muito lucrativas tais como *marketing direto*, *cookies*, coleta de informações denominada *Big Data* que serve a interesses econômicos e, muitas vezes, prejudiciais aos usuários da rede. De maneira que as atividades oferecidas “gratuitamente” (pois a remuneração é indireta) passaram a ser uma importante fonte de renda de vários provedores de acesso a internet e de conteúdo.⁷

Neste sentido, Giovanni Maria Riccio⁸:

I providers sono soggetti che svolgono, in misura professionale ed imprenditoriale, la propria attività; detta attività, ovviamente, è remunerativa, ossia comporta un arricchimento patrimoniale della posizione dell'intermediario a titolo diretto – gli utenti pagano un canone fisso di abbonamento ai servizi offerti o una somma versata una tantum e commisurata all'entità delle controprestazioni –, o a titolo indiretto – il servizio è offerto gratuitamente agli utenti, ma il provider ottiene un guadagno consentendo ad altre imprese di utilizzare detto servizio per scopi pubblicitari.

A economia da informação fundamenta-se nesta coleta, administração e no armazenamento destas informações. E a “monetização” destes dados trouxeram novas práticas que demandam, não só uma reforma da legislação sobre proteção de dados pessoais, mas também uma atuação proativa de um órgão específico e independente para garantir o cumprimento e a eficácia das normas de proteção de dados pessoais.⁹

6 The economist. *Data, data everywhere*. A special report on managing information. Disponível em: <<http://www.emc.com/collateral/analyst-reports/ar-the-economist-data-data-everywhere.pdf>>, acessado em 28 de maio de 2015.

7 A título de exemplo, em 2004, o *Facebook* teve uma receita avaliada, inicialmente, em 0,4 milhões de dólares. Em 2014, suas receitas alcançaram a casa de 12,466 milhões de dólares. Disponível em: <<http://en.wikipedia.org/wiki/Facebook>>, acessado em 28 de maio de 2015. Por sua vez o *Google*, em 2001, teve uma receita de 86,426 milhões de dólares. Em 2015, as suas receitas alcançaram a casa de 66,001 bilhões de dólares. Disponível em: <<https://investor.google.com/financial/tables.html>>, acessado em 28 de maio de 2015.

8 *La responsabilità civile degli internet providers*. Torino: G. Giappichelli Editore, 2002.

9 PIZZETTI, Franco. Le Autorità Garanti per la Protezione dei Dati Personali e la Sentenza della Corte di Giustizia sul Caso Google Spain: è Tempo di Far Cadere il “Velo di Maya”. In: *Il Diritto dell'informazione e dell'informatica*, 2014, fasc. 4-5, Giuffrè, pp. 805 – 829. p. 815.

Neste sentido, o papel das denominadas “autoridades garantidoras”, “*supervisory authorities*”, em espanhol “*agencia de protección de datos*” ou, em italiano, “*autorità garante della protezione dei dati personali*” é de extrema relevância para poder acompanhar a contínua evolução tecnológica e, assim, fiscalizar e garantir a eficácia da norma sobre proteção de dados pessoais.

Por isso, o caso *Google Spain*, que será exposto neste artigo, revela que a decisão da Corte de Justiça europeia não é suficiente para garantir um dos direitos dos sujeitos dos dados, que seria a desindexação de suas informações pelas ferramentas de busca. A eficácia deste direito reconhecido nesta decisão depende de respostas a tantos outros questionamentos que caso a caso estes órgãos independentes irão definir.

Um papel importante destes órgãos é a atuação independente e proativa para oferecer aos provedores e aos usuários da rede indicações e recomendações necessárias a garantir a eficácia do direito reconhecido pela Corte de Justiça europeia, que decorre do direito à oposição e ao cancelamento de informações pessoais, ou seja, o direito à indexação, entendido como o direito de não ser facilmente encontrado (mas não necessariamente que os dados sejam eliminados da rede). Pizzetti Franco¹⁰ define o direito à indexação como:

[...] il diritto a non vedere facilmente trovata una notizia non più attuale. L'effetto principale della indicizzazione e diffusione delle notizie attraverso il motore di ricerca è infatti quello di concorrere in modo continuo a riattualizzare tutte le informazioni, facendole diventare tutte elementi del profilo in atto della persona a cui si riferiscono.

De maneira que se entende necessário o estudo sobre o direito à desindexação e se tal direito pode ser fundamentado no direito à oposição (art. 14, “a” da Diretiva 95/46/CE)¹¹ e ao cancelamento das informações pessoais (estabelecido no art. 12, “b” da mesma diretiva).¹² Além disso, este trabalho pretende analisar se as atividades realizadas pelos motores de busca na internet podem ser consideradas tratamento de dados pessoais tal

¹⁰ *Idem ibidem*, p. 808.

¹¹ DIREITO DE OPOSIÇÃO DA PESSOA EM CAUSA - Artigo 14º Direito de oposição da pessoa em causa: Os Estados-membros reconhecerão à pessoa em causa o direito de: a) Pelo menos nos casos referidos nas alíneas e) e f) do artigo 7º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efectuado pelo responsável deixa de poder incidir sobre esses dados;

¹² SECÇÃO V - DIREITO DE ACESSO DA PESSOA EM CAUSA AOS DADOS - Artigo 12º Direito de acesso: Os Estados-membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento: [...] b) Consoante o caso, a rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente directiva, nomeadamente devido ao carácter incompleto ou inexacto desses dados;

como definidas no art. 2º “b” da Diretiva 95/46/CE.¹³ Em suma, revelar a importância das *Supervisory Authorities* para a interpretação e a eficácia das normas de proteção de dados pessoais nestes aspectos ressaltados *supra*.

