Universidade do Minho
Escola de Direito

João Alexandre Silva Alves Guimarães

O REGIME JURÍDICO DO DIREITO AO ESQUECIMENTO (OU À DESINDEXAÇÃO) NA UNIÃO EUROPEIA E A SUA REPERCUSSÃO NO DIREITO BRASILEIRO

julho de 2019

O REGIME JURÍDICO DO DIREITO AO ESQUECIMENTO (OU À DESINDEXAÇÃO) NA UNIÃO EUROPEIA E A SUA REPERCUSSÃO NO DIREITO BRASILEIRO
João Alexandre Silva Alves Guimarães
UMinho | 2019

Universidade do Minho
Escola de Direito

João Alexandre Silva Alves Guimarães

O REGIME JURÍDICO DO DIREITO AO ESQUECIMENTO (OU À DESINDEXAÇÃO) NA UNIÃO EUROPEIA E A SUA REPERCUSSÃO NO DIREITO BRASILEIRO

Dissertação de Mestrado
Mestrado em Direito da União Europeia

Trabalho efetuado sob a orientação da
Professora Doutora Alessandra Silveira

julho de 2019

AGRADECIMENTOS

Após concluir a presente investigação, não poderia deixar de agradecer a algumas pessoas que fizeram parte desta caminhada e contribuíram para o seu êxito. Em primeiro lugar a Deus que me abençoou e colocou na minha vida a oportunidade de fazer este mestrado.

À Professora Doutora Alessandra Silveira, que desde o primeiro dia que estive em Portugal, como aluno de Mobilidade Internacional, me apoiou, me encorajou a fazer este mestrado e se prontificou sempre a ouvir minhas dúvidas – às quais gentilmente respondeu – e sem a qual a presente investigação nunca teria existido.

Aos meus pais, Élcio Alves Guimarães e Cléia Brígida da Silva Alves Guimarães, que me deram todo o apoio, carinho e amor, me incentivaram a prosseguir esse sonho, e foram sempre um local de refúgio, um porto seguro – e mesmo diante da distância se fizeram presentes. Papai, mamãe, o meu muito obrigado – amo-vos muito.

À minha querida irmã Ana Júlia Silva Alves Guimarães, que sempre me apoiou e incentivou em todos os momentos. Até fez música, ajudou-me e foi a melhor ouvinte nos momentos de dificuldade. Amo-te, minha pequena.

Aos familiares que enviaram mensagens de carinho e de apoio enquanto estive longe. Aos amigos que, de alguma forma, entre as idas e vindas Portugal/Brasil, estiveram presentes com palavras de ânimo, com incentivos e debates sobre o assunto, obrigado por escutarem ou lerem o que eu estava a dizer ou escrever.

Por fim agradeço à Escola de Direito da Universidade do Minho, através de todos os professores do Mestrado em Direito da União Europeia e todos os funcionários, que de alguma forma acrescentaram conhecimento e ajudaram no desenvolvimento desta investigação – recebam a minha gratidão.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO:

O REGIME JURÍDICO DO DIREITO AO ESQUECIMENTO (OU À DESINDEXAÇÃO) NA UNIÃO EUROPEIA E A SUA REPERCUSSÃO NO DIREITO BRASILEIRO

O presente estudo aprecia a evolução e a concretização do direito ao esquecimento (entendido como desindexação) na União Europeia, o seu sentido, propósito, fundamento e alcance. São analisados a Diretiva 95/46/CE (relativa ao tratamento de dados pessoais e a sua circulação no espaço da União Europeia) e o atual Regulamento (UE) 2016/649 que a revogou (Regulamento Geral de Proteção de Dados), bem como a jurisprudência do Tribunal de Justiça da União Europeia (TJUE), sobretudo o acórdão Google Espanha (C-131/12) de 2014, no qual o TJUE reconheceu o direito à desindexação/desassociação/deslistagem exercido contra os motores de busca na Internet. A partir do âmbito de aplicação material e territorial do RGPD, esta dissertação procura escrutinar em que medida a evolução do direito à proteção de dados pessoais informatizados (sobretudo no que diz respeito ao direito ao esquecimento ou à desindexação) tem servido de inspiração e influenciado a legislação e jurisprudência noutras latitudes (muito especialmente no Brasil). O trabalho tem por intuito demonstrar que um entendimento amplo de esquecimento desenvolvido no âmbito dos *mass media* tradicionais não se compadece com o atual desenvolvimento do direito à desindexação (nos termos em que o mesmo vem sendo concretizado pelo Direito da União Europeia), na medida em que a desindexação não retira informações da internet, apenas obriga o motor de busca a deixar de indexar/conectar o internauta aos dados pessoais do titular que o solicita, através da supressão de uma hiperligação.

Palavras-chaves: desindexação; direito ao esquecimento; motores de busca; proteção de dados pessoais no Brasil; Regulamento (UE) 2016/679.

ABSTRACT:

THE LEGAL REGIME OF THE RIGHT TO BE FORGOTTEN (OR TO DE-INDEXATION) IN THE EUROPEAN UNION AND ITS REPERCUSSION IN BRAZILIAN LAW

This study examines the evolution and realization of the right to be forgotten (understood as de-indexation) in the European Union, its meaning, purpose, foundation and scope. Directive 95/46/EC (concerning the processing of personal data and its movement within the European Union) and the current Regulation (EU) 2016/649, which repealed it (General Data Protection Regulation), as well as the case-law of the Court of Justice of the European Union (CJEU), in particular the Google Spain judgment (C-131/12) of 2014, in which the CJEU recognized the right to de-indexation / disassociation / delisting against internet search engines. From the material and territorial scope of the RGPD, this dissertation seeks to investigate the extent to which the evolution of the right to the protection of computerized personal data (especially with regard to the right to forgetfulness or de-indexation) has inspired and influenced the legislation and jurisprudence in other latitudes (especially in Brazil). The aim of this work is to demonstrate that a broad knowledge of forgetted developed within the traditional mass media is not in keeping with the current development of the right to de-indexation (as it has been achieved by European Union law), insofar as that the deindexation does not remove information from the Internet, only obliges the search engine to stop indexing / connecting the Internet user to the personal data of the holder who requests it, by deleting a hyperlink.

Keywords: deindexation; protection of personal data in Brazil; Regulation (EU) 2016/679; right to be forgotten; search engines.

ÍNDICE

INTRODUÇÃO

A internet pode ser considerada uma marca positiva no mundo porque, entre outros benefícios, dá aos indivíduos acesso à informação necessária para tomar decisões (tendencialmente) informadas. Ademais, a internet permite que as massas sejam ouvidas de maneira eficaz através de redes sociais. As pessoas estão mais conectadas e visíveis do que nunca. A internet permite velocidade e eficiência num grande número de processos, desde compras até importantes funções governamentais. No entanto, a internet também levou a uma grande coleta/recolha, retenção e catalogação de informações pessoais que representam uma séria ameaça à privacidade pessoal.[1]

Em um mundo tão tecnológico, a coleta de dados tornou-se uma das atividades mais recorrentes e de crescimento mais rápido, abrangendo diversas indústrias e facetas da vida quotidiana. Todos os dias criamos 2,5 quintilhões de bytes de dados, tanto que 90% dos dados existentes hoje foram criados entre 2014 e 2015.[2]

Pode dizer-se que a internet, nos dias atuais, é uma rede complexa, que se assemelha a uma teia de aranha, em que dois pontos são conectados por milhares de caminhos potenciais. Se uma mensagem não puder seguir o caminho mais curto e simples entre o remetente e o destinatário, ela poderá ser reencaminhada ao longo de qualquer outro caminho disponível. A distância entre os pontos pode ser longa, mas pelo facto de os sinais eletrónicos viajarem tão rápido, a diferença de tempo é insignificante. Assim, uma mensagem de correio eletrónico pode viajar pelo mundo e chegar a um computador a menos de um quilômetro de distância.[3]

A internet, de forma global, é cada vez mais utilizada e alimentada com um excessivo número de informações, especialmente de cunho pessoal, possibilitando que nada seja esquecido. Antigamente, quem desejasse manter o anonimato precisava apenas impedir que seu nome e número de telefone constassem das listas telefónicas, vulgarmente conhecidas por “páginas amarelas”. Porém, atualmente, mesmo tomando todas as medidas em prol da preservação da privacidade, é praticamente muito difícil

[1] Corrado, John. Not Forgetting Just Obscuring: American and European Attempts to Maintain Privacy in the Digital Age. Cardozo Journal of Internactional and Comparative Law, Volume 1, p. 308, 2018.
[2] Kitain, Jessica. Beware of Wearables: Protecting Privacy in a Data-Collecting World. Drexel Law Review Online, p. 1, 2016.
[3] Eoyang, Mieke. Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance. Journal of National Secutity Law & Policy, p. 263, 2017.

mantê-la. Uma informação que antes poderia levar meses ou até mesmo anos para ser adquirida, pode agora ser consultada com facilidade, estando à disposição dos utilizadores de internet.[4]

Cada página consultada, pelo telefone móvel, tablet ou computador, envia uma quantidade absurda de informações a quem a requisitou. Não se trata apenas de informações produzidas pelas grandes companhias, pois cada utilizador tem um perfil e, para melhor complementá-lo, são utilizadas as suas ligações, mensagens, cartões de crédito, viagens. Estes dados ficam armazenados para serem utilizados, seja como forma de publicidade, para saber os gostos e desejos de seus utilizadores, seja como forma de melhorar produtos, mapear o trânsito, a medicina, ou qualquer outro serviço existente que possa dar utilidade a estes dados.[5]

Viktor Mayer-Schönber afirma que enquanto estamos constantemente esquecendo e reconstruindo elementos do nosso passado, a generalidade dos internautas continua a acessar a lembrança digital e os factos que não foram reconstruídos. Assim, como o passado que lembramos vai mudando e evoluindo, o passado capturado na memória digital é constante e permanece congelado no tempo. É provável que essas duas visões entrem em choque, ou seja, a memória congelada que os outros têm sobre nós e a memória emergente em evolução que carregamos em nossas mentes. Nenhuma delas é uma representação precisa e completa do que somos. A primeira está trancada no tempo, enquanto a última, a interpretação do passado da nossa mente, é fortemente influenciada por quem somos no presente.[6]

Isto suscita-nos duas frases muito comuns no quotidiano dos internautas "uma vez na internet, para sempre na internet" ou "na internet nada se apaga". Essas frases corroboram a ideia de que a capacidade de armazenamento, seja por meios eletrônicos como nuvens ou por dispositivos físicos tornou-se praticamente ilimitada.

Schönberger afirma que as novas tecnologias fazem o ato de esquecer, que antes era regra, virar exceção. Por isso precisamos de mecanismos, legais e tecnológicos, para encontrar o equilíbrio. Não se trata apenas de perdoar atitudes questionáveis, mas de

[4] Souza, Bernardo de Azevedo e. Direito, Tecnologia e Práticas Punitivas. Porto Alegre: Canal Ciências Criminais, Posição 488 – 489 (Kindle Edition), 2016.
[5] De Alcantara, Larissa Kakizaki. Big Data e Internet das Coisas: Desafios de Privacidade e da Proteção de Dados no Direito Digital. São Paulo: Bok2, Posição 149 - 155 (Kindle Edition), 2017.
[6] Mayer-Schönberger, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press; Edição: Revised ed. for Kindle, p. 106 - 107, 25 de julho de 2011.

aceitar que ações comuns, como as de tirar fotos ou entabular conversas privadas, se porventura descontextualizadas não podem ser critério para definir o caráter ou a competência de alguém. O referido autor defende que as pessoas tenham total controle sobre as suas pegadas digitais: fotografias poderiam ter data de validade e ser apagadas depois de um certo tempo.[7]

Essa problemática nos conduz ao direito ao esquecimento (ou, mais concretamente, ao direito à desindexação, como explicaremos), um direito de que dispõe o titular de dados pessoais informatizados, integrado no mais complexo e abrangente direito fundamental à proteção de dados pessoais, previsto no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE).[8] Em Portugal, ainda antes de a CDFUE adquirir força juridicamente vinculativa em 2009, a proteção dos cidadãos perante o tratamento de dados pessoais informatizados foi consagrada no artigo 35.º da Constituição da República Portuguesa (CRP), no sentido de densificar, como explicam Gomes Canotilho e Vital Moreira, o moderno direito à autodeterminação informacional, dando a cada pessoa o direito de controlar a informação disponível a seu respeito e impedindo-a de transformar-se em simples objeto de informações.[9]

Na tentativa de captar a evolução do direito que nos ocupa, podemos recuar a Warren e Brandeis em 1890, segundo os quais, nos primórdios, a propriedade assegurava ao indivíduo o poder sobre as suas terras e o seu gado. Gradativamente foi sendo reconhecida a natureza espiritual do homem, os seus sentimentos e o seu intelecto. Assim, o âmbito de proteção da liberdade e da segurança se ampliou – o direito à vida passou a significar o direito a aproveitar a vida e o direito a não ser importunado; o direito à liberdade passou a assegurar o exercício de amplos privilégios civis; o direito à propriedade cresceu para abranger todas as formas de posses – intangíveis e tangíveis.[10]

Daí a tempos mais atuais, a autodeterminação informacional foi reconhecida pela CRP sob a epígrafe "Utilização da informática" em 1976, sendo então pioneira na consagração constitucional de direitos que especificamente protegem os dados pessoais

[7] Mayer-Schönberger, Viktor. Página 2.
[8] Castro, Caratina Sarmento e. A Jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspectivas para o direito ao esquecimento na Europa. Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos. Volume 1, Almedina, p. 1051, 2016.
[9] Canotilho, J.J. Gomes; Moreira, Vital. Constituição da República Portuguesa Anotada: Artigos 1º a 107º. Volume I, 4º edição revista. Coimbra Editora, p. 551, 2007.
[10] Warren, Samuel D.; Brandeis, Louis D.. The Right to Privacy. Harvard Law Review, Vol. IV (Nº. 5), 15 de Dezembro de 1890. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

dos cidadãos em relação ao uso das novas tecnologias. Como a epígrafe indicia, o artigo 35.º da CRP veio regular juridicamente problemas levantados pelo uso do computador, constituindo uma primeira expressão, com dignidade constitucional, do Direito da Informática ou, talvez, hoje, preferivelmente, do Direito da Eletrônica.[11]

O desenvolvimento e crescente uso dos meios tecnológicos que deixam "pegadas eletrônicas" tornam cada vez mais importantes as garantias contra o tratamento e a utilização abusiva de dados pessoais informatizados.[12] A sua relação de tensão com vários direitos, liberdades e garantias – tais como o desenvolvimento da personalidade, a dignidade da pessoa, a intimidade da vida privada – é inquestionável.[13]

Sendo assim, o direito de conhecer a finalidade ou "a que se destinam" os dados pessoais informatizados recorta-se, hoje, como um direito à autodeterminação informativa de particular relevo. Ou seja, trata-se de um direito à autodeterminação sobre informações referentes a dados pessoais que exige uma proteção clara quanto ao "desvio dos fins" a que se destinam essas informações.[14]

De uma forma global, o direito previsto no art. 35.º da CRP consagra a proteção dos cidadãos perante o tratamento de dados pessoais informatizados. A fórmula sobre o "tratamento" abrange não apenas a individualização dos dados, mas também a sua conexão, transmissão, utilização e publicação. O enunciado linguístico *dados* é o plural da expressão latina *datum* e está utilizada na Constituição Portuguesa no sentido que hoje lhe empresta a ciência informática como representação convencional de informação, sob a forma analógica ou digital possibilitadora do seu tratamento automático.[15]

Posteriormente, o Parlamento Europeu e o Conselho, em 1995, adotam a Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A Diretiva 95/46 foi adotada com dois objetivos principais: proteger o direito fundamental à proteção de dados, e garantir o livre fluxo de informações pessoais entre os Estados-Membros. Este último objetivo permitiu à UE conseguir uma maior harmonização da proteção de dados, exigindo que cada

[11] Castro, Catarina Sarmento e. 40 anos de "Utilização da Informática": O artigo 35.º da Constituição da República Portuguesa. e-Pública, Lisboa, v. 3, n. 3, p. 44, dez. 2016. Disponível em <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S2183-184X2016000300004&lng=pt&nrm=iso>.
[12] Canotilho, J.J. Gomes; Moreira, Vital. Página 550.
[13] Canotilho, J.J. Gomes; Moreira, Vital. Página 551.
[14] Canotilho, J.J. Gomes; Moreira, Vital. Página 553.
[15] Canotilho, J.J. Gomes; Moreira, Vital. Página 550.

Estado-Membro adotasse legislação nacional para proteger "os direitos e liberdades fundamentais das pessoas singulares." A diretiva exigiu que qualquer empresa sediada na UE cumprisse regras específicas para o processamento e a transferência de dados do consumidor europeu – o que promoveu um significativo avanço para a livre circulação no âmbito do mercado interno – além de conceder aos consumidores determinados direitos em relação aos seus dados pessoais, como o direito de ser notificado de todos os usos e divulgações sobre dados, colheita e processamento, e o direito de corrigir ou excluir dados pessoais.[16]

Entre os direitos constantes da diretiva destaca-se o direito de apagamento ou eliminação – o qual permite que um individuo requeira o apagamento de dados "incompletos, imprecisos ou armazenados de maneira incompatível com os propósitos legítimos buscados pelo responsável pelo tratamento".[17] Além disso, o artigo 12.º da Diretiva de Proteção de Dados previa: "Os Estados-Membros devem garantir a todos os titulares de dados o direito de obter do responsável pelo tratamento, conforme apropriado, a retificação, a eliminação ou o bloqueio dos dados ...". Ademais, o artigo 2.º definia o responsável pelo tratamento como "a pessoa física ou jurídica, a autoridade pública, a agência ou qualquer outro órgão que, individualmente ou em conjunto com outros, determina os propósitos e meios do processamento de dados pessoais". Desta forma, a diretiva permitia que os indivíduos exercessem algum controle sobre os seus dados pessoais que são processados por corporações, outras entidades, ou até mesmo por outros indivíduos.[18] Assim, a Diretiva 95/46 consagrou que quando um dado perde a finalidade para a qual foi recolhido, ou findo o prazo que estava estabelecido para o seu armazenamento, o mesmo deve ser apagado imediatamente, reconhecendo assim o direito ao apagamento.

O acórdão Google, proferido em sede de reenvio prejudicial para os efeitos de interpretação de normas da Diretiva 95/46, tornou-se um marco e referência dentro da UE sobre a temática que nos ocupa e exemplo para muitos países. A partir da decisão do TJUE, iniciou-se a discussão sobre o tratamento de dados pessoais pelos motores de

[16] Curtiss, Tiffany. Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies. Washington Journal of Law, Technology & Arts, p. 98 - 99, 2016.
[17] Parlamento Europeu e do Conselho. Directiva 95/46/CE. Luxemburgo, 24 de outubro de 1995. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>.
[18] Brougher, Jordan D.. The Right to be Forgotten: Applying European Privacy Law to American Eletronic Health Records. Indiana Health Law Review, p. 520 - 521, 2016.

pesquisa e consolidou-se o chamado "direito ao esquecimento" – que corresponderia à aplicação do direito ao apagamento, fixado na diretiva, aos motores de busca online.

O Tribunal de Justiça da União Europeia (TJUE) reconheceu que a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, colocar à disposição dos internautas por determinada ordem de preferência deve ser qualificada de "tratamento de dados pessoais", quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado "responsável" pelo dito tratamento.[19]

Neste julgamento o TJUE consagrou o direito à "desindexação" que permite ao titular do direito requerer uma "deslistagem" aos motores de busca, ou seja, a "desassociação" ou supressão de uma hiperligação, a retirada de um determinado resultado. Porém os veículos de notícias divulgaram-no como "direito ao esquecimento", pois quando se retira um resultado de uma pesquisa, ele acabaria sendo "esquecido" em relação às inúmeras outras informações que o motor de busca listou.

Motivo pelo qual o Regulamento 2016/679, conhecido como Regulamento Geral de Proteção de Dados (RGPD), coloca como título do artigo 17.º «Direito ao apagamento dos dados ("direito a ser esquecido")». Porém o n.º 2.º deste artigo 17.º, bem como a explicação desse direito no Ponto 66 das considerações do RGPD, ao referir a expressão "supressão de ligações", sugere que o direito a ser esquecido corresponderia a uma aplicação do direito ao apagamento (que se exerce offline) à esfera digital (agora exercido online) especialmente contra os motores de busca (desindexação):

> "Para reforçar o direito a ser esquecido no ambiente por via eletrónica, o âmbito do direito ao esquecimento deverá ser alargado através da imposição ao responsável pelo tratamento que tenha tornado públicos os dados pessoais da adoção de medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais

[19] Tribunal de Justiça da União Europeia. Acordão Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González – Processo C-131/12, 13 de maio de 2014. Disponível em < http://curia.europa.eu/juris/document/document.jsf?text=&docid=153853&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=8125412>.

de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos.”.[20]

A ideia do direito ao esquecimento como um direito mais amplo, ligado muito mais aos direitos de personalidade (à privacidade, à honra, à imagem, à palavra, etc.) do que ao atual direito à desindexação, tem origem num programa no canal televisivo alemão Zweites Deutsches Fernsehen – ZDF. Tal canal televisivo produziu um documentário que contava o julgamento do Caso Lebach, ocorrido em 1969 na Alemanha, em cujo processo dois réus foram condenados à prisão perpétua pela morte de quatro soldados que protegiam um depósito de armas e munições, porém um terceiro elemento, partícipe do crime, recebeu pena de reclusão de seis anos.[21] O Tribunal Constitucional Alemão, em 1973, decidiu que os veículos mediáticos não deveriam ocupar-se da figura e vida privada do criminoso por tempo ilimitado, proibindo que a emissora veiculasse aquele documentário na grade de sua programação, acatando a pretensão dos condenados.[22]

Porém, o que foi reconhecido pelo TJUE, através do acórdão Google, seria algo distinto. O TJUE entendeu que o resultado obtido pelo mecanismo de busca através da ligação entre dois ou mais termos é fruto de um tratamento de dados. Pois, ao combinar habilmente dados de login, cookies e endereços de IP, o Google é capaz de conectar a pesquisa a um determinado indivíduo ao longo do tempo e com impressionante precisão – a conexão entre quem procura a informação e os resultados da pesquisa é promissor o suficiente para que o internauta aceda aos links indexados.[23]

Um ser humano levaria inúmeras horas para acessar todas essas fontes de informação sequencialmente e compilar um dossiê abrangente, enquanto os mecanismos de busca integrados tornariam isso um caso rápido, simples, fácil e sem custos. Todavia, mesmo se todos os resultados apresentados a partir da busca forem perfeitamente precisos, o fruto da busca não corresponde à essência atual de uma pessoa, mas a uma composição estranhamente artificial de factos da vida, consistindo apenas de informação

[20] Parlamento Europeu e o Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Disponível em < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>.
[21] Camargo, Coriolano Almeida; Santos, Cleórbete. Direito Digital: novas teses jurídicas. Rio de Janeiro, Lumen Juris, p.51, 2018.
[22] Bundesverfassungsgericht. BVerfGE 35, 202 – Lebach, de 5 de junho de 1973. Disponível em < https://germanlawarchive.iuscomp.org/?p=62>.
[23] Mayer-Schönberger, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press; Edição: Revised ed. for Kindle, p. 6, 25 de julho de 2011.

que é disponível em formato digital, deixando de fora todo o resto, ou seja, a vivência do facto ali apresentado.[24]

O problema é que tais resultados são baseados em probabilidades. Eles ligam tenuemente os indivíduos a certas preferências. O resultado é uma versão digital e muito ampliada do juízo por associação, uma vez que inferências baseadas em características individuais correspondentes são usadas para julgar e apresentar uma lista de resultados.[25]

Cabe ressaltar que os sites que editam e armazenam conteúdo, que são indexados nos mecanismos de busca, desfrutam da liberdade de expressão e permitem o direito à informação ao público. O prejuízo inicia na falta de interesse público – e o lapso de tempo permite ao indivíduo a quem tal conteúdo se relaciona o direito de pleitear a sua eliminação e consequente a desindexação. É verdade que grande parte da informação é, embora em menor escala, de algum interesse para algumas pessoas, ou que tal conteúdo faz parte da coleção histórica da sociedade, como na biblioteca digital do jornal. Assim, parece raro se deparar com um caso claro e simples de supremacia do direito ao esquecimento.[26]

Por outro lado, há um dano evidente para o indivíduo que tem seu nome levantado nos resultados de pesquisa feitos pelos mecanismos de busca, porque às vezes o conteúdo está totalmente fora do contexto original e o resultado da pesquisa leva a sites que o usuário que fez a pesquisa nem imaginava existir.[27]

Portanto é necessário entender que não há decisão editorial dos sites que publicaram jornalisticamente um conteúdo no passado para divulgá-lo novamente em um momento posterior. O mecanismo de pesquisa é responsável por avançar entre milhares de outros conteúdos que preenchem determinados critérios de pesquisa e mostram páginas que podem prejudicar o direito de alguns indivíduos. Assim, é possível afirmar que os mecanismos de busca são responsáveis "pelo fornecimento de conteúdo potencialmente infrator aos direitos fundamentais da personalidade por apresentar como

[24] Mayer-Schönberger, Viktor. Página 104.
[25] Mayer-Schönberger, Viktor. Página 105.
[26] Silvestre, Gilberto Fachetti; Borges, Carolina Biazatti; Benevides, Nauani Schades. The Procedural Protection of Data De-Indexing in Internet Search Engines: The Effectiveness in Brazil of the So-Called "Right to be Forgotten" Against Media Companies. Revista Jurídica, [S.l.], v. 1, n. 54, p. 40, mar. 2019.
[27] Silvestre, Gilberto Fachetti; Borges, Carolina Biazatti; Benevides, Nauani Schades. Página 40.

resultado de pesquisa informações que não demonstrem interesse público atual devido à imprecisão e anacronismo".[28]

Se o conteúdo da página original do site não for excluído ou editado, mas apenas desindexado dos resultados da pesquisa, haverá, por um lado, a manutenção do conteúdo original, embora com menos visibilidade, sacrificando em menor medida, as liberdades comunicativas e reconhecendo o valor histórico da informação, e, por outro lado, a criação de dificuldades para acessar as páginas indiscriminadamente, ou seja, páginas que não estão relacionadas com o contexto original de um conteúdo potencialmente prejudicial para o indivíduo a que se refere.[29]

Ou seja, o direito à desindexação é o direito que permite a um indivíduo que se sente prejudicado por um resultado, através de uma busca com seu nome juntamente com um determinado termo, solicitar ao motor de busca a desindexação de um ou mais resultados – ou seja, ao aparecer a lista de resultados, alguns deles serem suprimidos e não existir uma hiperligação a um determinado link.

Esse direito é de todos aqueles que estejam no espaço da UE que se sentir prejudicado. O TJUE reconheceu que os motores de busca fazem o tratamento para cada resultado e para cada usuário que procura a informação por forma a ser mais compatível com o seu perfil. Aquele que se sentir prejudicado exerce esse direito contra o motor de busca, por meio extrajudicial através das Autoridades Nacionais de Proteção de Dados – contra o Google existe a possibilidade para pedir a desindexação através de um site denominado "Transparecy Report" (que esse trabalho irá explicar a frente) – ou finalmente por via judicial.

Assim, o direito ao esquecimento (ou à desindexação) é um direito fundamental da pessoa humana na UE, integrado no âmbito da proteção de dados pessoais, hoje regulamentado pelo RGPD. Cabe ressaltar que o esquecimento, no sentido do acórdão Google do TJUE, deve ser interpretado como desindexação, pois qualquer outra forma não condiz com a fundamentação legislativa ou jurisprudencial no território dos Estados-Membros.

[28] Silvestre, Gilberto Fachetti; Borges, Carolina Biazatti; Benevides, Nauani Schades. Página 40.
[29] Silvestre, Gilberto Fachetti; Borges, Carolina Biazatti; Benevides, Nauani Schades. Página 41.

Este trabalho pretende demonstrar os motivos pelos quais o direito ao esquecimento na internet tem particularidades que o afastam daquele sentido amplo, associado aos tradicionais *mass media* e a um amplo leque de direitos de personalidade, como habitualmente entendido na doutrina e jurisprudência brasileiras. Apesar da expressão algo equivocada, o "direito a ser esquecido" do artigo 17.º do RGPD transporta para o online o que o direito ao apagamento já assegurava offline. Mas quando o "esquecimento" é exercido contra os motores de busca no sentido do acórdão Google, então converte-se num direito à desindexação ou à supressão de uma hiperligação – nada além disso – pois ninguém pode ser definitivamente esquecido na internet.

1. DA AUTODETERMINAÇÃO INFORMACIONAL AO DIREITO AO ESQUECIMENTO COMO DESINDEXAÇÃO

A consagração de um conjunto de pretensões jurídico-políticas denominado direito de proteção de dados surge em um contexto internacional de crescente percepção da informação relativa aos indivíduos, no âmbito da utilização da informação relativa aos indivíduos, e da utilização de meios informáticos para o desenvolvimento humano nas sociedades democráticas.[30]

O direito à proteção de dados apresenta-se essencialmente como um direito de garantias de um conjunto de valores fundamentais individuais de que se destacam a privacidade e a liberdade, em poucas palavras, a autodeterminação individual.[31]

Assim, o artigo 35º da Constituição da República Portuguesa (CRP) veio reconhecer, no âmbito da utilização da informática, o direito à autodeterminação informativa, que se traduz no direito a conhecer a informação que sobre cada um de nós é tratada, ou no direito de saber que dados pessoais estão a ser recolhidos, utilizados, conservados, comunicados e para que finalidade e ainda por quem estão a ser tratados, de modo a que o cidadão detenha ou retome o controle sobre os seus dados.[32]

A primeira vez que se ouviu o termo autodeterminação informacional em Portugal foi na CRP de 1976. A redação deste artigo sofreu grandes alterações desde a sua inclusão no texto constitucional justificadas pela natureza da matéria a regular e pela necessidade de adaptar o conteúdo da regulamentação às normas e diretivas comunitárias que foram entrando em vigor neste domínio – esta necessidade fez-se particularmente sentir em relação à Diretiva n.º 95/46 do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares face ao tratamento de dados pessoais e à livre circulação desses dados.[33]

A sua versão original de 1976 era constituído de três números onde consagrou-se o direito de informação e acesso do titular dos dados pessoais, que consistia em "tomar conhecimento do que constar dos registos mecanográficos a seu respeito", então ainda

[30] Calvão, Filipa Urbano. O Direito Fundamental à Proteção dos Dados Pessoais e a Privacidade 40 Anos Depois. Jornadas nos quarenta anos da Constituição da República Portuguesa – Impacto e Evolução, Manuel Afonso Vaz, Catarina Santos Botelho,Luís Heleno Terrinha, Pedro Coutinho (Coord.), Universidade Católica Editora, p. 87, 2017.
[31] Calvão, Filipa Urbano. Página 89.
[32] Calvão, Filipa Urbano. Página 89.
[33] Mirada, Jorge; Medeiros, Ruy. Constituição Portuguesa Anotada. Volume I, 2º ed., Revista – Lisboa: Universidade Católica Editora, p. 565, 2017.

desenhado sem quaisquer limitações e no mesmo número institui-se o seu direito de retificação e de atualização dos dados. Foi importante a consagração da ideia da finalidade a que se destinam os dados, que permanecerá como princípio enformador e calibrador dos tratamentos de dados pessoais, além de estabelecer a proibição do tratamento de dados que versasse sobre convicções políticas, fé religiosa e vida privada, ressalvando os casos em que o seu tratamento fosse meramente estatístico e proibir a instituição de um número nacional único identificativo de cada cidadão.[34]

Relativamente ao texto original constante do artigo 35.º, o legislador na revisão de 1982 foi sensível à evolução tecnológica e substituiu a referência a "registos mecanográficos" por "registos informáticos". Esta revisão passa a estar em consonância com o funcionamento das bases de dados, algumas de porte considerável, já em funcionamento, abandonando-se a referência à mecanografia, ou seja, a referência offline. A alteração ilustrou bem a necessidade de adaptação do texto constitucional a um novo tempo, substituindo-se uma redação que a todos os cidadãos dava o direito de tomar conhecimento do que constasse de registos mecanográficos a seu respeito, para lhes dar o mesmo direito, agora, relativamente aos registos informatizados.[35]

Em 1989 procedeu-se uma nova alteração da redação do artigo em ordem a permitir o fluxo transfronteiriço de dados pessoais, que era proibido na redação anterior, salvo nos casos previstos na lei.[36]

A segunda revisão constitucional, através da Lei Constitucional n.º 1/89, foi reflexo das normas previstas na Convenção 108, aprovada a 28 de janeiro de 1981, do Conselho da Europa, para a proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados de carácter pessoal – e deixa, em 1989, de proibir de forma genérica os fluxos transfronteiras de dados pessoais, para prever que a lei regulará o fluxo de dados transfronteiras, estabelecendo formas adequadas de proteção. Assim, a maior exigência do texto constitucional de 1982, que instituíra como regra a proibição, admitindo exceções, passa a consagrar uma regra que se aproxima da norma menos exigente da Convenção que, no artigo 12.º, n.º 1, previa os fluxos transfronteiras de dados, embora admitisse derrogações.[37]

[34] Castro, Catarina Sarmento e. Página 45.
[35] Castro, Catarina Sarmento e. Página 45.
[36] Mirada, Jorge; Medeiros, Ruy. Página 565.
[37] Castro, Catarina Sarmento e. Página 47.

O direito consagrado no artigo 35.º é um direito de defesa e um direito de liberdade com um conteúdo negativo, pois permite ao indivíduo decidir que, quando e em que condições poderá usar, ou tornar pública, informação que lhe diz respeito, o que dignifica a possibilidade de não revelar dados de natureza pessoal, ou de recusar o tratamento dessa informação em certas circunstâncias. Esse direito coloca em causa a tutela da reserva sobre factos cujo conhecimento por terceiros deve depender da decisão do seu titular, independentemente de respeitarem ao núcleo mais estrito da sua vida privada.[38]

O princípio do consentimento ou da autodeterminação é a pedra angular sobre a qual se estrutura o tratamento dos dados pessoais. Certo que não é a vontade do titular dos dados que define o nível de proteção a que eles ficam sujeitos, dependendo a proteção outorgada a cada tipo ou categoria de dados da vontade do legislador, mas existe um relação necessária entre o consentimento e a licitude da recolha e tratamento dos dados que apenas poderá ser afastada ou derrogada nos casos particulares previstos na lei.[39]

Além disso a proteção de dados constantes de ficheiros manuais, como descrito no artigo 35.º, é uma consequência lógica do alargamento do âmbito de proteção deste preceito, pois ele regula a proteção de quaisquer dados pessoais, como dados informativos armazenados em computadores isolados, dados em circulação na internet e dados recolhidos em ficheiros manuais. Cabe ressaltar que à autodeterminação informacional é um dos direitos, liberdades e garantias em que o seu destinatário direto não é somente o Estado e as entidades públicas em geral, mas também as entidades privadas detentoras de ficheiros de dados pessoais.[40]

Esse modelo de autodeterminação informacional, como modelo constitucional segue como forma de assegurar as faculdades individuais que integram o conteúdo essencial do direito à proteção dos dados pessoais perante o uso das novas tecnologias, principalmente da informática foi confirmada pelo em decisão jurisprudencial que marcou a construção do direito à autodeterminação informacional na Alemanha.[41]

O Tribunal Constitucional alemão considerou que integrava o conteúdo do direito geral de personalidade previsto pelo artigo 2.1 da Constituição da Alemanha, o

[38] Mirada, Jorge; Medeiros, Ruy. Página 572.
[39] Mirada, Jorge; Medeiros, Ruy. Página 574.
[40] Canotilho, J.J. Gomes; Moreira, Vital. Página 557.
[41] Mirada, Jorge; Medeiros, Ruy. Página 568.

direito à "proteção do indivíduo contra a recolha, armazenamento, utilização e transmissão dos seus dados pessoais sem restrições", conferindo, de igual modo, a cada cidadão a possibilidade de decidir sobre o abandono e a utilização dos seus dados pessoais.[42]

O Tribunal Constitucional Federal alemão, naquela ocasião, decidiu que:

> [...] no contexto do processamento de dados moderno, a proteção do indivíduo contra a coleta, armazenamento, uso e divulgação ilimitados de seus dados pessoais é abrangida pelos direitos pessoais gerais da constituição alemã. Este direito básico garante, a esse respeito, a capacidade do indivíduo de determinar, em princípio, a divulgação e o uso de seus dados pessoais. Limitações a essa autodeterminação informativa são permitidas apenas no caso de interesse público superior.[43]

A autodeterminação informacional tem como âmbito subjetivo a proteção das garantias do direito à privacidade, trata-se de um direito universal, como sucede com a generalização dos direitos, liberdades e garantias de natureza pessoal, sendo que todas as pessoas pelo facto de o serem, gozam desse direito.[44]

A revisão de 1997 fixou o texto atualmente em vigor no artigo 35.º da Constituição Portuguesa. As modificações foram sobretudo determinadas pela necessidade da transposição da Diretiva 95/46 para o direito interno, já que o teor de algumas normas constitucionais impedia a sua transposição para a ordem jurídica portuguesa, por conflitarem com a normativa europeia. Mas as modificações contemplaram, ainda, uma importante alteração, provocada pela expansão do uso da internet a que se assistiu nos anos 90.[45]

Porém, mesmo com a revisão do artigo em diferentes fases, houve uma evolução tecnológica notável em relação ao avanço da legislação. A criação científica e as vantagens que estão no nosso dia a dia na simplificação de uma série de atos da vida como

[42] Mirada, Jorge; Medeiros, Ruy. Página 568.
[43] Bundesverfassungsgericht (BVerfG). Volkszählungsurteil - BVerfGE 65 de 15 de dezembro de 1983.
[44] Canotilho, J.J. Gomes; Moreira, Vital. Páginas 557 - 558.
[45] Castro, Catarina Sarmento e. Página 48.

o pagamento de faturas nos ATM, do inglês: *Automated Teller Machine*, ou por via eletrônica, a aquisição de bens e serviços online, a aproximação das pessoas ou o encurtamento das distâncias, o acesso a melhores cuidados de saúde, o maior acesso ou acesso mais facilitado à informação e ao conhecimento, muito devido à internet.[46]

Esta evolução trouxe consigo novos desafios à privacidade – relacionados sobretudo com a exposição crescente e quase inevitável da vida de cada um, voluntária em muitos casos, nas redes sociais por exemplo, involuntária noutros, baseados em leis e regulamentos, tanto perante o Estado como perante as empresas, que por sua vez permitem ou são forçadas a disponibilizar os dados ao Estado. Se considerarmos o conjunto da informação pessoal recolhida pelas empresas quando navegamos na internet ou "interagimos" nas redes sociais, a partir dos *likes*, interesses, opiniões, localização, fotografias, círculo de amigos, restaurantes, hotéis, viagens, com os correspondentes dias e horas de reserva, bens adquiridos, ou quando usamos dispositivos para medir a batida cardíaca ou o nível de açúcar no sangue, os níveis detalhados de consumo de eletricidade ao longo do dia por máquina ou dispositivo que funcione a energia elétrica, que revela se está alguém em casa, ou ainda quanto vemos televisão (TV) e com isso revelamos quantas pessoas estão em casa, os programas vistos, e se pensarmos que pode ser usado para as mais variadas finalidades, por exemplo para marketing feito à medida do perfil do cliente, controlo do acesso à informação, vigilância da circulação no espaço público, etc., compreendemos que as empresas que oferecem as plataformas eletrônicas ou as tecnologias que servem para disponibilizar ou conservar esta informação são detentoras de um conhecimento muito exato sobre as pessoas – e, por vezes, tendo uma percepção mais exata da vida delas do que a que elas próprias detêm – justificando-se a afirmação de que a internet conhece-nos melhor do que nós próprios.[47]

Contudo, mesmo no novo quadro tecnológico e valorativo, a apreciação do artigo 35.º da CRP deve orientar-se pela descoberta sobre se, nesta relação de tensão, a tutela dos interesses do mercado, de eficiência, de investigação e de segurança justificam a aniquilação da privacidade, a adulteração da identidade pessoal, o condicionamento da liberdade individual e a perversão da democracia.[48]

[46] Calvão, Filipa Urbano. Página 91.
[47] Calvão, Filipa Urbano. Páginas 91 - 92.
[48] Calvão, Filipa Urbano. Página 95.

Desenvolvendo a invocação do interesse público da segurança como valor supremo cuja salvaguarda exige o sacrifício da liberdade e da autonomia individual, a alegação de que a transparência do Estado e do poder público é condição da democracia, que conduz à exigência de transparência da sociedade e portanto de cada cidadão, a somar à voluntária exposição na internet, resulta num tal grau de exposição da vida das pessoas, que é suscetível de conduzir à medieval aldeia global, onde não sobra espaço para a reserva ou privacidade.[49]

Mas da mesma forma, cabe ainda reformular o n.º 1 do artigo 35.º na parte relativa aos direitos de acesso, retificação e atualização, para enquadrar constitucionalmente outras dimensões jurídicas de tutela dos dados pessoais, como o direito à eliminação de dados ou o direito à desindexação. O reconhecimento desses direitos é cada vez mais essencial para se poder salvaguardar a privacidade das pessoas. Em um tempo que está vulgarizada a navegação na internet, a consideração da extensão de informação que aí fica para sempre, através da memória digital, poderá justificar o reconhecimento da natureza fundamental ao direito, já reconhecido no plano legal, de eliminação de informação ou, pelo menos, de nos motores de busca não se apresentar como resultado determinada informação a partir da identificação de uma pessoa.[50]

No âmbito União Europeia, a Convenção Europeia dos Direitos do Homem (CEDH) de 1950, que entrou em vigor em 1953, estabeleceu direito à proteção de dados pessoais como parte dos direitos tutelados, previsto no artigo 8.º da CEDH, garantindo o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência e estabelece as condições em que são permitidas restrições a este direito.[51]

Com o surgimento da tecnologia da informação na década de 60 foi acompanhado por uma crescente necessidade de adotar regras mais pormenorizadas para salvaguardar as pessoas através da proteção dos seus dados e os dados pessoais. Em meados da década de 70, o Comité de Ministros do Conselho da Europa adotou várias resoluções sobre a proteção de dados pessoais que faziam referência ao artigo 8.º da CEDH.[52] Em 1981, foi aberta a assinatura a Convenção para a proteção das pessoas

[49] Calvão, Filipa Urbano. Página 95.
[50] Calvão, Filipa Urbano. Página 97 - 98.
[51] Conselho da Europa. Convenção Europeia dos Direitos do Homem, STCE n.º. 005, 1950
[52] Conselho da Europa, Comité de Ministros (1973), Resolução (73) 22 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor privado, de 26 de setembro de 1973; CdE, Comité de Ministros (1974), Resolução

relativamente ao tratamento automatizado de dados de caráter pessoal, conhecida como a Convenção 108. Essa Convenção era o único instrumento internacional juridicamente vinculativo no domínio da proteção de dados.[53]

A Convenção 108[54] aplicou-se a todos os tratamentos de dados pessoais realizados tanto pelo setor privado como pelo setor público, incluindo os tratamentos de dados efetuados pelas autoridades policiais e judiciárias. Protegeu as pessoas contra os abusos que podem acompanhar a recolha e o tratamento de dados pessoais e procura simultaneamente regular o fluxo transfronteiriço de dados pessoais. Quanto à recolha e tratamento de dados pessoais, os princípios estabelecidos na Convenção respeitaram, em especial, à recolha e tratamento automatizado de dados de forma leal e lícita, armazenados para finalidades determinadas e legítimas, não podendo ser utilizados para fins incompatíveis com essas finalidades nem conservados por tempo superior ao necessário. Dizem também respeito à qualidade dos dados, estabelecendo, em especial, que têm de ser adequados, pertinentes e não excessivos (proporcionalidade), bem como exatos.[55]

Além de prever garantias relativas à recolha e tratamento de dados pessoais, a Convenção proibiu, na ausência de garantias jurídicas adequadas, o tratamento de dados «sensíveis», tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa.[56]

A Convenção consagrou igualmente o direito das pessoas a saberem que existem informações armazenadas a seu respeito e, se necessário, a que elas sejam retificadas. Só eram admitidas restrições aos direitos estabelecidos na Convenção quando estiverem em causa interesses superiores, como a proteção da segurança do Estado.[57]

Todos os Estados-Membros da UE ratificaram a Convenção 108. Em 1999, a Convenção foi alterada para permitir a adesão da União Europeia.[58] Em 2001, foi adotado um protocolo adicional à Convenção 108 que estabeleceu disposições sobre fluxos

(74) 29 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor público, 20 de Setembro de 1974.