2. O *Leading Case* Conhecido como “*Google Spain*” e a Decisão da Corte de Justiça de 13 de Maio de 2014

No caso em questão, questionava-se se a atividade desenvolvida pelos motores de busca poderia ser considerada coleta, tratamento e armazenamento de dados, e consequentemente, estaria sujeita à legislação de proteção de dados pessoais.

O caso originou-se na Espanha, em 24 de maio de 2007 (Proc. no. TD/00463/2007)¹⁴ sendo que um cidadão espanhol solicitou a desindexação de informações relativas ao fato de ter sido processado por débitos devidos à Seguridade Social. Ocorre que, na execução fiscal, o espanhol teve alguns imóveis vendidos em hasta pública. Estes fatos ocorreram em 1998 e, na época, foram publicados pelo Jornal *La Vanguardia Ediciones SL*, um veículo de comunicação de grande circulação na Espanha.

Porém, muito embora o fato tivesse ocorrido a mais de dez anos, o reclamante foi surpreendido com a indexação desta notícia quando utilizava a ferramenta de busca da *Google*. Assim, mesmo a notícia tendo sido veiculada de forma lícita pelo jornal espanhol, *La Vanguardia*, ao interessado parecia um abuso de direito que estes acontecimentos permanecessem em destaque na relação resultante da ferramenta de busca quando um internauta digitasse o nome dele.

Consequentemente, o reclamante ingressou com uma reclamação perante a *Agência Espanhola de Proteção de Dados – AEPD*, em 2007 solicitando que seus dados não aparecessem indexados na página do site de busca *Google Spain*:

El demandante ejerció su derecho de oposición en reiteradas ocasiones, mediante correos electrónicos, para que se procediera a la exclusión de sus datos personales de los índices de resultados elaborados por Google. que manifestó que “la solución dependía del BLOQUEO de la página de donde salen los resultados, por el titular de la Web referenciada (es decir, por la Diputación Provincial de).”¹⁵

13 b) «Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

14 Disponível em: <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2007/common/pdfs/TD-00463-2007_Resolucion-de-fecha-20-11-2007_Art-ii-culo-17-LOPD_Recurrida.pdf>, acessado em 24 de maio de 2015.

15 *Idem ibidem* (caso disponível em arquivo eletrônico no site da *AEPD*).

No caso, entendeu-se que não há o que pedir em face do jornal *La Vanguardia*, posto que a notícia veiculada à época era verídica e relevante. Porém, quanto ao pedido contra a *Google Spain*, a *AEPD* concluiu que sendo uma ferramenta de busca, realiza a coleta, tratamento e armazenamento dos dados pessoais e que está sujeita à legislação de proteção de dados que garante ao interessado o cancelamento de suas informações quando forem irrelevantes.¹⁶

Nesta decisão de 20 de novembro de 2007, a Agência Espanhola de Proteção de Dados, *RESOLUCIÓN Nº. R/01046/2007*, estabeleceu um marco ao reconhecer que o indivíduo tem direito de seus dados não constarem nas ferramentas de busca (*derecho all ovido*) com fundamento na dignidade da pessoa humana:¹⁷

En efecto, si atendiendo a motivos fundados y legítimos relacionados con circunstancias personales, el tratamiento de datos personales afecta a la dignidad de la persona, la LOPD y la LSSI le reconocen la posibilidad de ejercer el derecho de oposición directamente ante el buscador, el cual deberá adoptar medidas adecuadas para que retire los datos de sus índices e impida el acceso futuro a los mismos (TD/00463/2007).

A *Google Spain* recorreu desta decisão perante a Corte de Justiça da União Europeia, questionando, entre outras questões: 1) se as ferramentas de busca realizam atividades descritas no artigo 2º, alínea “b” da Diretiva 95/46/CE; 2) se o operador desta ferramenta de busca pode ser considerado responsável pelo tratamento dos dados nos termos da Diretiva 95/46/CE; e 3) se a *Google* estaria sujeita à lei espanhola e poderia ser processada e condenada por um órgão espanhol pois sua sede está em outro país, inclusive não sendo membro da União Europeia.

Em razão da complexidade do caso, serão analisados estes três questionamentos. Na sentença da Corte de Justiça da União Europeia de 13 de maio de 2014¹⁸, entendeu-se:

16 Para ter acesso a um estudo detalhado sobre o tema, *vide*: LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. In: *Revista dos Tribunais*, ano 103, vol. 946, agosto de 2014, p. 77 – 109. _____; NUNES, Lydia Neves Bastos Telles (coords.). *Estudos avançados de direito digital*. Rio de Janeiro, Elsevier, 2014. Material complementar no site: LIMA, Cíntia Rosa Lima de. Direito ao esquecimento e marco civil na internet. Disponível em <http://elsevier.com.br/site/produtos/Detalhe-Produto.aspx?tid=95308&seg=4&cat=207&tit=ESTUDOS%20AVAN%20ADOS%20DE%20DIREITO%20DIGITAL>. Acesso em 13.11.14.

17 Disponível em: <http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2007/memoria_AEPD_2007.pdf>, acessado em 24 de maio de 2015.

18 Disponível em: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/3._Sentencia_Gran_Sala_de_13_de_mayo_de_2014._Asunto_C-131-12._Google_v_AEPD_y_Mario_Costeja.pdf>, acessado em 10 de maio de 2015: “SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 13 de mayo de 2014 «Datos personales — Protección de las personas físicas en lo que respecta al tratamiento de dichos datos — Directiva 95/46/CE — Artículos

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. 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. 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.

Este julgamento foi importante por três aspectos: primeiro pela caracterização de tratamento de dados (que será abordada no item 4 deste artigo); reconhecimento do direito subjetivo à desindexação (interpretação do art. 14 da Dir. 95/46/CE); e, por fim, por entender que a legislação aplicável e foro competente são definidos no local onde a empresa tiver um estabelecimento, não necessariamente a sua sede, podendo ser a filial (nos termos do art. 4º da Dir. 95/46/CE).

2.1. A Interpretação dada ao Art. 14 “a” e Art. 7 “e” e “f” da Diretiva 95/46/CE

O art. 14 da *Personal Data Protection Directive* (Dir. 95/46/CE) estabelece alguns direitos dos titulares dos dados. Na alínea “a”, garante-se o direito de opor-se ao tratamento de seus dados pessoais:

Los Estados miembros reconocerán al interesado el derecho a: a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernen sean objeto de tratamiento, salvo cuando la

2, 4, 12 y 14 — Ámbito de aplicación material y territorial — Motores de búsqueda en Internet — Tratamiento de datos contenidos en sitios de Internet — Búsqueda, indexación y almacenamiento de estos datos — Responsabilidad del gestor del motor de búsqueda — Establecimiento en territorio de un Estado miembro — Alcance de las obligaciones de dicho gestor y de los derechos del interesado — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7 y 8».

legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

O art. 7º da referida diretiva estabelece algumas exceções em que se permite o tratamento de dados: na alínea “e”, entende-se permitido o tratamento realizado com a finalidade de interesse público e finalidade social; e na alínea “f”, entende-se que o tratamento de dados pode ser permitido desde que não prejudique direitos e garantias fundamentais do titular dos dados.

Desta forma, o tribunal sempre deve analisar o direito à desindexação do titular do dado em confronto com outros direitos e garantias fundamentais, tais como o direito à liberdade de expressão e o direito à informação. Nota-se que se o fato não tiver mais relevância social ou interesse público, deve prevalecer a proteção dos dados garantindo ao titular o direito à desindexação fundado na dignidade da pessoa humana.

Neste sentido, Franco Pizzetti¹⁹ destaca que o pedido de indexação não será legítimo quando tal tratamento seja motivado por um interesse público, *in verbis*:

Diventa di conseguenza essenziale per la Corte individuare quali siano le finalità del trattamento di deindicizzazione dei dati personali sui motori di ricerca, se non altro per verificare se, in ragione di tali finalità, il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 7, lettera c), ovvero sia necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure dei terzi a cui vengono comunicati i dati.

No caso em tela, a Corte de Justiça europeia confirmou o entendimento da AEPD e quanto a estes dois quesitos, o tribunal entendeu que: 1) sobre a atividade das ferramentas de busca na internet (*search engines*), trata-se de medida de tratamento de dado nos termos do artigo 2º, alínea “b” da Diretiva 95/46/CE, porque a Google recupera, registra e organiza estes dados, sendo que tais condutas se encaixam no conceito de “tratamento de dados” estabelecido na norma comunitária; e 2) sobre a responsabilidade do operador desta ferramenta de busca, o Tribunal de Justiça entendeu que o provedor deste aplicativo de busca pode ser considerado responsável pelo tratamento dos dados nos termos do art. 2º, “d” da Diretiva 95/46/CE.²⁰

¹⁹ *Op. cit.*, p. 815.

²⁰ d) «Responsável pelo tratamento», a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinadas por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário;

2.2. Competência e Legislação Aplicável na Transferência Transfronteiriça de Dados

Outro aspecto importante da decisão em análise foi a interpretação que a Corte de Justiça europeia deu ao art. 4º, “a” da Dir. 95/46/CE, que reza:

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. 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;

O elemento de conexão para definir a legislação aplicável e o tribunal competente para processar e julgar com fundamento nesta Diretiva é a existência de um “estabelecimento” do responsável pelo tratamento de dados pessoais no Estado Membro da União Europeia.

Neste caso, a Diretiva é bem clara ao utilizar o termo “estabelecimento” e não “sede”. Portanto, de forma correta, a Corte de Justiça europeia entendeu que a *Google Inc.* tem sede na Califórnia, porém tem uma filial na Espanha, a *Google Spain*, e por isso, está sujeita ao Direito Comunitário porque a Espanha é um Estado membro e, também, está sujeita às leis espanholas sobre proteção de dados pessoais.

No caso, o Tribunal europeu constatou que a *Google Spain* realiza atividades no território Espanhol, inclusive com a instalação de uma filial da *Google Inc.* no território espanhol e, portanto, tem-se por satisfeito o elemento de conexão definido no art. 4º, “a” da Dir. 95/46/CE. No item “2” do dispositivo, o Tribunal conclui:

El artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro.

Este tema é um dos maiores desafios do legislador no que tange alguns aspectos da internet, que desconhece limites geográficos e, por isso, a solução mais adequada seria estabelecer tratados internacionais sobre o tema. Desta forma, este conflito restaria mitigado haja vista que existiria uma uniformização das regras sobre proteção de dados pessoais.