[53] Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, p. 15 – 16, 2014.

[54] Conselho da Europa. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, Conselho da Europa, STCE n.º 108, 1981.

[55] Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, p. 16, 2014.

[56] Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, p. 16, 2014.

[57] Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, p. 16, 2014.

[58] Conselho da Europa. Alterações à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (STCE n.º 108) que permitem a adesão das Comunidades Europeias, adotadas pelo Comité de Ministros em Estrasburgo, em 15 de junho de 1999; artigo 23.º, n.º 2, da Convenção 108 na redação em vigor.

transfronteiriços de dados para Estados não signatários, os chamados países terceiros, e sobre a criação obrigatória de autoridades nacionais de controlo de proteção de dados.[59]

A Carta dos Direitos Fundamentais da União Europeia (CDFUE) autonomizou o direito à proteção de dados pessoais em seu artigo 8.º relativamente ao direito à proteção da vida privada no seu artigo 7.º.[60] Para o Direito da União Europeia, nem todos os dados pessoais são suscetíveis, pela sua natureza, de causar prejuízo à vida privada da pessoa em causa, mas todos devem ser igualmente protegidos. Pode traduzir então a relevância atribuída pela ordem jurídica europeia ao direito fundamental à proteção de dados pessoais, como um direito distinto ou autônomo relativamente àquele da proteção da vida privada. A CDFUE também dá um passo adiante em relação a várias Constituições dos Estados-Membros da União Europeia e também em relação à Convenção Europeia dos Direitos do Homem (CEDH) no domínio da proteção de dados, na medida em que consagra um direito fundamental que protege dados que não têm de ser privados e muito menos íntimos, basta que sejam pessoais.[61]

Cabe ressaltar que a competência da União Europeia para regular a matéria relativa à proteção de dados de carácter pessoal está previsto no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e relaciona-se com o adequado funcionamento do mercado interno.[62] Ou seja, a competência para o estabelecimento de normas relativas à proteção de dados decorre da necessidade de fazer circular informações pessoais entre os Estados-Membros, sendo uma consequência do bom funcionamento de

[59] Conselho da Europa. Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, STCE n.º 181, 2001.

[60] A CDFUE os prevê em seus artigos 7.º e 8.º:

Artigo 7.º

Respeito pela vida privada e familiar

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8º

Protecção de dados pessoais

1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[61] Silveira, Alessandra. Direitos humanos fundamentais originariamente protegidos offline mas exercidos online – e a recíproca, é verdadeira?. Direito & solidariedade, Elisaide Trevisam/Lívia Gaigher Bósio Campello (coords.), Editora Juruá, Curitiba, 2017

[62] O TFUE estabelece em seu artigo 16.º:

Artigo 16.º

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do Direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.

As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia.

um mercado interno e do aumento do fluxo transfronteiriço de dados, que acompanha a livre circulação de pessoas, mercadorias, serviços e capitais.[63]

Esta caracterização autônoma na Carta dos Direitos Fundamentais da União Europeia representou um afastamento notável da compreensão tradicional da proteção de dados como uma mera faceta do direito à privacidade. Agora reconhecida como um direito fundamental, a proteção de dados goza do mais alto status dentro da legislação da UE, juntamente com o restante dos direitos fundamentais igualmente reconhecidos pela Carta e sendo reafirmado no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que se refere em particular, à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições da UE.[64]

Em 1995, a União Europeia adotou a Diretiva de Proteção de Dados, Diretiva 95/46, com dois objetivos principais: proteger o direito fundamental à proteção de dados, e garantir o livre fluxo de informações pessoais entre os Estados-Membros. Este último objetivo permitiu à UE conseguir uma maior harmonização da proteção de dados, exigindo que cada Estado-Membro adotasse legislação nacional para proteger "os direitos e liberdades fundamentais das pessoas singulares.". A diretiva exigia que qualquer empresa sediada na UE cumprisse regras específicas para o processamento e a transferência de dados do consumidor europeu, concedendo aos consumidores determinados direitos em relação aos seus dados pessoais, como o direito de ser notificado de todos os usos e divulgações sobre dados, colheita e processamento, e o direito de corrigir ou excluir dados pessoais.[65]

A Diretiva 95/46 impunha certos requisitos de privacidade àqueles que coletam dados de utilizadores. Isso exigia, por exemplo, que as empresas protejam as informações pessoais com níveis de segurança adequados, e só possam transferir dados para outros países (ditos países terceiros) com um "nível adequado de proteção". Isto significou (e assim continua) que as empresas europeias que procuram utilizar serviços de países terceiros devem assegurar que a privacidade e a segurança dos dados são equivalentes aos praticados na UE.[66]

[63] Silveira, Alessandra. Direitos humanos fundamentais originariamente protegidos offline mas exercidos online – e a recíproca, é verdadeira?. Direito & solidariedade, Elisaide Trevisam/Lívia Gaigher Bósio Campello (coords.), Editora Juruá, Curitiba, 2017
[64] Peguera, Miquel. The Shaky Ground of the Right to Be Delisted. Vanderbilt Journal of Entertainment and Technology Law, Volume 18, Issue 3, 514-515, 2016.
[65] Curtiss, Tiffany. Página 99
[66] Curtiss, Tiffany. Página 99

Segundo o considerando 41 da Diretiva 95/46, "Todas as pessoas devem poder beneficiar do direito de acesso aos dados que lhes dizem respeito e que estão em fase de tratamento, a fim de assegurarem, nomeadamente, a sua exatidão e a licitude do tratamento.".[67] Em conformidade com estes princípios, as pessoas em causa deveriam ter o direito, nos termos da legislação nacional, de obterem do responsável pelo tratamento a retificação, o apagamento ou o bloqueio dos seus dados se considerarem que o seu tratamento não cumpre o disposto na Diretiva, nomeadamente devido ao caráter incompleto ou inexato desses dados.[68]

O artigo 2.º da Diretiva 95/46 trouxe as definições de dado pessoal como «qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa")" é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social», além do tratamento de dados como "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".

O artigo 12.º da mesma diretiva descreveu o Direito de Acesso, impondo aos Estados-Membros a obrigatoriedade de garantir às pessoas em causa o direito de obterem do responsável pelo tratamento:

> a) Livremente e sem restrições, com periodicidade razoável e sem demora ou custos excessivos:
>
> - a confirmação de terem ou não sido tratados dados que lhes digam respeito, e informações pelo menos sobre os fins a que se destina esse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados,

[67] Parlamento Europeu e o Conselho. Diretiva 95/46/CE, e 24 de outubro de 1995, considerando 41.
[68] Idem, artigo 12.º, al. b)

> - a comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados,
>
> - o conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito, pelo menos no que se refere às decisões automatizadas referidas no nº 1 do artigo 15º;
>
> 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;
>
> c) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos da alínea b), salvo se isso for comprovadamente impossível ou implicar um esforço desproporcionado.

Os pedidos de apagamento ou eliminação dos dados baseiam-se muitas vezes na alegação de que o tratamento de dados não tem uma base legítima. Essas alegações surgem geralmente quando o consentimento foi revogado ou quando certos dados já não são necessários à prossecução da finalidade para que foram recolhidos. O ónus da prova de que o tratamento dos dados é legítimo recairá sobre o responsável pelo tratamento, uma vez que é ele o responsável pela legitimidade do tratamento. O princípio da responsabilidade exige que o responsável pelo tratamento esteja em condições de demonstrar, a todo o tempo, que as suas operações de tratamento de dados têm uma base legal legítima, caso contrário terá de interromper esse tratamento.[69]

Se o tratamento dos dados for contestado com fundamento na inexatidão dos dados ou na ilicitude do tratamento, a pessoa em causa pode exigir, nos termos do princípio do tratamento leal, que os dados em causa sejam bloqueados. Isto significa que os dados não serão eliminados, mas que o responsável pelo tratamento deverá abster-se

[69] Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, p. 118 – 119, 2014.

de os utilizar durante o período de bloqueio. Este bloqueio será particularmente necessário nos casos em que a continuação da utilização de dados inexatos ou detidos ilegitimamente seja suscetível de prejudicar a pessoa em causa. O legislador nacional deve regular, em maior pormenor, as condições da constituição e do cumprimento da obrigação de bloquear a utilização dos dados.[70]

As pessoas em causa têm ainda o direito de obter do responsável pelo tratamento a notificação a terceiros de qualquer bloqueio, retificação ou apagamento, caso estes tenham recebido dados antes destas operações de tratamento. Uma vez que o responsável pelo tratamento deve documentar a comunicação de dados a terceiros, deverá ser possível identificar os destinatários dos dados e pedir a eliminação deles. Porém, se os dados tiverem sido, entretanto publicados, por exemplo, na internet, poderá ser impossível obter totalmente o apagamento dos dados, uma vez que não será possível encontrar os destinatários deles. Nos termos da Diretiva 95/49 era obrigatório contactar os destinatários dos dados para os informar da retificação, apagamento ou bloqueio dos dados,[71] "salvo se isso for comprovadamente impossível ou implicar um esforço desproporcionado".[72]

Sendo assim, o direito ao apagamento se consolidou através das legislações europeias a todos os Estados-Membros, garantindo a todos que estão no território da UE que os dados pessoais em posse dos responsáveis pelo tratamento ao findar o prazo para o armazenamento do dado ou não ter mais a utilidade para qual foi solicitado o responsável pelo tratamento deve apagar esse dado.

1.1. Acórdão Google Espanha (C-131/12)

O acórdão Google tornou-se um marco e referência dentro da UE e para todo o mundo. A partir da decisão do TJUE iniciou-se a discussão sobre o tratamento de dados pelos motores de busca e consolidou-se o "direito ao esquecimento" (ou à desindexação), que é o direito ao apagamento aplicado aos mecanismos de busca, ou seja, o direito a desindexar informações nas pesquisas realizadas por essa via.

[70] Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, p. 119, 2014.
[71] Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, p. 119, 2014.
[72] Parlamento Europeu e o Conselho. Diretiva 95/46/CE, e 24 de outubro de 1995, artigo 12.º, c).

O processo que deu origem ao acórdão C-131/12, opunha o Google Spain SL, Google Inc. contra Agencia Española de Protección de Datos (AEPD), e Mario Costeja González, sendo datado de 13 de maio de 2014. No processo pode ser lido que o Sr. Mario Costela Gonzaléz impetrou uma ação na AEPD contra o Jornal La Vanguardia Ediciones SL e contra o Google Spain e o Google Inc., pelo facto de, ao pesquisar na plataforma Google, era remetido a um link do jornal nas datas de "19 de janeiro e 9 de março de 1998, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome de M. Costeja González".

No próprio processo podemos ler que:

> "Em 5 de março de 2010, M. Costeja González, de nacionalidade espanhola e domiciliado em Espanha, apresentou na AEPD uma reclamação contra a La Vanguardia Ediciones SL, que publica um jornal de grande tiragem, designadamente na Catalunha (Espanha) «La Vanguardia», e contra o Google Spain e o Google Inc. Esta reclamação baseava-se no facto de que, quando um utilizador inseria o nome de M. Costeja González no motor de pesquisa do grupo Google (a seguir «Google Search»), obtinha ligações a duas páginas do jornal da La Vanguardia de, respetivamente, 19 de janeiro e 9 de março de 1998, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome de M. Costeja González.
>
> Com esta reclamação, M. Costeja González pedia, por um lado, que se ordenasse à La Vanguardia que suprimisse ou alterasse as referidas páginas, para que os seus dados pessoais deixassem de aparecer, ou que utilizasse determinadas ferramentas disponibilizadas pelos motores de busca para proteger esses dados. Por outro lado, pedia que se ordenasse ao Google Spain ou ao Google Inc. que suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de

> pesquisa e de figurar nas ligações da La Vanguardia. Neste contexto, M. Costeja González alegava que o processo de arresto, de que fora objeto, tinha sido completamente resolvido há vários anos e que a referência ao mesmo carecia atualmente de pertinência".[73]

Em decisão de 30 de julho 2010, a AEPD declarou inocente o jornal por estar a cumprir ordem do Ministério do Trabalho e dos Assuntos Sociais, porém condenou o Google Spain e o Google Inc.

Segundo o processo em questão:

> "A AEPD considerou que os operadores de motores de pesquisa estão sujeitos à legislação em matéria de proteção de dados, uma vez que realizam um tratamento de dados pelo qual são responsáveis e atuam como intermediários da sociedade de informação. A AEPD considerou que estava habilitada a ordenar a retirada dos dados e a interdição de aceder a determinados dados, por parte dos operadores de motores de pesquisa, quando considere que a sua localização e a sua difusão são suscetíveis de lesar o direito fundamental de proteção dos dados e a dignidade das pessoas em sentido amplo, o que abrange também a simples vontade da pessoa interessada de que esses dados não sejam conhecidos por terceiros. A AEPD considerou que esta obrigação pode incumbir diretamente aos operadores de motores de pesquisa, sem que seja necessário suprimir os dados ou as informações do sítio de internet onde figuram, designadamente quando a manutenção dessas informações nesse sítio seja justificada por uma disposição legal."[74]

As empresas do universo Google interpuseram dois recursos separados e a Audiência Nacional decidiu apensar os processos. A questão apresentada a de perceber qual a responsabilidade dos provedores do referido serviço, em relação a proteção dos

[73] Tribunal de Justiça da União Europeia. Acórdão C-131/12 - Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, 2014.
[74] Idem

dados pessoais dos cidadãos que não desejam informações específicas compartilhadas na internet. A questão enquadra-se na Diretiva 95/46 e de como ela pode ser interpretada, já que os serviços em causa surgiram após a publicação da mesma. Deste modo, a Audiência Nacional decidiu suspender o processo e remeteu para o Tribunal de Justiça.

A principal discussão deste processo foi perceber se os mecanismos de pesquisa influenciam no resultado do termo pesquisado e o quão interferem na privacidade ou nos dados de cidadãos comuns. Outro problema seria a localização das sedes das empresas em causa, uma vez que não se encontram sediadas dentro da jurisdição europeia e sim nos EUA.

Deve ser destacada a posição do Advogado-Geral Niilo Jääskinen no processo. Nos parágrafos 27 a 29 ele coloca que:

> "27. Em 1995, o acesso generalizado à Internet era um fenómeno novo. Hoje, passadas quase duas décadas, a quantidade de conteúdos digitalizados disponíveis online aumentou astronomicamente. Estes podem ser facilmente acedidos, consultados e difundidos através de redes sociais, assim como descarregados para diversos dispositivos, tais como computadores tabulares (tablet computers), telefones inteligentes (smartphones) e computadores portáteis. Contudo, é claro que o legislador europeu não previu a evolução da Internet para uma base global e abrangente de informação que é universalmente acessível e pesquisável.
>
> 28. No cerne do presente pedido de decisão prejudicial está o facto de a Internet ampliar e facilitar de uma forma inédita a difusão da informação (19). De modo semelhante, como a invenção da imprensa no século XV permitiu a reprodução de um número ilimitado de cópias que anteriormente tinham de ser escritas à mão, o carregamento de material para a Internet permite o acesso em massa à informação que anteriormente só podia ser eventualmente encontrada depois de pesquisas árduas, e num número limitado de locais. O acesso universal à informação na

> Internet é possível em todo o lado, com exceção dos países em que as autoridades limitaram, por diversos meios técnicos (tais como barreiras de proteção eletrónicas [electronic firewalls]) o acesso à Internet ou em que o acesso às telecomunicações é controlado ou escasso.
>
> 29. Devido a estes desenvolvimentos, o potencial âmbito de aplicação da diretiva no mundo moderno tornou-se surpreendentemente vasto. Pensemos no caso de um professor de direito da UE que descarregou, do sítio web do Tribunal de Justiça, a jurisprudência essencial do Tribunal de Justiça para o seu computador portátil. À luz da diretiva, o professor pode ser considerado um «responsável pelo tratamento» de dados pessoais provenientes de um terceiro. O professor tem ficheiros que contêm dados pessoais que são tratados automaticamente para pesquisa e consulta no contexto de atividades que não são exclusivamente pessoais ou domésticas. De facto, qualquer pessoa que hoje leia um jornal num tablet ou que siga uma rede social num smartphone parece dedicar-se ao tratamento de dados pessoais com meios automatizados e está potencialmente abrangida pelo âmbito de aplicação da diretiva, desde que não o faça exclusivamente a título privado. Além disso, a interpretação ampla dada pelo Tribunal de Justiça ao direito fundamental à vida privada, num contexto de proteção dos dados, parece expor qualquer comunicação humana por meios eletrónicos a uma fiscalização à luz deste direito.[75]

O Advogado-Geral discutiu em suas conclusões a aplicação territorial da Diretiva 95/46, concluindo que o TJUE deveria abordar a questão da aplicabilidade territorial na perspetiva do modelo de negócios dos prestadores de serviços de motores de pesquisa na internet. Conforme refere, este modelo baseia-se normalmente na publicidade na internet a partir de palavras-chave, que é a fonte de receitas e, enquanto tal, a razão de ser económica da disponibilização de uma ferramenta de localização de informação

[75] Tribunal de Justiça da União Europeia. Acórdão C-131/12 - Conclusões do Advogado-Geral Niilo Jääskinen, 25 de junho de 2013.

gratuita sob a forma de um motor de pesquisa. A entidade que se ocupa da publicidade na internet a partir de palavras-chave (denominado "prestador do serviço de referenciamento"), na jurisprudência do Tribunal de Justiça, está associada a um motor de pesquisa na internet. O Tribunal responderia ao primeiro grupo de questões prejudiciais no sentido de que o tratamento de dados pessoais é efetuado no contexto das atividades de um "estabelecimento" do responsável pelo tratamento, na aceção do artigo 4.°, n.° 1, alínea a), da diretiva, quando a empresa que explora o motor de pesquisa na internet abre, num Estado-Membro, com vista à promoção e venda dos espaços publicitários desse motor de pesquisa, uma sucursal ou uma filial cuja atividade se dirige aos habitantes desse Estado.[76]

Porém em sua conclusão, o Advogado-Geral Jääskinen afirmou que o direito à eliminação e ao bloqueio dos dados, regulados no artigo 12.°, alínea b), e o direito de oposição, previsto no artigo 14.°, alínea a), da Diretiva 95/46 não conferem à pessoa em causa o direito de se dirigir diretamente aos motores de pesquisa para impedir a indexação de informações referente à sua pessoa, legalmente publicada em páginas de internet de terceiros, alegando não desejar que tais informações sejam conhecidas pelos utilizadores da internet por considerar que as mesmas lhe podem ser prejudiciais ou pretender ser esquecida.[77]

O Advogado-Geral, embora a diretiva seja aplicável, afirmou que um motor de pesquisa não pode ser considerado um responsável pelo tratamento de dados, exceto em situações limitadas. Ele concluiu ainda que, mesmo se um motor de pesquisa fosse considerado um responsável pelo tratamento, um titular de dados não poderia impedir um motor de pesquisa de indexar informações pessoais legalmente publicadas em páginas de internet de terceiros, invocando que poderia ser prejudicial para ela ou que ela deseja que seja esquecida. Quanto às questões centrais, quais sejam, a caracterização do mecanismo de busca como um responsável pelo tratamento e o âmbito dos direitos do detentor do direito de apagar e objetar, o julgamento do TJUE subestimou substancialmente as respostas propostas pelo Advogado-Geral.[78]

[76] Idem
[77] Idem
[78] Peguera, Miquel. Página 528.

O Tribunal de Justiça então respondeu ao reenvio prejudicial da Audiência Nacional da Espanha, contrariando as recomendações do Advogado-Geral:

> "(...) importa examinar em primeiro lugar, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 2.°, alínea b), da Diretiva 95/46 deve ser interpretado no sentido de que a atividade de um motor de pesquisa, como fornecedor de conteúdos, que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência, deve ser qualificada de «tratamento de dados pessoais», na aceção daquela disposição, quando essas informações contenham dados pessoais. Em caso de resposta afirmativa, o órgão jurisdicional de reenvio pretende saber ainda se esse artigo 2. °, alínea d), deve ser interpretado no sentido de que o operador de um motor de pesquisa deve ser considerado «responsável» pelo referido tratamento de dados pessoais, na aceção dessa disposição.
>
> Segundo o Google Spain e o Google Inc., a atividade dos motores de pesquisa não pode ser considerada um tratamento dos dados que aparecem nas páginas de Internet de terceiros exibidas na lista de resultados da pesquisa, dado que esses motores tratam as informações acessíveis na Internet, no seu conjunto, sem fazer a seleção entre os dados pessoais e as outras informações. Além disso, mesmo admitindo que esta atividade deva ser qualificada de «tratamento de dados», o operador de um motor de pesquisa não pode ser considerado «responsável» por esse tratamento, uma vez que não conhece os referidos dados nem exerce controlo sobre os mesmos.
>
> Em contrapartida, M. Costeja González, os Governos espanhol, italiano, austríaco e polaco e a Comissão Europeia entendem que a referida atividade implica claramente um «tratamento de dados» na aceção da Diretiva 95/46, que é distinto

> do tratamento de dados efetuado pelos editores de páginas de internet e prossegue objetivos diferentes deste. O operador de um motor de pesquisa é «responsável» pelo tratamento de dados efetuado por esse motor, uma vez que é ele que determina a finalidade e os meios desse tratamento."[79]

A resposta do TJUE foi suficientemente clara quanto: i) à existência de um tratamento de dados pessoais por parte do operador do motor de pesquisa; ii) à responsabilidade do operador do motor de pesquisa; iii) ao elemento de conexão entre o tratamento de dados e o responsável pelo tratamento, quando este não possua a sua sede no espaço da UE; iv) à obrigação do operador do motor de pesquisa proceder à desindexação de resultados aquando do pedido do titular dos dados; e v) à extensão, alcance e limites dos direitos do titular dos dados.[80]

O TJUE reconheceu que cada pessoa tem o direito a que informações sobre si disponíveis na internet deixem de ser associadas ao seu nome, por meio de uma lista de resultados exibida na sequência de uma pesquisa efetuada em motores de busca, sem que, todavia, a constatação desse direito pressuponha que tal associação cause prejuízo à pessoa em causa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7.° (proteção da vida privada) e 8.° (proteção de dados pessoais) da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão numa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de pesquisa, mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa.[81]

Não será o caso se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais foi justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão.[82]

---

[79] Tribunal de Justiça da União Europeia. Acórdão C-131/12 - Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, 2014.
[80] Silveira, Alessandra; Marques, João. Do Direito a Estar Só ao Direito ao Esquecimento. Considerações Sobre a Proteção de Dados Pessoais Informatizados no Direito da União Europeia: Sentido, Evolução e Reforma Legislativa. Revista da Faculdade de Direito - UFPR, Vol. 61(n.º 3), pág. 102, 2016.
[81] Silveira, Alessandra; Marques, João. Página 102.
[82] Silveira, Alessandra; Marques, João. Página 102.