Sobre o tema, importante destacar o resultado do Grupo de Trabalho, *Working Party WP29 n. 148*, de 04 de abril de 2008, sobre a proteção de dados pessoais quanto aos motores de busca na internet. Neste documento, observou-se que a atividade dos motores de buscas multinacionais, como é o caso da *Google* que tem sede na Califórnia (Estados Unidos), mas destina seus serviços e sites a várias nações do mundo, deve-se aplicar o direito local se o provedor multinacional utiliza meios, automatizados ou não, situados no território de um Estado membro para o tratamento de dados.²¹

Além disso, em se tratando de matéria de proteção de dados, considera-se um direito fundamental estabelecido na Carta de Direitos Fundamentais da União Europeia, o que reforça a aplicação da Diretiva 95/46/CE sobre proteção de dados pessoais, ainda que o provedor for multinacional.²²

3. A Atuação da Autoridade Garantidora da Proteção de Dados Pessoais Espanhola em Diversos Casos em Face da *Google Spain*

Este caso tornou-se muito relevante e conhecido porque, devido ao recurso interposto pela *Google*, a questão foi decidida pela Corte de Justiça europeia. Porém, a *AEPD* já tinha realizado um importante estudo sobre as atividades dos buscadores na internet e concluiu em 1º de dezembro de 2007 um estudo denominado “*Declaración sobre buscadores de Internet*”.²³

A Espanha internacionalizou a Diretiva 95/46/CE através da *Ley Orgánica 15/1999*, de 31 de dezembro, sobre a *Protección de Datos de Carácter Personal (LOPD)*. O escopo da lei espanhola é sistematizar as regras sobre proteção de direitos e garantias fundamentais das pessoas físicas notadamente com relação a sua honra, intimidade pessoal e familiar quanto ao tratamento de dados.

O objetivo da lei espanhola de proteção de dados não é limitar o uso de informação, mas sim de garantir a coleta, o tratamento e o armazenamento dos dados pessoais de maneira adequada.²⁴

21 Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf>, acessado em 25 de maio de 2015.

22 RAMIRO, Mónica Arenas. Capítulo 12 - El alcance del Derecho al Olvido en Internet. In: TORRIJOS, Julián Valero (coord.). *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Thomson Reuters, 2013. pp. 325 – 380. p. 346.

23 Disponível em: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracion_AEPD_buscadores.pdf>, acessado em 22 de maio de 2015.

24 GARCÍA, Daniel Santos. *Nociones generales de la Ley Orgánica de Protección de Datos: práctica jurídica*. Madrid: Tecnos, 2005. p. 37.

Semelhantemente ao art. 4º “a” da Dir. 95/46/CE, o art. 2.1 da *LOPD* determina que basta que o tratamento de dados seja feito em território espanhol ou se tenha um estabelecimento neste território. No caso, não resta dúvida de que a *Google Spain* é uma filial da *Google Inc.* estabelecida em território espanhol, cujo alvo são cidadãos espanhóis, mantendo sua página identificada como “*Google Spain*”.

Assim, pode-se afirmar com tranquilidade que as normas elencadas na *LOPD* aplicam-se a *Google Spain* que se destina ao público espanhol além de ter uma filial neste país.

No título VI (arts. 35 a 42) da lei espanhola de proteção de dados pessoais, disciplina-se a atuação da *Agencia Española de Protección de Datos – AEPD*, definida, no art. 35, como “*un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones*”.

Portanto, a *AEPD* atua não só na fiscalização do cumprimento das normas de proteção de dados pessoais, mas de maneira proativa e preventiva, evitando que determinadas violações aos direitos e garantias fundamentais dos titulares dos dados ocorram por tratamento indevido dos dados.²⁵

Esta agência é um órgão independente e tem várias atribuições. Primeiro destaca-se o denominado “*procedimiento sancionador*”, ou seja, o art. 48 da *LOPD* determina que tal procedimento inicia de ofício por denúncia de um ou de vários indivíduos prejudicados ou por um acordo do Diretor da agência quando tenha conhecimento de um fato presumidamente ilícito nos termos da lei. Tal procedimento é regido pelas regras gerais de Direito Administrativo nos termos do Decreto Real 1.398/1993, de 4 de agosto.²⁶

A agência pode impor sanções que variam segundo a gravidade das infrações, que podem ser leves, graves e muito graves. Assim, o valor da multa estabelecida no art. 45 da *LOPD* varia segundo a gravidade da conduta.²⁷

E por fim, os indivíduos que se sintam lesados em razão de violação das normas de proteção de dados pessoais podem reclamar seus direitos mediante petição por escrito à *AEPD*, que instaurará um procedimento de inspeção dando à outra parte oportunidade de defender-se das alegações do autor da reclamação. Ao final, deve realizar uma audiência e concluir o procedimento em um prazo máximo de 06 (seis) meses. Nota-se extremamente

25 RAMIRO, Mónica Arenas. *Op. cit.*, p. 347.

26 MARCOS, Isabel Davara Fernández de. *Hacia la estandarización de la protección de datos personales*. Madrid: La Ley, 2011. p. 392.

27 NÚÑEZ, Eloy Velasco. Medidas restrictivas en internet: cómo retirar contenidos ilícitos. In: REILLY, Marcelo Bauzá; MATA, Federico Bueno de (coords). *El Derecho en la Sociedad Telemática: estudios en homenaje al profesor Valentín Carrascosa López*. Santiago de Compostela: Andavira, 2012. pp. 139 – 164. p. 161.

importante a atuação da agência espanhola de proteção de dados no sentido de complementar a LOPD e garantindo sua eficácia.²⁸

Além disso, a agência realiza estudos e levantamento de dados específicos para definir regras de boas condutas. Os códigos tipos, também denominados deontológicos ou códigos de boas condutas ou boas práticas resultam da necessidade de autorregulamentação no contexto das novas tecnologias. O art. 27 da Dir. 95/46/CE estabelece a elaboração destes códigos tipos, que foi transposto pelo direito espanhol no art. 32 da LOPD, que estabelece que:

Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, [...].