O Tribunal decidiu que a atividade de um mecanismo de pesquisa equivale a um processamento dos dados pessoais contidos nas páginas da internet que indexa e disponibiliza ao público por meio dos resultados da pesquisa. No entanto, considerou, contrariamente às conclusões do Advogado-Geral, que o motor de pesquisa determina os fins e os meios desse processamento e, portanto, deve ser considerado como um responsável pelo tratamento.[83]

De acordo com o TJUE, esse processamento "pode ser distinguido e é adicional àquele realizado por editores de sites, consistindo no carregamento desses dados em uma página da internet". Esse processamento pode afetar significativamente os direitos dos titulares de dados, porque os usuários que realizam pesquisas com base no nome de um indivíduo podem obter uma visão geral estruturada das informações relacionadas a essa pessoa disponíveis na internet. Esses usuários podem, assim, "estabelecer um perfil mais ou menos detalhado do assunto dos dados".[84] Como responsável pelo tratamento, observou o TJUE, um mecanismo de pesquisa "deve garantir, no âmbito de suas responsabilidades, poderes e capacidades, que a atividade atenda aos requisitos da Diretiva.".[85]

Embora exista legitimidade dos argumentos expedidos pelo Advogado-Geral e pela própria Comissão Europeia, o Tribunal de Justiça consagrou, sem nomear, o que foi reconhecido como o “direito ao esquecimento digital”, referindo que os direitos daqueles que utilizam a internet “prevalecem, em princípio, não apenas sobre os interesses económicos do operador do motor de pesquisa, mas também sobre o interesse deste público para encontrar tais informações sobre o nome dessa pessoa”.[86] Portanto, o Tribunal reconheceu um direito subjetivo para a pessoa interessada, caracterizando como “o direito que a informação em questão, relativa à sua pessoa, não seja mais, na fase atual, ligada ao seu nome com uma lista de resultados exibida após uma pesquisa efetuada com seu nome (...)”.[87]

O Google Espanha, no entanto, não abordou a questão de remover informações da internet em geral, mas concentrou-se em aspetos muito mais restritos. Considerou

[83] Peguera, Miquel. Página 528.
[84] Tribunal de Justiça da União Europeia. Acórdão C-131/12 - Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, 2014.
[85] Peguera, Miquel. Página 528 - 529.
[86] Tribunal de Justiça da União Europeia. Acórdão C-131/12 - Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, 2014.
[87] Idem

especificamente o problema que surge quando uma informação, que teria passado despercebida, enterrada nos arquivos de um jornal ou boletim oficial, é trazida à atenção do público por meio dos mecanismos de pesquisa da internet. Também abordou o facto de que as consultas baseadas em uma pessoa podem produzir um perfil mais ou menos detalhado do indivíduo.[88]

Em vez de discutir se o indivíduo pode solicitar a remoção de todas as informações do índice do mecanismo de pesquisa, o TJUE limitou-se a reconhecer o direito de solicitar a remoção do link da lista de resultados de pesquisa quando uma pesquisa é realizada com base no nome dessa pessoa. Como consequência, as informações ainda poderiam ser encontradas em pesquisas usando termos que não o nome da pessoa. Nesse sentido, como defendem Brendan Van Alsenoy e Marieke Koekkoek, o direito previsto pelo TJUE pode ser mais bem descrito como um "direito de ser excluído".[89]

No rescaldo da saga do Google Espanha, o Google criou um painel de especialistas com função consultiva para ajudá-lo a lidar com a implementação do julgamento. Apesar dos pedidos por mais transparência sobre os critérios de exclusão, uma das primeiras análises académicas da abordagem do Google para o encerramento de pedidos de desindexação para do detentor do dado a empresa revela que o mecanismo de pesquisa tem conseguido cumprir suas novas obrigações à luz do direito do RGPD.[90]

O TJUE decidiu que os interesses dos internautas na obtenção da informação devem ser considerados. O que não significa que os seus interesses prevaleçam, mas apenas que dever ser especialmente tidos em conta, ou seja, o Tribunal não deixa de reconhecer que o direito à desindexação não é, como não o é nenhum direito, absoluto, impondo-se a sua conciliação com outros direitos reconhecidos na ordem jurídica europeia.[91]

Por fim, a amplitude deste direito à desindexação reconhecido no acórdão Google foi bem evidenciada pelo facto de que a supressão da lista de resultados e a ligação a outras páginas da web, ou seja, a supressão do resultado, ou a desindexação é devida a uma publicação online pode ser legítima ou até mesmo legalmente obrigatória, já que a

[88] Peguera, Miquel. Página 511.
[89] Van Alsenoy, Brendan; Koekkoek, Marieke. Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'. International Data Privacy Law, Volume 5(Issue 2), 105–120, 2015.
[90] Idem
[91] Castro, Caratina Sarmento e. Página 1062.

publicitação em uma página web tem direitos e efeitos diferentes do que a hiperligação ou a indexação revelada em um motor de busca. O TJUE, então, considerou que a informação que se pretende "fazer esquecer" não tem de ser necessariamente prejudicial à pessoa em causa.[92]

1.2. Dados "Transparency Report" da Google

Após o julgamento do acórdão Google foi aberta a página de internet <https://support.google.com/legal/contact/lr_eudpa?product=websearch> para que qualquer cidadão comum possa requisitar a retirada do seu nome em pesquisas. Segundo o próprio Google na referida página de internet, para fazer o requerimento:

> "Quando efetuar um pedido desta natureza, iremos equilibrar os direitos de privacidade do indivíduo com os de interesse público e os direitos à distribuição da informação. Ao avaliar o seu pedido, verificaremos se os resultados incluem informação desatualizada acerca de si, bem como se existe interesse público na informação. Por exemplo, poderemos recusar remover uma determinada informação acerca de esquemas financeiros, negligência, condenações criminais, ou conduta pública de funcionários públicos.
>
> Precisará de uma cópia digital de um documento de identificação para preencher este formulário. Se estiver a enviar este pedido em nome de outra pessoa, tem de fornecer a respetiva identificação. Para enviar o pedido, é obrigatório preencher os campos assinalados com um asterisco." [93]

Segundo o Google, a sua própria equipa (Google Inc.) realiza as determinações relevantes, possuindo uma equipa de avaliadores treinados especialmente para esse propósito, com sede principal em Dublin, Irlanda. A equipa usa caminhos de escalonamento dedicados para que a equipa sénior e os advogados do Google decidam os

[92] Idem
[93] Google. Transparency Report - Solicitações de remoções da pesquisa em conformidade com a privacidade europeia. Disponível em <https://www.google.com/transparencyreport/removals/europeprivacy/>.

casos mais complexos. A partir de 1 de novembro de 2015, segundo dados internos, um pouco mais de 30% das solicitações foram elegíveis para uma segunda opinião.[94]

Segundo os mesmos dados, caso algum requerente discorde da decisão da empresa, se não for removido um URL dos resultados da pesquisa no site Google, o indivíduo poderá solicitar a uma autoridade local de proteção de dados que avalie a decisão da empresa.[95]

Para o Google existe quatro fatores que são importantes para a retirada da página do mecanismo de pesquisa, que são:

> **Ausência clara de interesse público:** por exemplo, sites agregadores com páginas que incluem informações de endereço ou de contato pessoal, ocorrências em que o nome do requisitante não aparece mais na página e páginas que não estão mais online.
>
> **Informações confidenciais:** páginas com conteúdo relacionado exclusivamente à saúde, orientação sexual, raça, etnia, religião, afiliação política ou ao status sindical de uma pessoa.
>
> **Conteúdo relacionado a menores:** conteúdo relacionado a menores ou a pequenas infrações ocorridas quando o requisitante era menor de idade.
>
> **Condenações executadas/exonerações/absolvições por crimes:** de acordo com a legislação local que rege a reabilitação de infratores, a tendência da Gooogle, segundo afirma, é ser favorável à remoção de conteúdo relacionado a uma condenação que tenha sido executada, à remoção de acusações consideradas falsas por um tribunal, bem como conteúdo relacionado a uma acusação criminal em que o requisitante foi absolvido, sendo consideradas a época do conteúdo e a natureza do crime. [96]

[94] Google. Transparency Report - Perguntas Frequentes sobre as solicitações de remoção da pesquisa em conformidade com a privacidade europeia. Disponível em <https://support.google.com/transparencyreport/answer/7347822?hl=pt-BR>.
[95] Idem
[96] Idem

A empresa ainda coloca os fatores que não a fazem retirar o que foi pedido do mecanismo de pesquisa, que são:

> **Soluções alternativas:** há outra maneira para que o requisitante remova a página dos resultados da pesquisa. Por exemplo, um requisitante pode ter publicado o conteúdo em um site que dá permissão para os usuários impedirem a exibição do conteúdo nos resultados da pesquisa. Quando possível, o Google afirma que informa aos requisitantes sobre essas ferramentas.
>
> **Motivos técnicos:** um URL incompleto ou corrompido é um erro técnico comum. Os requisitantes às vezes solicitam a remoção de páginas por consultas que não correspondem aos nomes deles ou ao nome da pessoa que o requisitante declara representar.
>
> **URL duplicado pelo mesmo indivíduo:** um requisitante envia diversas solicitações para remover a mesma página com o mesmo nome.
>
> **Forte interesse público:** o Google pode recusar a remoção se determinar que a página tem informações de forte interesse público. Determinar se o conteúdo é ou não do interesse público é algo complexo e pode levar vários fatores em consideração, incluindo, mas não limitado a, se o conteúdo é relacionado à vida profissional do requisitante, a um crime cometido no passado, um cargo político, um cargo público ou se o conteúdo é de autoria do próprio requisitante, bem como documentos governamentais ou de natureza jornalística. [97]

O Google, como exemplo, colocou na página de internet da transparência dois casos para qual foi solicitado desindexar resultados, com a seguinte ressalva “Ao avaliar cada solicitação, o Google precisa considerar os direitos dos indivíduos e o interesse

[97] Idem

público no conteúdo. Removemos todas as informações que podem identificar indivíduos afetados pelo conteúdo destes exemplos, a fim de proteger suas identidades.”.[98]

O primeiro caso descreve que “Recebemos uma ordem judicial da Autoridade de proteção de dados de Portugal para remover um artigo de notícias sobre a investigação criminal de um empresário conhecido por suposta fraude, falsificação de documentos e evasão fiscal”, tendo como desfecho final a remoção da página de internet.[99]

No segundo caso o Google revela que “Recebemos uma solicitação de um professor universitário para remover duas entradas de um blog que criticavam a decisão dele de implementar uma polêmica política de *campus*”, como desfecho foi indeferida a remoção da página de internet, porque o conteúdo estava relacionado à função pública do docente como professor universitário.[100]

Porém, depois que o Google recebeu um requerimento da Autoridade de proteção de dados de Portugal, fez declaração oficial dizendo que “removemos um URL do nosso serviço de pesquisas no país, com base na lei de difamação portuguesa, em vez de na lei de proteção de dados”, e complementam que a Autoridade de proteção de dados “ordenou judicialmente remoção do restante da entrada do blog”.[101]

Ou seja, o que se extrai das estatísticas e dos dois exemplos do próprio Google é que mesmo que o Regulamento (UE) 2016/679 traga em seu artigo 17.º: “O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais”, o Google não elimina todos os dados e muito menos sem demora, como frisa o texto da legislação europeia, além de possuir parâmetros próprios, e não os da lei, para desindexar as páginas que foram solicitadas.

[98] Google. Transparency Report - Remoções da pesquisa em cumprimento da legislação europeia sobre privacidade. Disponível em <https://transparencyreport.google.com/eu-privacy/overview>.
[99] Idem
[100] Idem
[101] Idem

1.3. Comissão Nacional de Proteção de Dados – Deliberação n.º 536/2016

Em Portugal a Comissão Nacional de Proteção de Dados (CNPD) é o órgão responsável por verificar a correta aplicação do Regulamento (UE) 2016/679, e anteriormente da Diretiva 95/46.

A Deliberação 536/2016 foi a decisão da Comissão no Processo n.º 13585/2014, na qual assegurou o direito da eliminação de dados, garantindo assim o direito dos titulares dos dados em face dos motores de pesquisa. Essa deliberação foi baseada na Diretiva 95/46 que estava em vigência a época.

Cabe ressaltar que o presente trabalho traz esta deliberação para demonstrar a aplicação da Diretiva 95/46, à época, e como o direito à desindexação está a ser reconhecido em Portugal. As deliberações e processos da CNPD correm em segredo de justiça e este foi o único processo que disponibilizaram através de solicitação feita por correio eletrónico.

No presente caso, em direito de resposta, o Google afirmou que o Google Portugal é um "estabelecimento" do Google Inc., com o único propósito de determinar a lei aplicável ao serviço do motor de pesquisa, e não o de considerar o Google Portugal como responsável pelo tratamento de dados. Além disso, afirma que o requerente é uma figura pública que exercia cargo público a época, e que os factos que estão presentes no processo eram de interesse público, o que caracterizaria a exceção à regra do direito de pedir a remoção do conteúdo.

Na sua decisão a CNPD ressalta o artigo 2.º, alíneas "b" e "d", da Diretiva 95/46, relativa a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Além disso ressalta o artigo 4.º, n.º 1, alínea "a", da mesma diretiva, onde prevê que o tratamento de dados no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro.

A CNPD afirma a liquidez na certeza de que o Google Inc., através do Google Portugal, se constitui como a responsável por esse tratamento, uma vez que a primeira criou em Portugal a segunda destinada a assegurar a promoção e a venda de espaços publicitários propostos por esse motor de pesquisa.

Além disso demonstra que a diretiva, em sua alínea "c" do n.º 1 do artigo 6.º consolida a necessidade de uma ponderação apurada e prévia ao tratamento de dados pessoais de diversos critérios, quanto à necessidade de acautelar eventuais e ponderosas razões de interesse público e de comprovado interesse mediático com motivos relevantes. Para a CNPD as figuras públicas, se bem que mais expostas à mediatização, não veem negado o seu direito fundamental ao bom nome e reputação e à reserva da intimidade da vida privada.

A CNPD informa que a notícia objeto do processo, presente nos resultados do motor de pesquisa do Google, são de acontecimentos com mais de oito anos de antiguidade na época da decisão. Afirma ainda que uma tal notícia, com o decorrido lapso temporal, e sem conhecida atualização, merece a maior das dúvidas e dificilmente pode sobrevir ao vitalício direito à privacidade.

Foi decidido então que não está acautelado o critério da proporcionalidade, a que se aludiu, sendo inadmissível a manutenção da associação do resultado obtido no motor de pesquisa pela procura do nome da participante, e o Google teve de proceder à desindexação dos resultados do URL citado do seu motor de pesquisa, qualquer que seja a versão que se possa aceder em território nacional.

A CNPD afirma que, como pode ser observado, as decisões do TJUE tiveram inspiração no caso Google Spain de 2014, processo C-131/12, no qual pela primeira vez foi consagrado o direito ao esquecimento sob a ótica da desindexação dos motores de pesquisa. Os processos seguintes concretizaram o direito ao esquecimento e a proteção de todos os cidadãos e residentes no espaço dos Estados-Membros.

O processo do Google Spain serviu como referência para os Estados-Membros, como Portugal, nomeadamente para a Deliberação n.º 536/2016 do CNPD, que concretizou o direito estabelecido no julgamento de 2014, assegurando a exclusão de uma URL que atingia diretamente a vida privada, mesmo sendo de uma figura pública, e obrigou o Google a desindexar a URL do nome do requerente. Podemos assim observar um avanço na resposta às novas tecnologias, tendente a assegurar de forma concreta o direito à desindexação, exercido por qualquer cidadão, seja ele figura pública ou não.

1.4. O Regulamento Geral de Proteção de Dados (Regulamento 2016/679)

A União Europeia adotou o novo Regulamento Geral de Proteção de Dados (RGPD) que inclui o direito ao apagamento («direito a ser esquecido»), reconhecendo o direito à desindexação com etapas específicas para os responsáveis pelo tratamento de dados apagarem informações mediante solicitação.

Além disso, de acordo com o artigo 18.º do RGPD, conhecido como "Direito à limitação do tratamento", o titular dos dados tem o "direito de obter do responsável pelo tratamento a limitação do tratamento" de dados pessoais. Quando o processamento é restrito, os responsáveis pelo tratamento de dados têm permissão para armazenar os dados pessoais, mas não para processá-los ainda mais. O responsável pelo tratamento deve tornar os dados inacessíveis, em vez de excluí-los completamente, como no caso do direito ao esquecimento. Nesse caso, o titular dos dados tem o direito de ser eliminado em várias circunstâncias específicas, inclusive quando "os dados pessoais não forem mais necessários em relação aos objetivos para os quais foram coletados ou processados de outra forma". Em contrapartida, o "Direito à limitação do tratamento" aplica-se mais estritamente, *inter alia*, aos casos em que "a exatidão dos dados é testada pela pessoa em causa".

A restrição do processamento deve ocorrer imediatamente mediante solicitação do sujeito de dados e por último "por um período que permita ao responsável pelo tratamento verificar a exatidão dos dados". Estas normas substituem, e melhor qualificam, as disposições relativas ao apagamento e bloqueio de dados na Diretiva relativa à proteção de dados, Diretiva 95/46/CE.[102]

Posso ver os meus dados? Podem parar de processar os meus dados? Podem apagar os dados que armazenei? Estas são todas as solicitações que um titular de dados pode fazer no âmbito do RGPD. O RGPD concede direitos aos titulares de dados para acesso, restrição de processamento e remoção de certos tipos de dados pessoais mantidos pelos responsáveis pelo tratamento de dados.[103]

[102] Frosio, Giancarlo F.. The Right to be Forgotten: Much ado about nothing. Colorado Techlogy Law Journal, 309 - 310, 2017.
[103] Lode, Sarah L.. "You Have the Data" . . . The Writ of Habeas Data and other Data Protection Rights: Is the United States Falling Behind? Indiana Law Journal & Supplement, Volume 94, p. 51, 2018.

O RGPD traz no início de suas considerações o ponto pelo qual o direito a ser esquecido está presente. No ponto 65 coloca que "Os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o "direito a serem esquecidos" quando a conservação desses dados violar o presente regulamento ou o direito da UE ou dos Estados-Membros aplicável ao responsável pelo tratamento.".[104]

Esse ponto ressalva principalmente que "Este direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na internet".[105]

O ponto 65 também traz a possibilidade no caso de existir o interesse público no dado, afirmando que:

> "(…) o prolongamento da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial."[106]

E conclui dizendo que o responsável pelo tratamento deverá adotar as medidas que se demonstrem razoáveis, utilizando toda a tecnologia disponível e os meios que a mesma coloca ao dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar os dados.[107]

O direito ao apagamento, que também é listado como o direito a ser esquecido, é o direito de um titular de dados solicitar que sua informação seja removida ou apagada

[104] Parlamento Europeu e o Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016.
[105] Idem
[106] Idem
[107] Idem

quando certas circunstâncias estiverem presentes. O direito ao apagamento está disponível, de acordo com o RGPD, quando (1) os dados não são mais necessários para as finalidades que foram coletadas, (2) a pessoa em questão retirou o devido consentimento (e não há outros fundamentos legais para processamento) (3) a pessoa em causa se oponha adequadamente ao processamento de dados, (4) os dados sejam processados ilegalmente, (5) os dados devem ser apagados para cumprimento de uma obrigação legal ou (6) os dados foram coletados em relação ao oferta de serviços da sociedade da informação.[108] Se uma dessas condições for atendida, o responsável pelo tratamento de dados precisará excluir prontamente os dados e, se os dados tiverem sido tornados públicos pelo responsável pelo tratamento, deverá também tomar as medidas necessárias para informar outros responsáveis pelo tratamento que estão processando os dados sujeitos a apagamento e tais responsáveis devem apagar quaisquer links, cópias ou replicações desses dados.[109]

Existe uma distinção importante entre diretivas e regulamentos da UE, e essa distinção está entre as razões pelas quais a Comissão Europeia se esforçou para substituir a Diretiva de Proteção de Dados por um regulamento. As diretivas são atos legislativos amplos, orientados por objetivos, que fornecem orientações para a implementação do Estado-Membro, mas dependem da aprovação independente de uma lei em todos os Estados-Membros dentro de um período designado. Os regulamentos são peças legislativas específicas e estreitas que se tornam diretamente aplicáveis – e obrigatórias – em todos os Estados-Membros sem necessidade de transposição através de uma lei em cada Estado. Quando a Comissão Europeia considerou pela primeira vez a reforma da proteção de dados, ainda não era claro que uma diretiva seria substituída por um regulamento. A Comissão comprometeu-se a abordar as seguintes questões:

(1) Abordar o impacto das novas tecnologias; (2) Reforçar a dimensão do mercado interno da proteção de dados; (3) Abordar a globalização e melhorar as transferências internacionais de dados; (4) Proporcionar um quadro institucional mais forte para o

[108] Conforme descrito no artigo 17.º do RGPD com o título "Direito ao apagamento dos dados («direito a ser esquecido»)", o seu primeiro número já destaca que a eliminação dos dados é de responsabilidade daquele que faz o tratamento do mesmo e que a eliminação desses dados deve ser feito de imediato, sem demora justificativa, para os fins colocados nas alíneas do primeiro ponto, de "a" a "f".
[109] Lode, Sarah L.. Página 52.

cumprimento efetivo das regras de proteção de dados; (5) Melhorar a coerência do quadro jurídico de proteção de dados.[110]

O primeiro desafio, abordando o impacto das novas tecnologias, concentra-se na dificuldade em garantir o consentimento livre e informado e na proteção de dados confidenciais, garantindo a transparência para os indivíduos na internet. O segundo desafio no reforço da dimensão do mercado interno em matéria de proteção de dados tem em conta os meios limitados de que dispõem os nacionais para apresentar queixas perante os seus tribunais, garantir a segurança jurídica e reduzir os encargos administrativos do sistema de notificação. Respondendo ao terceiro desafio, melhorar as transferências internacionais de dados, a Comissão apenas previu a aprovação de uma nova lei na União Europeia e isso não teria sido suficiente. O quarto e quinto desafios referem-se à questão supra, na medida em que a diretiva é incapaz de resolver as incoerências entre os Estados-Membros, porque atualmente cada Estado impõe diferentes regimes regulamentares e proporciona mais proteções do que outros em algumas áreas, bem como menos em outros.[111]

Embora as limitações do direito ao esquecimento sejam semelhantes às estabelecidas no caso do Google Spain, sua proteção foi reforçada pelo facto de que, se um responsável pelo tratamento é obrigado a apagar dados pessoais que tornou público, deve tomar medidas razoáveis para informar outros responsáveis pelo tratamento que também publicaram os dados pessoais para apagar qualquer link ou cópias. Esta disposição tem como alvo um problema que o Google Spain deixou por resolver. Embora a reivindicação do direito ao esquecimento de Mario Costeja Gonzáles tenha sido bem-sucedida contra o Google, não ficou claro se outros mecanismos de pesquisa atenderiam à decisão, já que o mesmo link pode ter aparecido no Yahoo ou no Bing, entre outros. Sob a provisão do RGPD, provavelmente haverá uma proteção mais ampla para os indivíduos, porque outros responsáveis pelo controle serão notificados de que o indivíduo tem uma reivindicação válida a ser esquecida. Os responsáveis pelo tratamento podem então remover o link como uma estratégia preventiva para evitar serem processados, o que garantirá uma aplicação mais uniforme do RGPD. Portanto, o regulamento orienta os mecanismos de pesquisa a equilibrar devidamente o direito à privacidade e o direito à

[110] Safari, Beata A.. Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. Seton Hall Law Review, Volume 47, 820 – 821, 2017
[111] Safari, Beata A.. 821 – 822.

informação, e mais orientações para os responsáveis pelo tratamento de dados resultarão em maior uniformidade de decisão nas solicitações do direito ao esquecimento.[112]

O direito a ser esquecido, mesmo não tendo sido incluído na Diretiva de Proteção de Dados, estava implícito no documento do artigo 12.º. Embora o RGPD (aparentemente) confunda os dois termos do artigo 17.º, intitulado «Direito ao apagamento dos dados ("direito a ser esquecido")», há debates sobre se o direito de ser esquecido e o direito de apagar representam a mesma ideia. Segundo alguns doutrinadores, o direito de apagar e o direito de ser esquecido são termos intercambiáveis.[113] Outros doutrinadores argumentam que os dois não representam a mesma ideia, pois o direito a ser esquecido inclui dados "que não violam qualquer norma"[114]. O apagamento permite que os titulares de dados solicitem a eliminação dos seus dados pessoais quando a sua retenção ou processamento viola os termos do regulamento, em particular (mas não exclusivamente) por estarem incompletos ou imprecisos.[115] Por outro lado, o direito de ser esquecido causaria a exclusão de informações pessoais, independentemente de as informações serem prejudiciais ou terem sido processadas ilegalmente.[116]

Além de oferecer mais proteção aos usuários da internet, o RGPD também impõe obrigações mais rigorosas aos intermediários de dados. A Diretiva 95/46 identificou duas categorias de intermediários: responsáveis pelo tratamento e os subcontratantes. Esses responsáveis são entidades que "determinam o propósito e os meios do processamento de dados pessoais", enquanto os subcontratantes são entidades que processam (ou seja, coletam, registram, organizam ou usam) os dados pessoais em nome do responsável pelo tratamento.[117]

No entanto, apenas os responsáveis pelo tratamento de dados estavam sujeitos a obrigações.[118] Esse especto foi fortemente criticado porque o advento dos mecanismos de

[112] Alessi, Stefania. Eternal Sunshine: The Right to be Forgotten in the European Union after the 2016 General Data Protection Regulation. Emory International Law Review, Volume 32, 165-166, 2017.
[113] Mitchell-Rekrut, Cooper. Search Engine Liability under the Libe Data Regulation Proposal: Interpreting Third Party Responsibilities as Informed by Google Spain. Georgetown Journal of International Law, Volume 45, Pág. 861, 2014.
[114] Cofone, Ignacio. Google v. Spain: A Right to Be Forgotten? Chicago-Kent Journal of International and Comparative Law, Volume 15(No. 1), Pág. 8, 2015.
[115] Cofone, Ignacio. Página 6.
[116] Safari, Beata A.. Página 832.
[117] Safari, Beata A.. Página 811.
[118] Burri, Mira; Schär, Rahel. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. Journal of Information Policy, Volume 6, p. 494, 2014.

pesquisa e redes sociais avançou o processamento rapidamente, dificultando a distinção entre responsáveis pelo tratamento e subcontratantes. Consequentemente, os intermediários de dados poderiam facilmente evitar as disposições de proteção de dados.[119]

O RGPD mantém essas duas categorias, mas impõe obrigações a ambas. Sob a nova disciplina, os subcontratantes têm uma obrigação independente de garantir a segurança dos dados pessoais. Por exemplo, os subcontratantes devem garantir a conformidade com o RGPD a ser nomeado pelos responsáveis pelo tratamento. Assim, os subcontratantes devem relatar todas as informações necessárias para demonstrar conformidade com o regulamento e permitir auditorias conduzidas pelo responsável pelo tratamento. Ao processar dados pessoais, os subcontratantes devem seguir as instruções escritas dos responsáveis e impor obrigações de confidencialidade em todos os funcionários que processam os dados.[120]

O direito de ser esquecido permite que um indivíduo controle seus dados pessoais se não for mais necessário para seu propósito original, ou se, por algum outro motivo, desejar retirar o consentimento quanto ao seu processamento, entre outras razões.[121]

Para Dawn Carla Nunziato embora a linguagem do regulamento nominalmente forneça ao responsável pelo tratamento de dados uma "liberdade de expressão" para o pedido de eliminação da pessoa em causa, outros aspetos do regulamento que incluem as multas exorbitantes por incumprimento e a "necessidade" da limitação da liberdade de defesa de expressão, provavelmente distorcerá o equilíbrio em favor dos direitos de remoção do titular dos dados e contra o direito do responsável pelo tratamento de dados à liberdade de expressão. Outras questões processuais que envolvem o processo de revisão e de remoção previsto no regulamento também irão inclinar a balança a favor do apagamento e contra a liberdade de expressão.[122]

Para Daphne Keller, os termos do regulamento, incluindo a exigência de que o responsável pelo tratamento de dados elimine os dados pessoais imediatamente, enquanto avalia o mérito da alegação do titular dos dados, e o ônus da prova colocada no

[119] Cuijpers, Colette; Purtova, Nadezhda; Kosta, Eleni. Data Protection Reform and the Internet: The Draft Data Protection Regulation. Tilburg Law School Research Paper No. 03/2014, pag. 6, 2014.
[120] Alessi, Stefania. Página 165.
[121] Safari, Beata A.. Página 835 .
[122] Nunziato, Dawn Carla. The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten. University of Pennsylvania Journal of International Law, Volume 39, p. 1055, 2018.

responsável pelo tratamento de dados, juntamente com as exorbitantes penalidades financeiras por incumprimento, criará um desequilíbrio sem precedentes no ecossistema da internet em favor dos pedidos de eliminação, vindo dos titulares de dados, e contra o direito de acesso e o direito de publicar informações na internet.[123]

Nunziato acrescenta dizendo que um mecanismo de pesquisa ou outro responsável pelo tratamento de dados é necessário para restringir o processamento de dados enquanto se aguarda a verificação de que os fundamentos legítimos do responsável pelo tratamento de dados prevalecem sobre os do titular dos dados.[124]

As obrigações dos responsáveis pelo tratamento de dados sob o RGPD são mais rigorosas do que sob o Diretiva 95/46. Por exemplo, os responsáveis pelo tratamento devem fornecer proteção de dados "por design ou padrão", o que significa que eles devem garantir a máxima proteção da privacidade como uma linha de base. Para fazer isso, os responsáveis pelo tratamento devem processar dados pessoais limitados ao propósito específico para o qual foram processados. Esta obrigação colide com a quantidade de dados pessoais coletados, a extensão de seu processamento, o período de armazenamento e sua acessibilidade. A privacidade por padrão aplica o princípio da proporcionalidade porque protege uma invasão mínima do direito à privacidade.[125]

Além disso, o RGPD impõe cargas de prova mais pesadas em comparação com a diretiva. Primeiro, os responsáveis pelo tratamento devem provar que obtiveram o consentimento do indivíduo para o processamento de dados pessoais. Em segundo lugar, se o indivíduo se opuser ao processamento de dados, o responsável pelo tratamento deve demonstrar "motivos legítimos convincentes (...) que anulem os interesses, direitos e liberdades do titular dos dados" para justificar o processamento de dados pessoais e manter as informações online.[126] Portanto, alguns autores argumentaram que o RGPD torna mais fácil objetar às informações online e removê-las porque fornecer prova de consentimento e, especialmente, de motivos legítimos convincentes pode consumir tempo e recursos para o responsável pelo tratamento.[127]

---

[123] Keller, Daphne. *The Center for Internet and Society.* Stanford Law School, 2015. Disponível em <http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law>.
[124] Nunziato, Dawn Carla. Página 1056.
[125] Alessi, Stefania. Página 165.
[126] Alessi, Stefania. Página 165.
[127] Prorok, Christine. "The Right to be Forgotten" in the EU's General Data Protection Regulation. The Michigan Journal of International Law. The Michigan Journal of International Law, 2016

Finalmente, ao contrário da diretiva, o RGPD prevê[128] pesadas sanções administrativas. Por infração do Direito ao Esquecimento, os responsáveis pelo tratamento e subcontratantes poderiam ser multados em até 20 milhões de euros ou até quatro por cento de seu facturamento anual mundial total do exercício anterior.[129]

O "direito ao esquecimento" foi fortalecido quando comparado com o julgamento do Google Spain, pois inclui uma obrigação para o responsável pelo tratamento que tornou públicos os dados pessoais para informar outros responsáveis pelo tratamento que processam tais dados pessoais para apagar quaisquer links, ou cópias ou replicações desses dados pessoais. Ao fazê-lo, esse responsável pelo tratamento deve tomar medidas razoáveis, levando em conta a tecnologia disponível e os meios disponíveis para o responsável pelo tratamento, incluindo medidas técnicas.[130]

[128] O artigo 83.º, 5, do RGPD afirma que: A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:
a) Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5.º, 6.º, 7.º e 9.º; b) Os direitos dos titulares dos dados nos termos dos artigos 12.º a 22.º; c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44.º a 49.º; d) As obrigações nos termos do direito do Estado-Membro adotado ao abrigo do capítulo IX; e) O incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do artigo 58.º, n.º 2, ou o facto de não facultar acesso, em violação do artigo 58.º, n.º 1.
[129] Nunziato, Dawn Carla. Página 1051 - 1052.
[130] Burri, Mira; Schär, Rahel. Página 490.

2. A APLICAÇÃO EXTRATERRITORIAL DO DIREITO AO ESQUECIMENTO

A aplicação extraterritorial do direito ao esquecimento (ou à desindexação) continua sendo talvez a questão mais difícil a ser tratada em sua implementação. Um problema inerente ao uso de mecanismos de pesquisa é a sua capacidade de bloquear o acesso ao conteúdo online, o que impossibilita a execução perfeita. Como refere Luciano Floridi:

> "No entanto, temo que, em uma infosfera que não conhece fronteiras geográficas, agir nos mecanismos de busca para bloquear o acesso a conteúdos nunca será a solução definitiva. Se algum conteúdo for prejudicial, ele deverá ser bloqueado na origem, em qualquer mecanismo de pesquisa, em qualquer lugar ou removido completamente. Só isso seria uma implementação efetiva do direito de ser esquecido.[131]

O artigo 8.º da Declaração Universal dos Direitos Humanos (DUDH) afirma que "toda a pessoa tem direito a recurso efectivo para as jurisdições nacionais competentes contra os actos que violem os direitos fundamentais reconhecidos pela Constituição ou pela lei".[132]

O Tribunal de Justiça da União Europeia, no acórdão Lindqvist[133], entendeu que a criação de uma página na Internet, a sua instalação num servidor, bem como a introdução de informações pessoais disponíveis a todos quantos se conectem à Internet constituía sim um tratamento de dados pessoais por meios automatizados na acepção da Diretiva 95/46.[134]

O TJUE afirmou que o tratamento em causa não constituía o exercício de uma atividade exclusivamente pessoal ou doméstica exclusiva pela diretiva, pois tal exceção teria por objeto as atividades que se inserem no âmbito da vida privada e familiar, o que

[131]Floridi, Luciano. We dislike the truth and love to be fooled, em entrevista para a Cyceon em 21 de novembro de 2016
[132] Assembleia Geral da ONU. Declaração Universal dos Direitos Humanos. Paris, 1948.
[133] Tribunal de Justiça da União Europeia. Acórdão Lindqvist, de 6 de novembro de 2003, proc. C-101/01. Disponível em < https://curia.europa.eu/jcms/jcms/j_6/pt/>.
[134] Silveira, Alessandra; Marques, João. Página 99.

manifestamente não seria o caso do tratamento de dados pessoais disponibilizados via Internet a um número indeterminado de pessoas.[135]

O advogado de Lindqvist sustentou o contrário, porém o TJUE entendeu que o âmbito de aplicação da diretiva não se limita ao exercício de uma atividade económica, pois disciplina a circulação de dados pessoais também no exercício de atividades sociais, no contexto mais amplo de uma integração europeia orientada pela proteção de direitos fundamentais.[136]

Ou seja, se existe violação contra a proteção de dados pessoais e tudo que ela engloba, reconhecido no acórdão Lindqvist, pelo TJUE, e era previsto na Diretiva 95/46 e agora no RGPD como um direito fundamental da pessoa humana, cabe os Estados-Membros e seus tribunais, além das instituições europeias protegerem e darem recursos a todos que estão no território da UE exercerem seus direitos.

Os critérios de aplicação do regime da UE em matéria de proteção de dados pessoais encontravam-se no artigo 4.º da Diretiva 95/46[137], nomeadamente o âmbito de aplicação geográfico do mesmo, dentro e fora da UE. Na perspectiva dos operadores transnacionais, o artigo 4.º era a disposição mais importante da diretiva uma vez que estipulava a (não) aplicabilidade da mesma às respetivas atividades. Por outro lado, aquela era uma disposição importante do ponto de vista do titular dos dados, o beneficiário e titular do bem jurídico protegido, uma vez que estabelecia os termos e limites da proteção garantida pelo regime da UE quanto aos seus dados pessoais.[138]

O funcionamento do artigo 4.º assentava em dois critérios principais, sendo o primeiro critério centrado nos responsáveis pelo tratamento estabelecidos na UE, que

[135] Silveira, Alessandra; Marques, João. Página 99.
[136] Silveira, Alessandra; Marques, João. Página 99.
[137] Artigo 4º: 1. Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente directiva ao tratamento de dados pessoais quando:
a) O tratamento for efectuado no contexto das actividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável;
b) O responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público;
c) O responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade.
2. No caso referido na alínea c) do nº 1, o responsável pelo tratamento deve designar um representante estabelecido no território desse Estado-membro, sem prejuízo das acções que possam vir a ser intentadas contra o próprio responsável pelo tratamento.
[138] Moniz, Graça Canto. Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD. UNIO - EU Law Journal, Vol. 4(Nº. 2), p. 121, 2018.

seria a "pessoa singular ou coletiva, 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[139], e o segundo critério dirigido aos responsáveis pelo tratamento de países terceiros ou não estabelecidos na UE, ou seja, a nacionalidade do responsável pelo tratamento, o local do seu estabelecimento principal ou a localização física do tratamento seriam irrelevantes para apurar a aplicação do direito da UE. Por conseguinte, o mesmo pode ser aplicado quando o estabelecimento principal estiver localizado num país terceiro.[140] Com efeito, foi justamente o sucedido no caso Google Spain.[141]

No que diz respeito ao seu âmbito territorial, a diretiva aplica-se não apenas aos responsáveis pelo tratamento estabelecidos no território da UE ou do Espaço Económico Europeu (EEE), mas também aos estabelecidos fora da UE ou do EEE em algumas circunstâncias, incluindo o caso em que "o tratamento é efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento", localizado no território de um Estado-Membro da UE ou do EEE.[142]

As organizações que não estão estabelecidas na UE/ EEE estão sujeitas ao RGPD quando processam dados pessoais de titulares de dados que estão na UE/EEE se as atividades de processamento estiverem relacionadas "à oferta de bens ou serviços" a tais sujeitos de dados no UE/EEE, ou "a monitorização do seu comportamento", na medida em que o seu comportamento ocorre dentro da UE/EEE.[143]

A aplicação do RGPD numa situação concreta não é o local de estabelecimento do responsável pelo tratamento, mas a localização do titular dos dados na União, seja este nacional, residente ou viajante temporário. Esta irrelevância da intensidade do vínculo do titular dos dados com a UE está de acordo com o objetivo da Diretiva 95/46, reiterado no

[139] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, artigo 2.º, alínea d.
[140] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, considerando 19: "considerando que o estabelecimento no território de um Estado-membro pressupõe o exercício efectivo e real de uma actividade mediante uma instalação estável; que, para o efeito, a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, não é determinante; que, quando no território de vários Estados-membros estiver estabelecido um único responsável pelo tratamento, em especial através de uma filial, deverá assegurar, nomeadamente para evitar que a legislação seja contornada, que cada um dos estabelecimentos cumpra as obrigações impostas pela legislação nacional aplicável às respectivas actividades;
[141] Moniz, Graça Canto. Página 122.
[142] Peguera, Miquel. Página 516.
[143] Gilbert, Francoise. GDPR: EU General Data Protection Regulation. *Orange County Lawyer*, *Volume 60*, 23-26, 2018.

RGPD, de garantir a proteção de todas as pessoas singulares, independentemente da sua nacionalidade ou local de residência, como decorre dos considerandos[144] 2 e 14.[145]

As instituições europeias endossam a visão de que a exclusão deveria ter um alcance extraterritorial. Quanto ao efeito territorial das decisões de exclusão, as orientações do Grupo de Trabalho do Artigo 29.º[146] observaram que a limitação da exclusão dos domínios da UE não pode ser considerada um meio suficiente para garantir satisfatoriamente os direitos dos titulares de dados de acordo com a decisão. Na prática, "isso significa que, em qualquer caso, a exclusão da listagem também deve ser eficaz em todos os domínios relevantes".[147]

Sendo assim, o RGPD pode influenciar de maneira significativa o estabelecimento de padrões globais para proteção de dados on-line em virtude de seu escopo territorial, como responsáveis pelo tratamento de dados pode ser esperado para ajustar a sua conformidade de acordo com o mais alto nível de proteção de dados exigido a partir deles.[148]

2.1. Acórdão Schrems (C- 362/14)

No acórdão Schrems, o TJUE fez pelo menos duas constatações cruciais para a prática de proteção de dados da UE e sua dimensão transatlântica. O tribunal luxemburguês considerou que a existência de uma decisão da Comissão que declara que um país terceiro assegura um nível de proteção adequado não pode eliminar nem reduzir os poderes das autoridades supervisoras nacionais de controlar e avaliar a adequação da proteção de dados nos termos da Carta dos Direitos Fundamentais da UE e da Diretiva

[144] Considerando 2: Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.
Considerando 4: O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdade e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística.
[145] Moniz, Graça Canto. Página 128.
[146] O Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do Regulamento Geral de Proteção de Dados).
[147] Grupo de Trabalho do Artigo 29.º. 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" C-131/12, 2014.
[148] Gömann, Merlin. The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement. Common Market Law Review, Volume 54(Issue 2), p. 584, 2017.

95/46 relativa à proteção de dados (embora permaneça exclusivamente dentro da própria jurisdição do tribunal declarar que um ato da UE, tal como uma decisão da Comissão, é inválido).[149]

O TJUE, nesse caso, seguiu a opinião do Advogado-Geral Yves Bot e declarou inválida a estrutura do "Porto Seguro", ao esclareceu que a vigilância em massa pelos serviços de segurança nos EUA para com aqueles que estão na UE é uma violação de seus direitos fundamentais e que os reguladores de proteção de dados podem decidir suspender a transferência de dados se encontrarem que as proteções oferecidas aos cidadãos europeus são inadequados, o que significa que não têm de obter uma decisão de inadequação por parte da Comissão Europeia.[150]

Ou seja, o TJUE assegurou os direitos fundamentais a proteção de dados de forma transatlântica ao proteger as pessoas que estão na UE, e assegurou o entendimento que para o dado pessoal ser transferido a países terceiros, o país que recebe o dado deverá assegurar a mesma segurança que a UE propõe em seu território. Essa decisão será elucidada a seguir.