Esta atribuição foi determinante para que a AEPD realizasse um estudo aprofundado sobre as ferramentas de busca na internet e concluisse que as atividades realizadas por estas ferramentas incluem-se na definição de tratamento de dados, determinada no art. 3, “c” da LOPD, *in verbis*: “*Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*”.

Em virtude da grande importância das ferramentas de busca, que são os aplicativos de internet mais utilizados, a agência espanhola deparou-se com o confronto entre os direitos dos usuários em obterem informações e o direito do sujeito dos dados em resguardá-los tendo em vista sua dignidade humana.

Assim, neste documento, a AEPD²⁹ conclui:

- 1. Los buscadores de Internet son servicios de la sociedad de la información sujetos a las garantías de la Ley Orgánica de Protección de Datos, además de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.*
- 2. Los buscadores de Internet tratan y retienen grandes volúmenes de datos de los usuarios a los que ofrecen sus servicios.*

28 MARCOS, Isabel Davara Fernández. *Op. cit.*, p. 403.

29 Disponível em: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracion_AEPD_buscadores.pdf>, acessado em 22 de maio de 2015.

3. El tratamiento de dicha información puede permitir registrar las actividades que el usuario lleva a cabo en la red posibilitando configurar perfiles de éste que pueden ser utilizados por la empresa sin que el usuario sea consciente ni esté suficientemente informado.

[...]

8- Los servicios de búsqueda están obligados a respetar los derechos de cancelación y oposición de personas cuyos datos se indexan desde otras páginas web en su función de buscador. Aunque la incorporación inicial de esta información personal a la red pueda estar legitimada en origen, su mantenimiento universal en Internet puede resultar desproporcionado.

4. Tratamento de Dados sob a Ótica das Autoridades Garantidoras e da Corte de Justiça Europeia

A atividade desenvolvida pelas ferramentas de busca já despertou o interesse de diversas comunidades. No Direito Comunitário europeu, o Grupo 29 – WP29 realizou diversos estudos sobre a proteção dos dados pessoais quanto às ferramentas de busca. Na opinião n. 136, de 20 de junho de 2007, foi reconhecido que a atividade das ferramentas de busca deve ser considerada como tratamento de dados.³⁰

Inclusive, neste documento destacou-se que a proteção dos dados pessoais deve ser tutelada como um direito e garantia fundamental. Ademais, as normas sobre o tema não podem ser consideradas estáticas porque as tecnologias evoluem constantemente, portanto, é natural que as normas sobre proteção de dados pessoais sejam interpretadas à luz das novas tecnologias que surgem constantemente. Neste ponto, destaca-se o importante papel das Autoridades Garantidoras que desenvolvem políticas públicas e critérios para a interpretação e aplicação das normas sobre proteção de dados.

Desta forma, o WP29 conclui na *Opinion n. 136*³¹ que:

National Data Protection Supervisory Authorities play an essential role in this respect in the framework of their missions of monitoring the application of data protection law, which involves providing interpretation of legal provisions and concrete guidance to controllers and data subjects. They should endorse a definition that is wide enough so that it can anticipate evolutions and catch all “shadow zones” within its scope, while making legitimate use of the flexibility contained in the Directive.

³⁰ Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>, acessada em 24 de maio de 2015.

³¹ *Idem ibidem*, p. 05.

No ano seguinte, o WP29 realizou estudos específicos sobre a proteção de dados pessoais no contexto dos motores de busca na internet, culminando na *Opinião n. 148, de 04 de abril de 2008*.³² Neste documento, fica clara que as ferramentas de busca caracterizam-se como tratamento de dados e, por isso, estão sujeitas à legislação de proteção de dados pessoais. Então, o WP29 neste documento conclui que as ferramentas de busca podem revelar um fato da vida privada do indivíduo que não mais seja relevante e a associação de tantas informações revelam dados sensíveis da intimidade e vida privada. Por isso, o titular de tais dados tem direito ao acesso de tais dados, bem como de corrigi-los ou apagá-los, *in verbis*:

When applied specifically to search engines, users must have the right to access any personal data stored about them according to Article 12 of the Data Protection Directive (95/46/EC), including their past queries, data gathered from other sources and data revealing their behaviour or origin. The Article 29 Working Party considers that it is essential that search engine providers provide the necessary means for the exercise of these rights, by means, for instance, of a web based tool that allows registered users direct access online to their personal data and provides the possibility of opposing certain data processing.

Secondly, the right to correct or delete information also applies to some specific cache data held by search engine providers, once these data no longer match the actual contents published on the Web by the controllers of the website(s) publishing this information. In such a situation, upon receiving a request from a data subject, search engine providers must act promptly to remove or correct incomplete or outdated information. The cache can be updated by an automatic instant revisit of the original publication. Search engine providers should offer users the possibility to request removal of such content from their cache, free of charge.

Por isso, tanto a AEPD quanto a *Autorità Garante della Protezione dei Dati Personali* italiana consideram que as ferramentas de busca na internet realizam atividades caracterizadas como tratamento de dados pessoais, e, por isso, estão sujeitas à legislação de proteção de dados pessoais.³³

No mesmo sentido, a Corte de Justiça europeia considera que as ferramentas de busca na internet realizam tratamento de dados e, portanto, estão sujeitas à lei de proteção de dados pessoais.