Devido à grande diferença nas leis de proteção da privacidade entre a UE e os Estados Unidos da América (EUA), as Autoridades Europeias de Proteção de Dados (APD) consideraram as leis dos EUA inadequadas. Embora isso pareça ter constituído um grande obstáculo para o funcionamento da economia digital global, os EUA e a UE superaram isso ao formar o Regime do "Porto Seguro" estabelecido pela Decisão 2000/520[151].[152]

[149] Burri, Mira; Schär, Rahel. Página 486.
[150] Hall, Holly Kathleen. Restoring Dignity and Harmony to United States-European Union Data Protection Regulation. Communication Law and Policy, Volume 23, p. 135, 2018.
[151] Em relação aos Estados Unidos da América, a Decisão 2000/520 deixa claro em seu 5.º ponto a relação construída, colocando que: "O nível adequado de proteção da transferência de dados a partir da Comunidade Europeia para os Estados Unidos da América (EUA), nos termos da presente decisão, pode conseguir-se se as organizações derem cumprimento aos princípios da "privacidade em porto seguro" relativos à proteção de dados pessoais transferidos de um Estado-Membro para os EUA (a seguir denominados "os princípios") e às diretrizes das questões mais frequentes (a seguir designadas "FAQ") que servem de guia no que respeita à aplicação dos princípios estabelecidos pelo Governo dos Estados Unidos em 21 de Julho de 2000. Por outro lado, as organizações devem dar a conhecer publicamente as suas políticas em matéria de proteção da vida privada e ficar abrangidas pelo âmbito da competência da Federal Trade Comission (FTC) que, nos termos do artigo 5.o da lei relativa ao comércio federal (Section 5 of the Federal Trade Commission Act), garante a proibição dos atos ou as práticas desleais ou enganosas relativas ao comércio, ou de outros organismos públicos que efetivamente assegurem o respeito dos princípios aplicados em conformidade com as FAQ.".
[152] McAllister, Craig. What About Small Businesses? The GDPR and its Consequences for Small, U.S.-Based Companies. Brooklyn Journal of Corporate, Financial & Commercial Law, p. 190, 2017.

As empresas americanas podem certificar que estão em conformidade com os princípios de proteção de dados do Regime do "Porto Seguro". A auto certificação[153] significava essencialmente que a empresa atestava publicamente que cumpre determinados padrões de privacidade europeus. Depois que uma empresa se auto certificou, ela pode transferir dados pessoais da EEE para os EUA sem entrar em conflito com a diretiva. O Regime do "Porto Seguro", portanto, forneceu às empresas sediadas nos EUA um método relativamente acessível de garantir a conformidade com as leis de privacidade mais estritas, permitindo também o fluxo contínuo de dados pessoais do EEE para os EUA. Em 2015, aproximadamente 4.400 empresas participaram do Safe Harbor.[154]

Porém em 2015 o acordo foi alterado pelo Tribunal de Justiça da União Europeia (TJUE), pois, através de Maximillian Schrems, segundo o acórdão, cidadão austríaco residente na Áustria, é utilizador da rede social Facebook desde 2008. Todas as pessoas que residam no território da UE e pretendam utilizar o Facebook são obrigadas, no momento da sua inscrição, a celebrar um contrato com a Facebook Ireland, filial da *Facebook Inc.*, com sede nos EUA. Os dados pessoais dos utilizadores do Facebook residentes no território da UE são, por completo ou em parte, transferidos para servidores pertencentes à Facebook Inc., situados em território dos EUA, onde são objeto de tratamento.[155]

Em 25 de junho de 2013, M. Schrems apresentou ao Comissário uma queixa em que lhe pedia que exercesse as suas competências estatutárias proibindo a Facebook Ireland de transferir os seus dados pessoais para os EUA. Alegava que o direito e as práticas em vigor neste país não asseguravam uma proteção suficiente dos dados pessoais conservados no seu território contra as atividades de vigilância aí exercidas pelas autoridades públicas. O autor baseou seu pedido nas revelações feitas por Edward

[153] O segundo e terceiro ponto do artigo 1.º da Decisão 2000/520 coloca que: "2. No que respeita a cada transferência de dados: a) A organização destinatária dos dados comprometer-se-á clara e publicamente a cumprir os princípios aplicados em conformidade com as FAQ; e b) A referida organização fica sujeita aos poderes legais dos entes públicos administrativos norte-americanos referidos no anexo VII da presente decisão, com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de pessoas singulares, independentemente do seu país de residência ou da sua nacionalidade, sempre que se verificar incumprimento dos princípios segundo as orientações das FAQ. 3. Considera-se que a organização que declarar a sua adesão aos princípios aplicados em conformidade com as FAQ cumpre o disposto no n.o 2, a partir da data em que comunicar ao Department of Commerce dos EUA ou ao seu representante, a divulgação do compromisso referido na alínea a) do n.o 2, bem como a identidade da entidade pública a que se refere a alínea b) do n.o 2.".
[154] McAllister, Craig. Página 190.
[155] Tribunal de Justiça da União Europeia. Acórdão C-362/14 - Maximillian Schrems contra Data Protection Commissioner, 2015.

Snowden sobre as atividades dos serviços de informação dos EUA, nomeadamente as da National Security Agency (Agência Nacional de Segurança, a NSA).[156]

O Comissário, entendendo que não estava obrigado a pesquisar sobre o facto denunciado arquivou-a pôr falta de fundamento, e considerou que não havia provas de que a NSA tivesse acesso aos dados pessoais do interessado. Acrescentou que as críticas suscitadas por M. Schrems na sua queixa não podiam ser invocadas de forma útil, dado que qualquer questão relativa ao caráter adequado da proteção dos dados pessoais nos EUA devia ser decidida em conformidade com a Decisão 2000/520 e que, nesta decisão, a Comissão tinha constatado que os EUA asseguravam um nível de proteção adequado.[157]

M. Schrems interpôs recurso para a High Court, o Supremo Tribunal de Justiça, sobre a decisão em causa no processo principal. Depois de ter analisado as provas apresentadas pelas partes no processo principal, aquele órgão jurisdicional declarou que a vigilância eletrónica e a interceção de dados pessoais transferidos da EU para os EUA respondiam a finalidades necessárias e indispensáveis ao interesse público. Porém, o referido órgão jurisdicional acrescentou que as revelações de E. Snowden tinham demonstrado que a NSA e outros órgãos federais cometeram "excessos consideráveis".[158]

O Supremo Tribunal de Justiça declarou então que o direito irlandês proíbe a transferência de dados pessoais para fora do território nacional, salvo se o país terceiro em questão assegurar um nível adequado de proteção da vida privada bem como dos direitos e liberdades fundamentais.[159]

Assim, segundo o Supremo Tribunal de Justiça, se o processo principal fosse julgado apenas com base no direito irlandês haveria então que concluir que atendendo à existência de uma dúvida séria sobre a questão de saber se os EUA asseguram um nível de proteção adequado dos dados pessoais, o Comissário devia ter procedido a uma investigação dos factos denunciados por M. Schrems na sua queixa, e que não teve razão ao arquivá-la.[160]

[156] Idem
[157] Idem
[158] Idem
[159] Idem
[160] Idem

Entretanto, o Supremo Tribunal de Justiça considera que este processo respeita a aplicação do Direito da União na aceção do artigo 51.° da Carta, pelo que a legalidade da decisão em causa no processo principal deve ser apreciada à luz do direito da UE.[161]

Segundo esse órgão jurisdicional, a Decisão 2000/520 não satisfaz os requisitos que decorrem tanto dos artigos 7.° e 8.° da Carta como dos princípios estabelecidos pelo Tribunal de Justiça no acórdão Digital Rights Ireland, referido no tópico passado. O direito ao respeito da vida privada, garantido pelo artigo 7° da Carta e pelos valores fundamentais comuns às tradições constitucionais dos Estados-Membros, ficaria privado do seu alcance se permitisse que os poderes públicos acedessem às comunicações eletrónicas de forma aleatória e generalizada, sem nenhuma justificação objetiva baseada em considerações de segurança nacional ou de prevenção da criminalidade, associadas especificamente aos indivíduos em causa e sem que essas práticas fossem rodeadas de garantias adequadas e verificáveis.[162]

O Supremo Tribunal de Justiça ressalva que no seu recurso, M. Schrems questiona na realidade a legalidade do regime do "Porto Seguro" estabelecido pela Decisão 2000/520 e do qual procede a decisão em causa no processo principal. Assim, embora M. Schrems não tenha contestado de modo formal a validade da Diretiva 95/46 nem da Decisão 2000/520, coloca-se a questão, segundo aquele órgão jurisdicional, de saber se, nos termos do artigo 25.°, n° 6, desta diretiva, o Comissário estava vinculado pela constatação efetuada pela Comissão na decisão, segundo a qual os EUA asseguram um nível de proteção adequado, ou se o artigo 8° da Carta autorizava o Comissário a afastar-se, sendo caso disso, dessa constatação.[163]

O TJUE julgou da seguinte forma:

> 1) O artigo 25.°, n.° 6, da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conforme alterada pelo Regulamento (CE) n.°1882/2003 do Parlamento Europeu e do Conselho, de 29 de setembro de 2003, lido à luz dos

[161] Idem
[162] Idem
[163] Idem

> artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ), emitidos pelo Departamento de Comércio dos Estados Unidos da América, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.° desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado.
>
> 2) A Decisão 2000/520 é inválida.[164]

Em oposição Edward M. Dean, ex-subsecretário adjunto para Serviços na Administração do Comércio Internacional do Departamento de Comércio, afirmou que o Regime do “Porto Seguro” foi o desafortunado bode expiatório de revelações geopolíticas mais amplas no que diz respeito à vigilância. Completou dizendo que "desde que o Safe Harbor se tornou vinculado às divulgações de vigilância, tornou-se alvo de críticas contínuas amplamente baseadas em mal-entendidos e falsas suposições sobre seu propósito e operação e os importantes benefícios de privacidade que proporcionava". No centro das críticas, disse Dean, estavam "falsas acusações de que os EUA estavam empenhados em “vigilância indiscriminada e em massa” dos dados transferidos para os EU ao abrigo do Safe Harbor".[165]

[164] Idem
[165] U.S.-EU Safe Harbor Framework. Testimony of Edward M. Dean, Deputy Assistant Secretary for Services, International Trade Administration, U.S. Department of Commerce, 2015. Disponível em < https://docs.house.gov/meetings/IF/IF16/20151103/104148/HHRG-114-IF16-20151103-SD012.pdf>.

Para os autores Alessandra Silveira e João Marques o TJUE considerou que o termo "adequado" que figura no artigo 25°, n° 6, da Diretiva 95/46 não exige que um país terceiro assegure um nível de proteção idêntico ao garantido na ordem jurídica da UE, mas exige que esse país terceiro assegure efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção dos direitos fundamentais substancialmente equivalente ao conferido pela UE.[166]

Com fundamento na segurança nacional, no interesse público ou na legislação interna dos EUA, a Decisão 2000/520 permitia interferências nos direitos fundamentais dos indivíduos cujos dados pessoais fossem ou pudessem ser transferidos da UE para os EUA e não continha qualquer alusão à existência de normas propostas a limitar intervenções que prosseguissem objetivos legítimos ou relativas à proteção jurídica eficaz contra as mesmas. Entendeu o TJUE que não é limitada ao estritamente necessário uma regulamentação que autoriza de modo generalizado a conservação da totalidade dos dados pessoais transferidos da EU para os EUA, primeiramente sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido, posteriormente sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos.[167]

Ao chegar a esta decisão, o TJUE concluiu que a "segurança nacional, interesse público e aplicação da lei" prevaleceu sobre os princípios do "Porto Seguro" quando em conflito. O "Porto Seguro" permitiu e até mesmo "ativou" a interferência da força pública americana nos direitos fundamentais dos dados dos cidadãos europeus.[168]

Antes da decisão da Schrems, os EUA e a EU pretendiam mudar a estrutura legal do "Porto Seguro".[169] Alguns meses após a decisão do tribunal, os EUA e a EU anunciaram um novo acordo, o Privacy Shield, para substituir o "Porto Seguro". Não está claro se o Escudo de Privacidade pode sobreviver a futuros escrutínios ou batalhas legais. Um dos desafios mais iminentes que o Privacy Shield enfrenta é o GDPR; O "Privacy Shield" precisará de ser revisto para se adequar ao novo marco legal. O próprio Max Schrems comentou o acordo dizendo que "é melhor que Safe Harbor, obviamente, mas

[166] Silveira, Alessandra; Marques, João. Páginas 104 – 105.
[167]Silveira, Alessandra; Marques, João. Páginas 105.
[168] Taylor, Rachel C.. Intelligence-Sharing Agreements & International Data Protection: Avoiding a Global Surveillance State. Washington University Global Studies Law Review, p. 752, 2018.
[169] Daugirdas, Kristina; Mortensen, Julian Davis. European Union and United States Conclude Agreement to Regulate Transatlantic Personal Data Transfers. American Journal of International Law, Volume 110, Issue 2, p.362, 2016.

longe do que o TJUE pediu". Como previsto, o Privacy Shield já foi questionado no tribunal. Apesar da opinião da Comissão Europeia de que o Privacy Shield é suficientemente robusto para cumprir a Diretiva Europeia de Proteção de Dados no lugar de "Porto Seguro", não é claro como o TJEU responderá aos desafios levantados.[170]

O pedido de M. Schrems questiona a compatibilidade de uma decisão da Comissão Europeia adotada nos termos do artigo 25°, n° 6, da referida Diretiva com a proteção dos direitos fundamentais protegidos pela UE. Entretanto, o artigo 3°, n° 1, primeiro parágrafo, da Decisão 2000/520 prevê uma regulamentação específica quanto aos poderes de que dispõem as autoridades nacionais de controle perante uma constatação efetuada pela Comissão Europeia relativamente ao nível de proteção adequado previsto no artigo 25° da Diretiva 95/46, ou seja, tal disposição da Decisão 2000/520 coíbe as autoridades nacionais de controle dos poderes que lhes são conferidos pelo artigo 28° da Diretiva 95/46. Sendo assim, o poder de execução atribuído pelo legislador da UE à Comissão Europeia no artigo 25°, n° 6, da Diretiva 95/46 não afere a esta instituição competência para limitar os poderes das autoridades nacionais de controle, razão pela qual a Comissão Europeia teria ultrapassado a competência que lhe é atribuída. Neste pressuposto, e atendendo a todas as considerações precedentes, o TJUE concluiu que a Decisão 2000/520 era inválida, cumprindo ao tribunal nacional do reenvio dar provimento à pretensão do requerente.[171]

Ou seja, o TJUE seguiu o Advogado-Geral e declarou inválido o Regime do Porto Seguro e assegurou os direitos fundamentais da proteção de dados aos que estão no território da UE.

Algumas organizações, incluindo o Google, iniciaram uma abordagem pró-ativa no pós "Porto Seguro". O Google enviou uma mensagem aos utilizadores da plataforma em nuvem, garantindo aos utilizadores que nada era mais importante do que "confiança, privacidade e segurança" e que, enquanto aguardavam um novo contrato do tipo utilizadores, adotavam as Cláusulas do Modelo de Contrato para transferência de dados da EU para os EUA.[172]

[170] Taylor, Rachel C.. Páginas 752 – 753.
[171] Silveira, Alessandra; Marques, João. Página 106.
[172] Taylor, Rachel C.. Páginas 752.

Em junho de 2016, os EUA e a EU concluíram as negociações do "Umbrella Agreement", fornecendo uma estrutura de proteção de dados para dados pessoais trocados entre os EUA e a EU para a prevenção, deteção, investigação e repressão de crimes para aplicação da lei. O acordo inclui especificamente o terrorismo dentro dos crimes que abrange. Com relação à estrutura, o "Umbrella Agreement" concentra-se no seguinte: (1) limitar o uso de dados àquele relacionado à abordagem da atividade criminosa; (2) restringir a transferência posterior dos dados para os casos em que o consentimento prévio é obtido do país que inicialmente forneceu os dados; (3) exigindo períodos de retenção para os dados obtidos para se tornarem públicos; e (4) fornecer ao indivíduo a quem os dados se referem o direito de acessar e corrigir imprecisões. O "Umbrella Agreement" não autoriza transferências de dados, mas fornece salvaguardas acordadas para dados compartilhados para fins de aplicação da lei, abordando preocupações anteriores da UE sobre a falta de salvaguardas acordadas.[173]

2.2. Caso Google Inc. vs. Commission nationale de l'informatique et des libertés (CNIL) (C-507/17)

De acordo com a decisão da agência francesa de proteção de dados (a Comissão Nacional de Tecnologia da Informação e Liberdades), quando uma pessoa solicita que um motor de pesquisa remova as referências ao seu nome a partir de certas informações, o motor de pesquisa deve fazê-lo não só em domínios europeus, mas em todos os seus domínios.[174]

De acordo com o argumento, apenas a desindexação global permitiria a eficácia e proteção global dos direitos dos cidadãos franceses. O motor de pesquisa recusou-se a cumprir esta decisão e depois de ter apelado ao Conselho de Estado, este reenviou prejudicialmente questionamentos ao TJUE.[175]

[173] Swire, Peter; Kennedy-Mayo, DeBrae. How Both the EU and the U.S. are "Stricter" than each other for the Privacy of Government Requests for Information. Emory Law Journal, Volume 66, 634 - 635, 2017.
[174] Commission Nationale de l'Informatique et des Libertés. Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X, 10 de março de 2016.
[175] Tribunal de Justiça da União Europeia. Acórdão C-507/17 - Request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017 — Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), 2017.

O Processo C-507/17 surgiu do desdobramento da "Deliberação da formação restrita n.° 2016-054 de 10 de março de 2016, pronunciando multa financeira contra a sociedade X", a sociedade X que é o Google.[176]

Essa deliberação foi baseada no processo C-131/12, já referido anteriormente nesse trabalho, e na Diretiva 95/46. O Tribunal francês teve o seguinte entendimento:

> "Por conseguinte, esta última é obrigada a respeitar os direitos de apagamento e de oposição previstos nos artigos 12. ° e 14. ° da diretiva, ao aplicar, quando as condições de aplicação destas disposições estiverem preenchidas, a desindexação de determinadas ligações. Essa técnica consiste em remover da lista de resultados exibidos como resultado de uma pesquisa sobre o nome de uma pessoa, links para páginas da Web publicadas por terceiros e contendo informações relativas a essa pessoa.
>
> O Tribunal declarou que o pedido de referência, diretamente submetido ao operador de motor de busca sem recurso prévio aos editores de sites da Internet, poderia ser aceite mesmo que a publicação das informações nos sites em questão fosse, por si só, mesmo legal.
>
> O Tribunal de Justiça considerou que, para avaliar o mérito de um pedido de exclusão, os direitos fundamentais à privacidade e à proteção dos dados pessoais prevalecem, em princípio, não apenas no interesse económico o operador do mecanismo de busca, mas também o interesse público em encontrar essa informação em uma busca pelo nome dessa pessoa. Contudo, não seria esse o caso se, por razões especiais, como o papel desempenhado por essa pessoa na vida pública, a interferência nos seus direitos fundamentais se justificasse pelo interesse superior desse público em ter como resultado desta inclusão, o acesso à informação em questão (parágrafo 99).

[176] Commission Nationale de l'Informatique et des Libertés. Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X, 10 de março de 2016.

> O Tribunal recordou ainda que o tratamento em questão, permitindo que qualquer usuário para obter uma visão geral estruturada das informações relacionadas com uma pessoa na Internet, fornecendo um perfil mais ou menos detalhada do último é suscetível de afetar de forma significativa os direitos fundamentais das pessoas, garantida pelos artigos 7 e 8 da Carta dos direitos fundamentais da União Europeia.
>
> Por último, o Tribunal de Justiça declarou que as recusas de desindexação ou as respostas insatisfatórias do operador poderiam ser impugnadas, em especial, perante a autoridade nacional de proteção de dados."

A Comissão Nacional para a Proteção de Dados e Liberdades (doravante CNIL ou a Comissão) é regularmente procurada por utilizadores da internet que residem na França para contestar a recusa do Google em conceder seu pedido de desindexação – e reportou ao Google, no dia 9 de abril de 2015, por meio de carta, que, para serem eficazes as anulações, não deveriam limitar-se às extensões europeias do seu motor de pesquisa.

Por meio de carta também, como descrito no processo, no dia 24 de abril de 2015, o Google assinalou que continuaria suas reflexões sem efetuar qualquer alteração em seu sistema, pois poderia garantir a efetividade do direito de desindexação.

A narrativa da deliberação continua no dia 21 de maio de 2015, quando o presidente da CNIL notificou formalmente o Google para "se retirar das extensões do nome de domínio de seu mecanismo de pesquisa dentro de quinze dias."

Em 8 de junho de 2015, a Mesa composta regularmente pelo Presidente e pelos dois Vice-Presidentes da Comissão, decidiu publicitar a notificação em conformidade com as disposições do artigo 13.º- I da Lei de Proteção de Dados.

Segundo a deliberação, a Mesa levou em conta, por um lado, a necessidade de informar os operadores de motores de pesquisa, os utilizadores da internet e os editores de conteúdos do âmbito dos direitos de oposição e supressão de dados e, por outro lado, para garantir a plena eficácia desses direitos, estendendo as desindexações já concedidas pela empresa a todos os nomes de domínio do mecanismo de pesquisa. A notificação

formal e a deliberação do escritório, nas versões francesa e inglesa, foram notificadas à empresa Google.

A pedido do próprio Google, no dia 18 de junho de 2015, foi realizada reunião na sede da CNIL, conforme a deliberação, para entrar em conformidade o que deveria ser alterado. Por carta a empresa pediu tempo adicional para realizar todas as analises técnicas e jurídicas necessárias, e foram concedidos 3 dias de tempo extra.