4.1. As Ferramentas de Busca Caracterizadas como Tratamento de Dados

As ferramentas de busca (*search engines*) coletam informações que são inseridas na rede e relaciona tais informações com os parâmetros de pesquisa inseridos pelos usuários. Por isso, não resta dúvida que tal conduta caracteriza-se como tratamento de dados.

³² *Op. cit.*, p. 23.

³³ PIZZETTI, Franco. *Op. cit.*, p. 813.

No caso, corretamente, o tribunal europeu concluiu que a atividade do motor de busca da empresa *Google* na internet, enquanto fornecedor de conteúdos, ou seja, a sua atividade consiste em localizar a informação publicada ou inserida na rede por terceiros (parâmetros de busca) e indexá-la automaticamente. Além disso, a empresa armazena tal informação por tempo indefinido, colocando-a a disposição dos internautas observada certa ordem de preferência. Em suma, as condutas realizadas pela empresa são mencionadas no art. 2º, “b” da Diretiva 95/46/CE, o que impõe a aplicação das normas de proteção de dados a tais atividades.

4.2. O Direito Subjetivo do Indivíduo à Desindexação de suas Informações Pessoais (Art. 12 “b” e Art. 14 “a” da Diretiva 95/46/CE)

Uma vez caracterizado o motor de busca como tratamento de dados, passa-se à análise dos direitos dos titulares dos dados. Em outras palavras, se o usuário teria direito de acesso a suas informações, bem como direito de corrigi-las e apagá-las nos termos dos arts. 14 “a” e 12 “b” da Diretiva 95/46/CE respectivamente.

Tais direitos são assegurados pela legislação de proteção de dados pessoais, o que se aplica em face das ferramentas de busca. O problema é como tais direitos podem ser exercidos?

As leis de proteção de dados pessoais garante direitos aos titulares dos dados, prevendo inclusive medidas para que possam pleitear seus direitos seja perante a Autoridade Garantidora, seja perante o Poder Judiciário. O direito assegurado no art. 14 “a” da Dir. 95/46/CE permite que o titular se oponha aos dados que estiverem sendo utilizados ilicitamente por quem quer que seja, ressalvadas as hipóteses de interesse público. Além de se opor, o titular pode solicitar a correção, quando suas informações estiverem erradas; ou o cancelamento de suas informações (art. 12 “b” da Dir. 95/46/CE).

A legislação utiliza termos abrangentes porque inviável pensar que a cada termo tecnológico novo, cada *software* novo que administram dados pessoais etc, o Legislador tenha que atualizar a legislação vigente. Por isso, entendemos que o direito ao cancelamento assegurado no direito comunitário europeu, bem como no art. 16 da LOPD, fundamenta o direito à desindexação de informações pessoais que não sejam mais atuais e nem relevantes sob o ponto de vista histórico, artístico e cultural e se não prejudicar o interesse público.

Neste sentido foi a conclusão do Tribunal de Justiça europeu no caso *Google Spain*, bem como grande parte da doutrina desenvolvida sobre o tema.³⁴ Resta evidente que a

³⁴ PIZZETTI, Franco. *Op. cit.*, p. 816.

AEPD exerceu um papel muito importante quanto aos estudos realizados sobre o tema, para que o tribunal chegasse a tal conclusão. Isto porque estas agências são independentes e atuam de maneira vocacionada com a finalidade precípua de fiscalizar o cumprimento das leis de proteção de dados pessoais, bem como estabelecer códigos de boas condutas como exposto acima.

Assim, mais fácil será alterar o conteúdo de códigos de boas condutas que poderão prever regras novas a partir da evolução das novas tecnologias sem ter que alterar a legislação sobre proteção de dados pessoais. Isto porque ao término do processo legislativo para fazer determinada atualização específica na lei, ela não será mais necessária porque, fatalmente, outras tecnologias surgirão e demandarão outras medidas.

5. Impacto do Caso *Google Spain* na Sociedade Brasileira

O *Marco Civil da Internet* (MCI), como é conhecida a Lei n. 12.965/2014, que estabelece direitos e garantias dos usuários da internet no Brasil não pode ser considerada uma lei sobre proteção de dados pessoais. Isto porque devido à complexidade do tema, como se observa da experiência do Direito Comunitário europeu, demanda um microsistema com princípios e regras específicos.

No entanto, esta legislação brasileira menciona em muitos de seus dispositivos regras principiológicas de proteção de dados pessoais. A saber, o artigo 7º, incisos VIII e IX³⁵, que dispõem que para a coleta e o uso dos dados pessoais dever-se-á contar com o consentimento informado e expresso do seu titular; inciso X³⁶ que garante o direito à exclusão de dados pessoais, além de outros dispositivos de caráter geral.

Atualmente, discute-se um anteprojeto de lei brasileiro sobre proteção de dados pessoais (APL PDP). Quanto ao âmbito de aplicação da norma, o art. 2º do anteprojeto considera o local do tratamento dos dados onde o titular se encontrava no momento da coleta.

35 CAPÍTULO II - DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

36 X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

Dir. 95/46 CE	LOPD (ES)	APL PDP (BR)
Artigo 4º 1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de <u>un establecimiento del responsable del tratamiento en el territorio del Estado miembro</u>. 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;	Artículo 2. <i>Ámbito de aplicación.</i> 1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a) <u>Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.</u> [...]	Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, <u>independentemente do país de sua sede e do país onde esteja localizado o banco de dados</u>, desde que: I - a operação de tratamento <u>seja realizada no território nacional</u>; ou II - os dados pessoais objeto do tratamento tenham sido <u>coletados no território nacional</u>. § 1º Consideram-se coletados no território nacional os dados pessoais <u>cujo titular nele se encontre no momento da coleta</u>.

Neste ponto, não nos parece razoável esta regra e um tanto obscura. Isto proque os buscadores na internet (tratamento automatizado) realizam suas atividades cotidianamente, o que inviabilizará a aplicação da norma, vez que o titular pode estar em trânsito ou em vários lugares nos vários momentos da coleta em razão da ubiquidade.

Portanto, nos parece mais lógica a regra do art. 4º da Diretiva 95/46/CE e do art. 2º da LOPDP espanhola que estabelece a ideia de “estabelecimento”. Neste ponto particular, o direito comunitário europeu deveria influenciar e servir de base para o direito pátrio brasileiro. Porém, a palavra “estabelecimento” comporta a possibilidade de um estabelecimento virtual o que comprometeria esta regra. Neste caso, nos parece melhor adotar o critério do público alvo como foi destacado no caso *Yahoo!Fr*, ou seja, se o site é todo traduzido na língua daquele território e se identifica com o público do território, a lei nacional será aplicada bem como o tribunal competente será definido pelas leis locais.³⁷

37 Como o tema sobre jurisdição competente e legislação aplicável (elementos associados à soberania nacional, portanto, ligados à ideia de território geográfico) é por si complexo e demanda um estudo a parte, o que não é possível neste artigo. Desta forma, vide: LIMA, Cíntia Rosa Pereira de Lima. *Op. cit., passim*.

Além disso, busca-se a harmonização das regras relacionadas aos temas de internet, que desconhece limites geográficos, daí interessante o diálogo entre vários países para que as experiências mais bem-sucedidas possam ser aproveitadas por outros países que ainda não adotaram uma legislação de proteção de dados pessoais como o Brasil.

Quanto aos direitos dos usuários, o direito ao acesso e ao cancelamento (ou exclusão) das informações pessoais já estão elencados no Marco Civil da Internet como destacado *supra*. Todavia, no APL PDP brasileiro, art. 17, incisos II e IV garantem-se, respectivamente, o direito de acesso e o direito ao cancelamento, neste particular, bem-parecido com o direito comunitário europeu.

Importante destacar que o APL PDP brasileiro usa um termo que não é utilizado na Diretiva 95/46/CE e nem tão pouco na LOPD espanhola, que é a “dissociação” (destacado *infra* no quadro comparativo entre as redações das respectivas leis). De modo que, a nosso ver, o Direito Brasileiro é mais claro ao garantir o direito à indexação, porque além de utilizar “retificação” e “exclusão”, adiciona outro “dissociação”, que está muito próximo ao sentido da palavra “desindexação”. Em suma, é um ponto importante e que o Brasil poderá influenciar o Direito comunitário europeu, corroborando com o fundamento legal ao direito à desindexação.

Dir. 95/46 CE	LOPD (ES)	MCI (BR)
Artigo 12º Direito de acesso: Os Estados-membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento: [...] b) Consoante o caso, a <u>rectificação, o apagamento ou o bloqueio</u> dos dados cujo tratamento não cumpra o disposto na presente directiva, nomeadamente devido ao carácter incompleto ou inexacto desses dados;	Artículo 16. Derecho de rectificación y cancelación. <i>1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de <u>rectificación o cancelación del interesado en el plazo de diez días.</u></i>	Art. 7º [...] <u>X - exclusão definitiva</u> dos dados pessoais que tiver fornecido a determinada aplicação de internet, <u>a seu requerimento, ao término da relação entre as partes</u> , ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
		APL PDP (BR) Art. 17. O titular dos dados pessoais tem direito a obter: [...] II - acesso aos dados; [...] e IV - <u>dissociação, bloqueio ou cancelamento</u> de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.

Muito embora o anteprojeto de lei brasileiro sobre proteção de dados pessoais não mencione especificamente as ferramentas de busca, a definição de tratamento de dados estabelecida no art. 5º, inc. II³⁸ do APLPDP remete-nos à definição do direito comunitário europeu, de maneira que se pode concluir que as ferramentas de busca desenvolvem tais atividades descritas na definição de tratamento de dados.

Dir. 95/46 CE	LOPD	Anteprojeto de Lei de PDP
Artigo 2º b) «Tratamento de dados pessoais» («tratamento»), <u>qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados</u> , tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;	Artigo 2.1 “ <i>Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias</i> ”.	Artigo 5º II - tratamento: <u>conjunto de ações referentes</u> a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;

Por fim, o APLPDP brasileiro não estabelece a criação de um órgão independente, apenas menciona em diversos artigos a atuação do “órgão competente”, sem indicar qual seria este órgão.

6. Conclusões

A proteção dos dados pessoais é um tema que, muito embora tenha sido destaque em diversos organismos internacionais que trataram do tema, ainda hoje impõe desafios para o Legislador e para os operadores do Direito. A *Strasbourg Convention* n. 108, de

38 II - tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;

28 de janeiro de 1981, sobre proteção de dados pessoais, deixou claro que nesta matéria apenas leis não seriam suficientes.

Esta é a conclusão que pode ser retomada quando analisamos o caso conhecido como *Google Spain*, em que o Tribunal de Justiça europeu, no julgamento de 13 de maio de 2014, entendeu que as ferramentas de busca realizam condutas descritas em lei como tratamento de dados, ou seja, coleta, produção, recepção, classificação, utilização, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração que pode ser feita de maneira automatizada ou não.