Em 18 de junho de 2015, conforme descreve a deliberação de dia 30 de julho de 2015, a Companhia entrou com um recurso gratuito junto ao Presidente da CNIL para obter a retirada do aviso de incumprimento e da medida de publicidade associada. Este recurso foi rejeitado por carta de 16 de setembro de 2015, comunicada à instituição francesa por carta de 21 de setembro seguinte. No final de sua investigação, a CNIL notificou o Google, em 17 de novembro de 2015, em um relatório detalhando as violações da Lei de Proteção de Dados que considerava constituídas e solicitando o pronunciamento de uma sanção financeira pública.

Também foi incluído no relatório um aviso da sessão de Treino Restrito de 28 de janeiro de 2016 indicando à organização que tinha um período de um mês para enviar seus comentários por escrito. Em 18 de janeiro de 2016, o Google enviou comentários por escrito sobre o relatório, que foram reiterados oralmente na reunião realizada em 28 de janeiro de 2016.

Como justificativa para a decisão, a deliberação traz que, para proteger a sua privacidade e os seus dados pessoais, as pessoas singulares têm o direito de solicitar ao responsável pelo tratamento de dados que apague os seus dados, em particular devido à sua natureza incompleta ou imprecisa e opor-se, por razões legítimas, ao tratamento dos seus dados, como previa a Diretiva 95/46.

Complementa dizendo que os artigos acima citados devem ser interpretados conforme a decisão do acórdão Google, de 13 de maio de 2014, proc. C-131/12, que exige que a aplicação concreta dos direitos de oposição e a supressão, através do procedimento de desindexação, garantam a eficácia dos direitos fundamentais dos titulares dos dados, nomeadamente o direito ao respeito pela vida privada e à proteção de dados pessoais, sem a possibilidade de evasão.

Para o tribunal francês, o TJUE afirmou que o objetivo da então Diretiva 95/46, vigente a época, era a garantir a proteção completa dos direitos fundamentais em específico naqueles que se referem a vida privada, colocando que:

> "O objetivo da Diretiva 95/46 [é] assegurar uma proteção eficaz e abrangente dos direitos e liberdades fundamentais das pessoas singulares, incluindo o direito à privacidade, no que diz respeito ao tratamento de dados pessoais (ponto 53),
>
> A Diretiva 95/46 visa assegurar um elevado nível de proteção dos direitos e liberdades fundamentais das pessoas singulares, incluindo as suas vidas privadas, no que diz respeito ao tratamento de dados pessoais (ponto 66).
>
> O operador desse motor, enquanto pessoa, para determinar os fins e os meios dessa atividade, deve assegurar, no âmbito das suas responsabilidades, competências e possibilidades, o cumprimento dos requisitos da Diretiva 95/46. assegurar que as salvaguardas previstas por ele possam ser totalmente eficazes e que uma proteção efetiva e abrangente das pessoas envolvidas, incluindo seu direito ao respeito por suas vidas privadas, possa efetivamente ser alcançada. (considerando 38)
>
> Afirma igualmente que a proteção concedida pela Diretiva 95/46/CE deve aplicar-se a todos os residentes europeus sem a possibilidade de evasão:
>
> Resulta dos considerandos 18 a 20 e o artigo 4.º da Diretiva 95/46 que o legislador da União pretendeu evitar que uma pessoa fosse excluída da proteção garantida por esta diretiva e que essa proteção fosse contornada, que prevê um âmbito territorial particularmente vasto (ponto 54).
>
> Não se pode aceitar que o tratamento de dados pessoais efetuado para efeitos da exploração desse motor de busca esteja isento das obrigações e garantias previstas pela Diretiva 95/46, o que

> prejudicaria a eficácia desse mecanismo de pesquisa. e a proteção eficaz e abrangente dos direitos e liberdades fundamentais das pessoas singulares que pretende assegurar (v., por analogia, L'Oréal e o., EU: C: 2011: 474, pontos 62 e 63), em especial o respeito pela vida privada (ponto 58).”

O Google, por outro lado, em resposta ao CNIL, conforme descrito na deliberação, contestou, em primeiro lugar, que o aviso formal não tem base jurídica na medida em que se baseia numa regra jurídica imprecisa e imprevisível e, por outro lado, que não é com base em queixas específicas.

O Google afirmou que a CNIL excede seus poderes, impondo-lhe uma medida extraterritorial, sustentando primeiramente que a Lei francesa, Lei n.º 78-17, de 6 de janeiro de 1978, conforme alterada, não se aplica a solicitações feitas no mecanismo de pesquisa fora da França, que correspondem a uma atividade que não é direcionada a utilizadores franceses da Internet nem indissociável a sua subsidiária francesa..

O Google explica na deliberação que os termos de pesquisa do mecanismo de pesquisa, seja a origem geográfica do utilizador que realiza a pesquisa, o idioma usado para exibir os resultados, a classificação dos resultados na lista e os termos da pesquisa em si, constituem tantas operações sob o mesmo tratamento da informação. E completa dizendo que, as várias extensões geográficas do motor de pesquisa foram criadas ao longo do tempo pela empresa, a fim de oferecer um serviço adaptado à língua nacional de cada país, ao passo que explorou inicialmente o seu serviço, somente através do nome de domínio único “google.com”.

Neste ponto o Google faz referência ao acórdão de 13 de maio de 2014, colocando que:

> “Deve notar-se que, explorando automaticamente, de forma constante e sistemática, a Internet para informação aí publicada, 'um mecanismo de pesquisa coleta esses dados que subsequentemente extrai, armazena e organiza como parte de seus programas de indexação, armazena em seus servidores e, quando apropriado, comunica e disponibiliza para seus usuários forma de listas dos resultados de sua pesquisa. Uma vez que estas

> operações estão explícita e incondicionalmente abrangidas pelo artigo 2. °, alínea b), da Diretiva 95/46, devem ser consideradas um tratamento na aceção dessa disposição (...) (n. ° 28).”

Complementa o raciocínio dizendo que a Lei de Proteção de Dados francesa é aplicável a todo o processamento relacionado a serviços, no território nacional, a atividade do motor de busca instalado, se referindo ao processo anterior citado, disse:

> “Resulta do exposto que a primeira questão deve ser respondida, a), que o artigo 4. °, n. ° 1, alínea a), da Diretiva 95/46 deve ser interpretado no sentido de que o tratamento de dados pessoais é efetuado no contexto das atividades de um estabelecimento da responsável por esse tratamento no território de um Estado-Membro, na aceção dessa disposição. Sempre que o operador de um motor de pesquisa estabeleça, num Estado-Membro, uma sucursal ou filial para promover e vender o espaço publicitário oferecido por esse motor e cuja atividade se destina aos habitantes desse Estado-Membro”.

O Google argumentou que é competência da Comissão determinar os procedimentos de desindexação quando o tratamento em questão é implementado, na aceção do artigo 48.º do Regulamento (UE) 2016/649 no todo ou em parte, no território nacional francês, inclusive quando o responsável pelo tratamento está estabelecido no território de outro Estado-Membro da Comunidade Europeia.

A empresa também argumenta que uma desindexação em todos os finais do mecanismo de pesquisa viola o princípio da lei internacional de cortesia e afeta a soberania dos estados por causa de seus efeitos extraterritoriais.

Em terceiro e último ponto, o Google, dentro da deliberação, argumentou que uma deserção global iria infringir desproporcionalmente a liberdade de expressão e informação, afirmando que:

> “A decisão de desindexar é tomada, conforme especificado pelo Tribunal de Justiça, apenas se as condições para a aplicação dos

> direitos de oposição (sujeito à prova de um interesse legítimo) ou de cancelamento (condicionado em particular à demonstração da natureza obsoleta, incompleta ou errada das informações em questão). Assim, intervém no final de um controlo de proporcionalidade destinado a preservar o equilíbrio estrito entre, por um lado, o respeito dos direitos à vida privada e a proteção dos dados pessoais das pessoas e, por outro lado, o interesse público em ter acesso a informações, particularmente no caso de um papel desempenhado na vida pública do candidato.
>
> Uma limitação das desindexações às extensões europeias parece, por um lado, infundada, na medida em que os diferentes nomes de domínio (para [...] a França, para a Espanha, para a Austrália, etc.). são apenas caminhos técnicos para aceder a um único tratamento e, em segundo lugar, imperfeitos na medida em que as ligações não referenciadas permanecem acessíveis a partir das extensões não europeias do motor de pesquisa.
>
> Assim, qualquer utilizador, onde quer que esteja, pode aceder a páginas web não referenciadas, realizando a sua pesquisa a partir de uma extensão não europeia do motor de pesquisa.
>
> Tal medida não permite responder aos imperativos de eficiência, exaustividade, eficácia e não-evasão exigidos pela decisão do TJUE acima mencionada, na medida em que a violação da privacidade e da confidencialidade a proteção dos dados pessoais dos sujeitos de dados persiste.
>
> Portanto, apenas um desindexação de todo o mecanismo de pesquisa provavelmente permitirá a proteção efetiva dos direitos dos indivíduos."

Em decisão, a CNIL sentenciou que o Google foi legitimamente criticado no aviso de 21 de maio de 2015, por não prosseguir com as desindexações em todas as extensões do nome de domínio do motor de pesquisa. A CNIL disse, em uma carta enviada ao Presidente do G29 em 21 de janeiro de 2016, após o prazo final para

cumprimento, que a empresa assumiu o compromisso de melhorar seu dispositivo de desindexação, indicando que seria estendido a todos os domínios do seu mecanismo de pesquisa (incluindo versões do Google para países fora da UE) quando a solicitação aparece como originária do país do solicitante, sendo o país determinado em prioridade pelo endereço IP do utilizador.

Mas para a CNIL, esse critério de localização baseando no IP do usuário não seria satisfatório, partindo do princípio que a informação não desindexada permanece disponível para qualquer utilizador fora do território abrangido pela medida de filtragem e, por outro lado, a evasão desta medida pelos utilizadores em causa continua a ser possível.

Complementa dizendo que esta solução impede que um residente francês tenha acesso o conteúdo não indexado a partir do território francês, mas não fora desse território. Adicionalmente, esse residente, ainda seria capaz de ter acesso a informações desindexadas no território francês durante uma estadia em outro país da UE, consultando uma extensão fora da EU do motor de pesquisa a partir de uma conexão Wi-fi ou até mesmo uma viagem fora da UE, seja qual for o tipo de conexão usada, consultando a versão local do mecanismo de pesquisa.

A CNIL ainda aduz que as zonas fronteiriças do território francês beneficiam frequentemente de dupla cobertura pela rede telefónica francesa e pela rede telefónica estrangeira, e por isso um residente francês pode escapar à medida de filtragem atribuindo um endereço IP estrangeiro, embora esteja localizado no território nacional.

Conclui dizendo que existem soluções técnicas que podem contornar a medida de filtragem proposta pela empresa, permitindo que o usuário escolha a origem geográfica de seu endereço IP, como no uso de uma VPN, por exemplo.

Na deliberação, a CNIL afirma que qualquer utilizador da internet localizado fora do território francês não será afetado pela medida de filtragem e poderá continuar a ter acesso às informações não indexadas, caso consulte as extensões não europeias do motor de pesquisa, ou seja consultar o Google em versão não francesa (.fr), em qualquer país da EU ou qualquer versão do mesmo, se estiver localizado fora da UE.

Porém, para a CNIL, a proteção de um direito fundamental não pode variar de acordo com o destinatário dos dados. O direito europeu, tal como o direito francês, prevê que o titular dos dados pode exercer o seu direito a um processamento de dados, sem as possíveis diferenças de impacto dos destinatários, afirmando, assim, que a solução proposta pela empresa permanece incompleta.

Como punição a CNIL impôs ao Google uma sanção pecuniária no valor de 100.000 (cem mil) euros e a obrigatoriedade da deliberação se tornar pública.

Após todo esse prejuízo, o Google então recorreu ao Conselho de Estado Francês, que reenviou prejudicialmente no 21 de agosto de 2017 ao TJUE dando início ao processo Google Inc./Commission nationale de l'informatique et des libertés (CNIL), Processo C-507/17.

O processo reenviado pelo Conselho de Estado, o Supremo Tribunal francês, colocando o Google Inc. como recorrente e a CNIL, além dos interessados que são Wikimedia Foundation Inc., Fondation pour la liberté de la presse, Microsoft Corp., Reporters Committee for Freedom of the Press e o., Article 19 e o., Internet Freedom Foundation e o., Défenseur des droits, foi apresentado três questões prejudiciais para o TJUE responder, que são:

> "1.º Deve o "direito à supressão de uma hiperligação", como consagrado pelo Tribunal de Justiça da União Europeia no seu acórdão de 13 de maio de 2014[177], com fundamento nas disposições dos artigos 12.º, alínea b), e 14.º, alínea a), da diretiva de 24 de outubro de 1995[178], ser interpretado no sentido de que o operador de um motor de busca é obrigado, quando acolhe um pedido de supressão de uma hiperligação, a efetuar essa supressão em todos os nomes de domínio do seu motor, de forma a que as ligações controvertidas deixem de ser exibidas, seja qual for o local a partir do qual é efetuada a pesquisa com base no nome do

[177] Tribunal de Justiça da União Europeia. Acordão Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González – Processo C-131/12, 13 de maio de 2014.
[178] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.

requerente, incluindo fora do âmbito de aplicação territorial da diretiva de 24 de outubro de 1995?

2.º Em caso de resposta negativa a esta primeira questão, deve o "direito à supressão de uma hiperligação", como consagrado pelo Tribunal de Justiça da União Europeia no seu acórdão supra referido, ser interpretado no sentido de que o operador de um motor de busca apenas é obrigado, quando acolhe um pedido de supressão de uma hiperligação, a suprimir as ligações controvertidas dos resultados exibidos na sequência de uma pesquisa efetuada a partir do nome do requerente no nome de domínio correspondente ao Estado onde se considere que o pedido foi efetuado ou, de forma mais genérica, nos nomes de domínio do motor de busca que correspondem às extensões nacionais desse motor para todos os Estados-Membros da União Europeia?

3.º Além disso, em complemento da obrigação invocada na segunda questão, deve o "direito à supressão de uma hiperligação", como consagrado pelo Tribunal de Justiça da União Europeia no seu acórdão supra referido, ser interpretado no sentido de que o operador de um motor de busca, quando acolhe um pedido de supressão de uma hiperligação, é obrigado, através da técnica designada "bloqueio geográfico", a partir de um endereço IP supostamente localizado no Estado de residência do beneficiário do "direito à supressão de uma hiperligação", a suprimir os resultados controvertidos das pesquisas efetuadas a partir do seu nome, ou mesmo, de forma mais genérica, a partir de um endereço IP supostamente localizado num dos Estados-Membros aos quais se aplica a diretiva de 24 de outubro de 1995, independentemente do nome de domínio utilizado pelo internauta que efetue a busca?"

Deve-se salientar que a dúvida principal, mesmo baseado ainda na antiga Diretiva 95/46, que era vigente a época do reenvio, trata da Secção V, nomeada como

“Direito de Acesso da Pessoa em Causa aos Dados” e da Secção VII, “Direito De Oposição da Pessoa em Causa”.

O Primeiro questionamento do Supremo Tribunal Francês, baseada da histórica decisão no acórdão Google Spain, de 2014, sobre a previsão dos artigos 12.º e 14.º da Diretiva 95/46:

> Artigo 12.º
>
> Direito de acesso
>
> Os Estados-Membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento:
>
> b) Consoante o caso, a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente diretiva, nomeadamente devido ao carácter incompleto ou inexato desses dados;
>
> Artigo 14.º
>
> 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 7.º, 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 objeto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efetuado pelo responsável deixa de poder incidir sobre esses dados;

O Supremo Tribunal Francês indaga qual a abrangência que a decisão pode atingir, pedindo uma resposta do TJUE se o motor de pesquisa, no caso o Google, deve desindexar a informação pedida pelo usuário apenas do domínio francês (.fr), ou se o

mesmo deve retirar de todos os seus domínios, fazendo uma desindexação global, aplicando a diretiva fora do território da UE, pelo facto de pessoas que estariam fora da França ou da UE ainda poderiam ter aceso às informações desindexadas em seu país de origem.

O segundo reparo parte de uma possível contrariedade para a aplicação global da diretiva. A dúvida está em se o motor de pesquisa deverá retirar apenas do domínio francês ou se deverá desindexar a informação solicitada de todos os motores de pesquisas nos Estados-Membros.

Com essa localização identificada automaticamente pelo motor de pesquisa, o Supremo Tribunal Francês indaga a possibilidade de obrigar a desindexação para qualquer IP registado em Estados-Membros, através dessa tecnologia, mesmo que esteja buscando as informações em domínios de fora da UE.

Catarina Santos Botelho afirma que, neste momento, continua pendente no TJUE um reenvio prejudicial do Conselho de Estado Francês acerca da legitimidade de a Autoridade de Proteção de Dados francesa impor ao Google o apagamento em âmbito internacional de "links" dos seus motores de pesquisa. O que, neste cenário, se pretende é uma desindexação ao nível global e não somente ao nível da localização geográfica europeia, que no processo é o "google.fr". Como já era esperado, segundo a autora, a decisão deste reenvio é aguardada com bastante expetativa.[179]

Mesmo que a Diretiva 95/46 fora revogada pelo Regulamento (UE) 2016/679, o reenvio prejudicial do Conselho de Estado Francês continua válido, pois o Regulamento, que está em vigência, tem redação prevendo a aplicação em tratamentos de dados transfronteiriço, previsto no 3.º (2) e (3), além do 4.º (23) do Regulamento, trazendo ainda as mesmas dúvidas do reenvio prejudicial.

Para Graça Canto Moniz O artigo 3.º, n.º 1, do RGPD mantém o princípio de que o regime da UE de proteção de dados pessoais é aplicável se os dados pessoais são tratados no contexto das atividades de um estabelecimento de um responsável pelo tratamento no território da União. A novidade é que esta regra é alargada a subcontratantes. Na prática, isto significa que os subcontratantes passam a estar

[179] Botelho, Catarina Santos. Novo ou velho direito? – O Direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global. AB INSTANTIA, 5(7), 49-71, 2017.

diretamente vinculados pelo RGPD e pelas obrigações aí previstas, como a do artigo 30.º, n. º 2 (registo das atividades de tratamento), do artigo 31.º (cooperação com a autoridade de controlo), do artigo 32.º (segurança do tratamento), do artigo 33.º, n.º 2 (notificação de violação de dados pessoais), do artigo 37.º (designação do encarregado de proteção de dados) e do artigo 44.º (transferência de dados pessoais para países terceiros ou organizações internacionais).[180]

O RGPD acrescenta que quando o responsável pelo tratamento ou aos subcontratantes está estabelecido na UE e o tratamento se encontra no contexto das atividades desse estabelecimento, não é relevante se o "processamento propriamente dito ocorrer na UE". Isso visa esclarecer que não é necessário que o próprio estabelecimento participe do processamento, como foi o caso do Google Espanha.[181]

Com efeito o artigo 3.º do RGPD pressupõe que o responsável pelo tratamento tem uma ligação substancial à UE, seja porque ali tem um estabelecimento seja porque trata os dados pessoais de titulares de dados aí localizados e as suas atividades são direcionadas para os mesmos ou, melhor dizendo, para o mercado da UE, para os seus consumidores ou para a "comunidade comercial da UE.[182]

Para Moniz, o novo âmbito de aplicação do RGPD é reduzido quando comparado com o artigo 4.º, número 1, alínea a da Diretiva 95/46. Pode-se argumentar que o responsável pelo tratamento de dados estabelecido em um terceiro país sempre terá uma forte conexão com a UE, no sentido de processar dados pessoais de pessoas ali localizadas e suas atividades direcionadas ao mercado da UE, seus consumidores ou, em geral, e apresentam uma forte defesa do artigo 3.º baseado na ideia de que os operadores estrangeiros não serão surpreendidos pelo Direito da União desde estes só serão alvo de legislação da UE se visarem a UE.[183]

O aspeto relevante não é o local de estabelecimento do responsável pelo tratamento dos dados, mas a localização física da pessoa em causa na UE, seja domiciliada, residente ou viajando temporariamente, seja qual for a sua nacionalidade. Isto está de acordo com o objetivo da antiga diretiva e do RGPD de assegurar a proteção

[180] Moniz, Graça Canto. Página 126.
[181] Moniz, Graça Canto. Página 126.
[182] Moniz, Graça Canto. Páginas 127 – 128.
[183] Moniz, Graça Canto. Página 128.

de todas as pessoas singulares, independentemente da sua nacionalidade ou local de residência, de acordo com os considerandos 2 e 14.[184]

No dia 10 de janeiro foi publicado a conclusão do Advogado-Geral, Sr. Maciej Szpunar, sobre esse processo. Em nota oficial do TJUE ressaltou que:

> "As conclusões do advogado-geral não vinculam o Tribunal de Justiça. A missão dos advogados-gerais consiste em propor ao Tribunal de Justiça, com toda a independência, uma solução jurídica nos processos que lhes são atribuídos. Os juízes do Tribunal de Justiça iniciam agora a sua deliberação no presente processo. O acórdão será proferido em data posterior."[185]

O Advogado-Geral ressalvou alguns aspetos importantes durante a sua conclusão. Em resposta à primeira pergunta feita ao TJUE, o Sr. Maciej Szpunar entendeu que no Caso Google Spain o Google não determinou o limite geográfico da implementação de uma desindexação, e que o Tribunal rejeitou o argumento apresentado pela Google Spain e pelo Google Inc. segundo o qual o tratamento dos dados pessoais em questão não era efetuado "no âmbito das atividades" do Google Spain, mas exclusivamente pelo Google Inc. Complementou ainda, que o Tribunal esclareceu que o objetivo da Diretiva 95/46 é o de assegurar uma proteção efetiva e integral dos direitos e liberdades fundamentais das pessoas, nomeadamente o direito à privacidade, no que diz respeito ao tratamento de dados pessoais e que a expressão "no contexto das atividades" não pode ser interpretada restritivamente.[186]

Para o Advogado-Geral, ao mencionar apenas "a lista dos resultados apresentados na sequência de uma pesquisa realizada com base no nome de uma pessoa", o Tribunal não especificou o enquadramento em que esta pesquisa foi realizada, por quem e qual a localização geográfica. Na sua opinião a desindexação é necessária dependendo do local a partir do qual a pesquisa é conduzida. Pedidos de pesquisa feitos fora do território da UE não devem sofrer desindexação dos resultados da pesquisa.