Sendo assim, os operadores dos sites de busca são responsáveis pelo tratamento de dados pessoais, e, por isso, deve atender os pedidos e reclamações dos titulares que tenham suas informações indexadas, expondo dados, muitas vezes, desatualizados e socialmente irrelevantes.

Interessante que o art. 16 da LOPD espanhola determina o prazo célere de 10 dias para que o responsável pelo tratamento de dados atenda à solicitação do indivíduo. A celeridade na resposta a estes tipos de demanda é de fundamental importância porque em minutos uma determinada informação pode ser transmitidas simultaneamente em todos os continentes do planeta. O anteprojeto de lei brasileiro sobre proteção de dados pessoais não menciona nenhum prazo, mas esta lacuna deveria ser preenchida antes da aprovação do texto de lei.

Por outro lado, o APL PDP brasileiro é inovador ao garantir ao usuário o direito à “dissociação”, ou seja, o direito à “desindexação”. No entanto, antes da entrada em vigor deste diploma, a nosso ver, o direito à desindexação exercido em face dos operadores das ferramentas de busca na internet tem amparo sob o fundamento do art. 7º, inc. X do Marco Civil da Internet.

Em suma, neste tema, há uma forte tendência em uniformizar as legislações evitando situações desproporcionais em que a lei de determinado país é extremamente benéfica aos operadores dos sites de busca em detrimento dos direitos dos usuários e titulares dos dados. O ideal é a garantia de direitos semelhantes em vários países em virtude da internet ser utilizada como um mecanismo de comunicação essencialmente transfronteiriço.

Por esta razão, basta que estes operadores das ferramentas de busca alvejem a população de determinado território para estar sujeito às leis e à jurisdição local; bem como sujeitos às autoridades competentes para fiscalizar o cumprimento das normas de proteção de dados pessoais daquele país. O julgamento do caso *Google Spain* pelo Tribunal de Justiça europeu revela a importância da atuação destes órgãos para que a decisão do tribunal seja cumprida.

7. Referências

- COLOMBO, Matteo. *Regolamento UE sulla Privacy: principi generali e ruolo del data protection officer*. Milão: Associazione Data Protection Officer, 2015.
- DEAN, Tami R; CIELOCHA, Kristin M; HANDSFIELD, Lara J. Becoming Critical Consumers and Producers of Text: Teaching Literacy with Web 1.0 and Web 2.0. *Reading Teacher*, 2009, Vol.63 (1), p. 40 - 50.
- GARCÍA, Daniel Santos. *Nociones generales de la Ley Orgánica de Protección de Datos: práctica jurídica*. Madrid: Tecnos, 2005.
- MARCOS, Isabel Davara Fernández de. *Hacia la estandarización de la protección de datos personales*. Madrid: La Ley, 2011.
- NÚÑEZ, Eloy Velasco. Medidas restrictivas en internet: cómo retirar contenidos ilícitos. In: REILLY, Marcelo Bauzá; MATA, Federico Bueno de (coords). *El Derecho en la Sociedad Telemática: estudios en homenaje al profesor Valentín Carrascosa López*. Santiago de Compostela: Andavira, 2012. pp. 139 – 164.
- PIZZETTI, Franco. Le Autorità Garanti per la Protezione dei Dati Personali e la Sentenza della Corte di Giustizia sul Caso Google Spain: è Tempo di Far Cadere il “Velo di Maya”. In: *Il Diritto dell’informazione e dell’informatica*, 2014, fasc. 4-5, Giuffrè, pp. 805 – 829.
- LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. In: *Revista dos Tribunais*, ano 103, vol. 946, agosto de 2014, p. 77 – 109.
- _____; NUNES, Lydia Neves Bastos Telles (coords.). *Estudos avançados de direito digital*. Rio de Janeiro, Elsevier, 2014. Material complementar no site: LIMA, Cintia Rosa Lima de. Direito ao esquecimento e marco civil na internet. Disponível em <http://elsevier.com.br/site/produtos/Detailhe-Produto.aspx?tid=95308&seg=4&cat=207&tit=ESTUDOS%20AVAN%20ADOS%20DE%20DIREITO%20DIGITAL>. Acesso em 13.11.14.
- RAMIRO, Mónica Arenas. Capítulo 12 - El alcance del Derecho al Olvido en Internet. In: TORRIJOS, Julián Valero (coord.). *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Thomson Reuters, 2013. pp. 325 – 380.
- REILLY, Marcelo Bauzá; MATA, Federico Bueno de (coords). *El Derecho en la Sociedad Telemática: estudios en homenaje al profesor Valentín Carrascosa López*. Santiago de Compostela: Andavira, 2012.

- RICCIO, Giovanni Maria. *La responsabilità civile degli internet providers*. Torino: G. Giappichelli Editore, 2002.
- TAPSCOTT, Don; WILLIAMS, Anthony D. *Wikinomics: how mass collaboration changes everything*. New York: Penguin Group, 2006.
- THE ECONOMIST. *Data, data everywhere*. A special report on managing information. Disponível em: <<http://www.emc.com/collateral/analyst-reports/ar-the-economist-data-data-everywhere.pdf>>
- TORRIJOS, Julián Valero (coord.). *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Thomson Reuters, 2013.
- ZITRAIN, Jonathan. *The future of the internet and how to stop it*. Virginia: Yale University Press, 2008.