[184] Moniz, Graça Canto. Página 126.
[185] Tribunal de Justiça da União Europeia. **Comunicado de Imprensa n.º 2/19**. Luxemburgo,10 de janeiro de 2019. Disponível em <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002pt.pdf>
[186] Tribunal de Justiça da União Europeia. Caso C-136/17 - Conclusions De L'avocat Général M. Maciej Szpunar, de 10 de janeiro de 2019.

Para o Sr. Szpunar o principal argumento contra uma obrigação mundial de desindexação é o balanço entre os direitos fundamentais e as lições relevantes no Google Spain e Google. Neste caso, o Tribunal atribuiu grande importância ao equilíbrio entre o direito à proteção de dados e a privacidade, com o interesse legítimo do público em obter acesso às informações solicitadas.

O Advogado-Geral afirma que o público-alvo não é um público global, mas está dentro do âmbito da Carta e, portanto, público europeu. E complementa que caso se admitisse o encerramento em todo o mundo, as autoridades da UE não seriam capazes de definir e determinar o direito a receber informação, e muito menos o equilíbrio com proteção dos direitos fundamentais da proteção de dados e privacidade. Este interesse público em acessar informações inevitavelmente variará de acordo com sua localização geográfica, de um terceiro estado para outro.

E como resposta à primeira questão o Advogado-Geral afirma que o artigo 8.° da Diretiva 95/46 não estava em causa no processo que deu origem ao acórdão Google Espanha e Google. Esta simples afirmação leva-me a supor que, contrariamente ao que a Google sugere nas suas observações, a resposta à primeira questão não pode ser deduzida desse acórdão. O facto de não se tratar de dados sensíveis, referidos no artigo 8.°, n.º 1, da Diretiva 95/46, não significa que um motor de busca não esteja sujeito a esta disposição.

A Directiva 95/46, de 1995, afirmou o Advogado-Geral, cujas obrigações são em princípio dirigidas aos Estados-Membros, não tinham sido elaborados tendo em mente os motores de pesquisa na sua forma actual, as suas disposições não se prestam a uma forma intuitiva e intuitiva. aplicação puramente literal a esses mecanismos de busca. Foi precisamente por esse motivo que, tal como no presente processo, o órgão jurisdicional de reenvio teve dúvidas no processo que deu origem ao acórdão Google Espanha e Google e submeteu a questão ao Tribunal de Justiça.

Por conseguinte, expôs o Sr. Szpunar, é impossível adotar uma abordagem «tudo ou nada» à aplicabilidade das disposições da Diretiva 95/46 aos motores de busca. Na minha opinião, é necessário examinar cada disposição do ponto de vista de saber se ela pode ser aplicada a um mecanismo de pesquisa.

Uma aplicação literal do artigo 8. °, n.° 1, da Directiva 95/46 exigiria que um motor de busca verifique que uma lista de resultados apresentados na sequência de uma pesquisa efectuada com base no nome de uma pessoa singular não contém qualquer ligação com páginas da Internet que incluam dados abrangidos por essa disposição e que o façam *ex ante* e de forma sistemática, ou seja, mesmo na ausência de um pedido de retirada de referência de uma pessoa em causa e para o advogado um controle sistemático *ex ante* não é possível nem desejável.

O Advogado-Geral terminou assegurando que no acórdão Google Spain e Google, o Tribunal de Justiça observou que na medida em que a actividade de um motor de pesquisa é susceptível de afectar de forma significativa, e adicionalmente comparada com a dos editores de sites, os direitos fundamentais à privacidade e a proteção dos dados pessoais, o operador do motor de pesquisa, enquanto pessoa que determina os fins e os meios dessa actividade, deve assegurar, no âmbito das suas competências, poderes e capacidades, que a actividade satisfaz os requisitos da Diretiva 95/46, a fim de: que as garantias previstas pela diretiva podem ter pleno efeito e que a protecção efectiva e completa dos titulares de dados, em particular do seu direito à privacidade, pode efectivamente ser alcançada.

O Sr. Maciej Szpunar trata da segunda e terceira questões de forma conjunta. Ele incide sobre o sistema de geobloqueio, onde a localização do utilizador é determinada usando técnicas de geolocalização, como a verificação do endereço IP. O bloqueio geográfico, que constitui uma forma de censura, é considerado injustificado no direito do mercado interno da UE, onde é objeto de um regulamento que visa impedir os profissionais que exercem as suas atividades num Estado-Membro. Um Estado-Membro pode bloquear ou restringir o acesso de utilizadores de outros Estados-Membros que pretendam transacionar informação na internet.

Para o Advogado-Geral, uma vez estabelecido o direito de retirada dos mecanismos de pesquisa, cabe ao operador do motor de pesquisa tomar qualquer medida à sua disposição para garantir uma desindexação, eficiente e completa. Este operador deve executar todas as etapas tecnicamente possíveis. No que diz respeito ao processo principal, isso inclui, em especial, a técnica denominada "geobloqueio", independentemente do nome de domínio utilizado pelo utilizador que realiza a pesquisa,

ressaltando ainda que uma desindexação deve ser feita não a nível nacional, mas a nível da UE.

A nível da UE, pois segundo ele, a Diretiva 95/46 procura estabelecer um sistema global de proteção de dados que transcenda as fronteiras nacionais. Com base no antigo artigo 100.º-A do TFUE, faz parte de uma lógica do mercado interno que inclui, há que recordar, um espaço sem fronteiras internas. Daqui decorre que uma desindexação a nível nacional seria contrária a esse objetivo de harmonização e à eficácia das disposições da Diretiva 95/46.

Em conclusão, o Advogado-Geral propõe que o operador do sistema de pesquisa seja obrigado a suprimir as ligações controvertidas dos resultados apresentados na sequência de uma pesquisa realizada com base no nome do recorrente efetuada em um motor de pesquisa na UE. Neste contexto, este operador é obrigado a tomar qualquer medida à sua disposição para garantir uma desindexação eficiente e completa. Isto inclui, em particular, a chamada técnica de "geobloqueio", a partir de um endereço IP conhecido, localizado num dos Estados-Membros abrangidos pela Diretiva 95/46, independentemente do nome de domínio utilizado pelo utilizador e de quem faz a pesquisa.

Para o Advogado-Geral, os motores de busca devem aplicar a desindexação em pedidos feitos nos Estados-Membros por toda o território da UE, isentando os mesmo de bloquearem em todos os domínios, ou seja, para ele não pode existir uma desindexação a nível global.

Como foi dito na nota oficial, o TJUE não é obrigado a seguir a posição do Advogado-Geral, e a apreciação do caso pelos juízes do Tribunal iniciou-se no dia 10 de janeiro de 2019 e até a conclusão desse trabalho não foi publicada a decisão oficial do Tribunal.[187]

A CNIL declarou que quando um cidadão da UE solicita que o Google remova suas informações do mecanismo de pesquisa, o Google deve "desindexar" todas as extensões do domínio de pesquisa. Como resultado, quando algum individuo pede para que um link seja excluído, o Google agora bloqueia o acesso a links "de todos os seus

[187] Tribunal de Justiça da União Europeia. O advogado-geral M. Szpunar propõe ao Tribunal de Justiça que limite à escala da União Europeia a supressão de hiperligações a que os operadores de motores de busca são obrigados a proceder, de 10 de janeiro de 2019.

domínios" em todo o mundo ", incluindo o principal dos EUA, Google.com" e não apenas o domínio do país onde reside o cidadão europeu. o direito a ser esquecido é um direito humano fundamental para todos os cidadãos da UE, pelo que qualquer empresa, seja dentro ou fora da UE, que processe as informações pessoais dos cidadãos da UE é obrigada a ter capacidade tecnológica para cumprir este direito a um pedido individual de eliminação.[188]

É importante reconhecer que o RGPD se aplica ao processamento de dados pessoais de titulares de dados "que estão na UE", significando que o titular dos dados não precisa necessariamente de ser cidadão ou residente de um país da UE para recorrer à proteção do RGPD. Em vez disso, a pessoa em causa só precisa de estar "na UE", mesmo que a sua presença na UE seja temporária.[189]

De acordo com as Diretrizes do GT Art. 29.º a CNIL, autoridade francesa de proteção de dados, ordenou que o Google aplique o direito de ser esquecido em todos os nomes de domínio do mecanismo de busca do Google, incluindo o domínio ".com ". Como muitas outras autoridades nacionais de proteção de dados na Europa, a CNIL supervisiona a aplicação da sentença do TJUE sobre o direito a ser esquecido em caso de recusa dos mecanismos de busca em realizar a retirada solicitada. Em resposta a centenas de reclamações individuais desde a decisão do caso Google Espanha, a CNIL solicitou que ao Google excluísse os resultados da pesquisa em várias ocasiões. Em todas essas instâncias, a CNIL solicitou expressamente que a desindexação tivesse que ser eficaz em todo o mecanismo de pesquisa, independentemente da extensão de domínio por meio da qual os utilizadores acedam às informações. No entanto, inicialmente, o Google aplicou o fechamento de lista apenas às extensões europeias de seu mecanismo de pesquisa. O direito de ser esquecido por infringir os resultados da pesquisa permaneceu acessível em território francês a partir do Google.com e de outras extensões não europeias.[190]

A solução proposta pelo Google foi a geolocalização. O Google estendeu a remoção dos URLs para qualquer versão baseada no domínio de seu mecanismo de pesquisa, sendo assim a partir de pesquisas baseadas em termos que o um Estado-Membro aceitou a solicitação de desindexação, não apareceria mais em nenhum domínio do

[188] Kuhn, McKenzie L.. 147 Million Social Security Numbers for Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches. Iowa Law Review, Volume 104, 433 - 434, 2018.
[189] Shapiro-Barr, Jeremy. The GDPR's Impact in the U.S.: Considerations for the U.S. Health Lawyer. Journal of Health & Life Sciences Law, Vol.12 (No. 1), pág. 40, 2018.
[190] Frosio, Giancarlo F.. Página 330.

mecanismo de busca. Se um residente francês solicitar ao Google que remova um resultado de pesquisa em consultas para o nome dele, o link não estará visível em nenhuma versão do site do Google, incluindo o Google.com, quando o mecanismo de pesquisa for acedido a partir da França. O Google usará o endereço IP do navegador para determinar sua localização. No entanto, a CNIL considerou esse desenvolvimento insuficiente para proteger os direitos dos usuários franceses. Ao impor uma multa de 100.000 euros ao Google, o Comitê restrito da CNIL observou que:

> "O direito de exclusão é derivado do direito à privacidade, que é um direito fundamental universalmente reconhecido no direito internacional dos direitos humanos. Apenas a exclusão de todas as extensões do mecanismo de pesquisa, independentemente da extensão usada ou da origem geográfica da pessoa que realiza a pesquisa, pode efetivamente garantir esse direito. A solução que consiste em variar o respeito pelos direitos das pessoas com base na origem geográfica daqueles que veem os resultados da pesquisa não oferece às pessoas uma proteção efetiva e completa do direito de serem retiradas da lista."[191]

Em matéria de extraterritorialidade, a CNIL observou especificamente que "esta decisão não mostra qualquer disposição por parte da CNIL em aplicar a lei francesa de maneira extraterritorial. Ela simplesmente solicita a total observância da legislação europeia por parte de atores não europeus que oferecem seus serviços na Europa".[192] Alguns pontos podem ser úteis para esclarecer essa posição. Não há país, além da França, onde a lei francesa deva ser aplicada. Existem domínios da Internet nos quais a lei francesa se aplicaria, como argumenta o Google: "em última análise, poderemos ter de implementar os padrões franceses nos sites de pesquisa do Google da Austrália (google.com.au) para a Zâmbia (google.co.zm) e em todos os lugares entre.".[193]

A desconexão está na perceção equivocada da natureza da internet. Os domínios digitais são apenas mundos fictícios não sancionados pelas regras internacionais que

[191] Commission Nationale de l'Informatique et des Libertés. Decision No. 2016-054 - Restricted Committee issuing Google Inc. with a financial penalty, de 10 de março de 2016.
[192] CNIL. Right to Delisting: Google Informal Appeal Rejected, de 21 de setembro de 2015, disponível em <https://www.cnil.fr/fr/node/15814>.
[193] Frosio, Giancarlo F.. Página 330.

definem a soberania nacional. O sistema de soberania da Vestefália dificilmente pode ser esticado para alcançar a internet.[194] O Google.com.au não é a Austrália, google.co.zm não é a Zâmbia, e os países ao redor do mundo estão pouco inclinados a lidar com o google.com sendo um protetorado dos EUA. Como a internet ainda não foi particionada em territórios digitais sob a jurisdição de um país específico, não há motivos para pensar que as regras francesas não devam ser aplicadas a titulares de dados franceses quando estiverem em roaming em qualquer domínio digital que não seja google.fr ou google.eu.[195]

No que diz respeito a um nível de proteção essencialmente equivalente aos direitos e liberdades fundamentais garantidos na UE, o Tribunal considerou que a legislação não se limita ao estritamente necessário, ou seja, não cumpre o teste intrínseco da proporcionalidade do direito da UE. O Tribunal chegou a esta conclusão porque a legislação dos EUA permite, de forma generalizada, o armazenamento de todos os dados pessoais de todas as pessoas cujos dados são transferidos da UE para os EUA sem qualquer diferenciação, limitação ou exceção, sem estabelecer um critério objetivo para determinar os limites do acesso das autoridades públicas aos dados e à sua utilização subsequente. Além disso, o Tribunal observou que a legislação que não prevê qualquer possibilidade de um indivíduo procurar recursos legais para ter acesso a dados pessoais relativos a ela, ou para obter a retificação ou a eliminação de tais dados, compromete a essência do direito fundamental de proteção judicial efetiva. Por todas essas razões, o Tribunal declarou inválida a decisão do "Porto Seguro".[196]

Como resultado, haveria maior proteção para os indivíduos e o direito poderia garantir um esquema regulatório mais eficaz. Na realidade, porém, é possível pedir a uma empresa que apague informações tornadas públicas por um indivíduo, tendo em vista o facto de já ter sido amplamente distribuído? Quando o Sr. Schrems entrou em litigio contra o Facebook, ele solicitou todos os documentos que a empresa possuía sobre ele., e recebeu um registro de cada pedaço de informação que mencionava o seu nome, se ele

[194] Demchak, Chris; Dombrowski, Peter. Cyber Westphalia: Asserting State Prerogatives in Cyberspace. Georgetown Journal of International Affairs, p. 33, 2013.
[195] Frosio, Giancarlo F.. Página 332.
[196] Burri, Mira; Schär, Rahel. Página 487.

ainda estava na página de Internet ou supostamente excluído há muito tempo, em uma enorme pilha de documentos.[197]

Essa ocorrência simboliza o facto de que, embora o RGPD possa convencer as empresas a remover informações das suas páginas de internet, que os clientes solicitam que sejam retiradas, elas nunca poderão realmente desaparecer. Na luta para imortalizar o direito à privacidade e torná-lo tangível, os defensores da privacidade tiraram uma foto dessa pilha de papéis na medida em que Sr. Schrems brincou sobre isso e disse: "É provavelmente a pilha de papéis mais filmada de todos os tempos!". Esse enorme interesse na pilha de papéis do Sr. Schrems é a tentativa europeia e americana de tornar palpável esse direito ilusório de privacidade. Na realidade, não está claro qual a privacidade que o direito a ser esquecido oferece.[198]

A ideia de que a aplicação extraterritorial do direito a ser esquecido pode desencadear um "*kraken*" que pode quebrar a internet deve ser contextualizada dentro do atual cenário político. A aplicação extraterritorial do direito a ser esquecido segue os passos de um movimento global em direção ao protecionismo de dados contra a dominação de facto dos conglomerados norte-americanos da internet.[199]

O Google pode reforçar esses medos, como argumenta contra a decisão da CNIL, apresentando argumentos como "qualquer precedente desse tipo (de ter que implementar padrões franceses em qualquer lugar) abriria as portas para países em todo o mundo, incluindo países não democráticos" exigir a mesma potência global.[200] As empresas que operam a internet devem servir como guardiões dos direitos dos cidadãos do mundo online de acordo com as leis e valores do país onde essas empresas estão incorporadas.[201]

Se as empresas não conseguem lidar com as leis e valores de uma determinada jurisdição, elas têm sempre a opção de não operar nessa jurisdição. Se as preocupações mundiais não forem tratadas adequadamente, poderemos testemunhar um futuro de segregação da informação e desintegração da rede. No longo prazo, a harmonização dos

[197] The City University of New York. Maximilian Schrems, Initiator of Europe v. Facebook. The US v. Europe v. Facebook: Digital Divisions?. New York, 2016.
[198] Safari, Beata A.. Páginas 835 – 836.
[199] Tribunal de Justiça da União Europeia. Acórdão C-362/14 - Maximillian Schrems contra Data Protection Commissioner, de 06 de outubro de 2015.
[200] Fleischer, Peter. Reflecting on the Right to be Forgotten. Google Blog. Disponível em <https://blog.google/topics/google-europe/reflecting-right-be-forgotten>.
[201] Frosio, Giancarlo F.. Página 336.

direitos dos utilizadores globalmente, por meio de consenso multilateral e internacional, deve ser o objetivo perseguido.[202]

O RGPD obriga todos os operadores presentes na internet ao cumprimento das normas de proteção de dados pessoais quer situados dentro quer fora do espaço europeu – ou seja, independentemente da localização física do servidor. Assim, desde que forneçam serviços que impliquem o tratamento de dados pessoais de cidadãos europeus, ficam sujeitos às normas europeias – eis a aplicação extraterritorial a empresas que operem na UE mas nela não tenham estabelecimento, conforme o artigo 3.º do RGPD.[203]

Assim sendo, a norma que consagra o direito ao esquecimento (direito à desindexação), tal como outras, valerá para esses operadores e determinará que o RGPD possa ser invocado perante eles. Tal significa que mesmo os operadores de maior dimensão com sede fora da Europa, que trabalham com volumosas quantidades de dados pessoais de cidadãos europeus, passam a estar sujeitos às normas europeias, designadamente em matéria de direito ao esquecimento.[204] Nesta medida, o TJUE deveria decidir no caso da CNIL, conforme o RGPD e sua própria jurisprudência, a favor de uma desindexação de forma global, trazendo segurança e privacidade ao titular dos dados em relação à desindexação de informações dos grandes motores de busca.

[202] Frosio, Giancarlo F.. Página 336.
[203] Castro, Caratina Sarmento e. Páginas 1066 - 1067.
[204] Castro, Caratina Sarmento e. Página 1067

3. A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO

No panorama do ordenamento jurídico brasileiro, segundo Danilo Doneda, a figura da proteção de dados como um direito autónomo e fundamental não deriva de uma diretriz explícita e literal, mas sim da apreciação dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, em conjunto com a proteção da intimidade e da vida privada.[205]

No Brasil, tanto na legislação em relação a proteção de dados, quanto nos primeiros acórdãos sobre o direito ao esquecimento é possível estabelecer uma influência da Alemanha. O Tribunal Constitucional Alemão, mesmo em ter julgado a tutela dos dados pessoais contra abusos da informática como parte integrante de um direito de autodeterminação informativa, há ainda uma parte na doutrina do país que o conteúdo desse direito corresponde antes ao âmbito de tutela do direito à imagem que cada um pode querer perante os outros e perante a sociedade em geral, quem aceite a sua caracterização como um direito de autodeterminação informativo pertencente todavia ao domínio dos direitos de comunicação enquanto liberdade de pensamento, de imprensa e de ciência, e quem sustente até que está em causa um verdadeiro direito de natureza real, um direito de propriedade da pessoa sobre os dados de natureza informática que lhe digam respeito.[206]

Com essa influência a proteção de dados pessoais no ordenamento jurídico brasileiro não se estrutura a partir de um complexo normativo unitário. A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão, previsto no artigo art. 5.º, IX e no art. 220 da Carta Magna, e do direito à informação, conforme o art. 5.º, XIV e o art. 220 da Constituição, além do direito ao receção de informações de interesse coletivo ou particular dos órgãos públicos, previsto no art. 5.º, XXXIII, assim como o direito à obtenção de certidões de repartições públicas, descrito no art. 5.º, XXXIV, do mesmo texto, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.[207]

[205] Donega, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. Espaço Jurídico Journal of Law, v. 12(n. 2), pág. 103, 2011.
[206] Mirada, Jorge; Medeiros, Ruy. Páginas 568 - 569.
[207] Donega, Danilo. Página 103.

A Constituição considera invioláveis a vida privada e a intimidade, conforme seu art. 5.º, X, como no caso específico da intercetação de comunicações telefónicas, telegráficas ou de dados, previsto no artigo 5.º, XII, da mesma maneira que instituiu a ação de *habeas data*, redigido no art. 5.º, LXXII, que estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, do qual o artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bases de dados e registros", elaborando uma abordagem sistemática baseada nos *Fair Information Principles*[208] à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro.[209]

A Constituição Federal de 1988 consagra ainda, de forma expressa, os direitos da personalidade humana, em seu artigo 5.º, X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente da sua violação".[210]

Segundo Bittencourt e Veiga, no ordenamento jurídico brasileiro, visto de forma ampla, os direitos da personalidade podem ser classificados pela tripartição clássica dos próprios direitos fundamentais, exposto da seguinte maneira:

Em primeiro lugar a Tutela Física da Personalidade, com previsão no Código Civil nos artigos 13 a 15, sobre o direito ao corpo vivo e o direito ao corpo morto. O segundo ponto está previsto nos artigos 16 a 21 do mesmo texto, a Tutela Moral da Personalidade. Por fim, os direitos do autor e do inventor, a cargo da Tutela Intelectual da Personalidade.[211]

Segundo o Art. 21 do Código Civil, prevê que: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.".[212]

[208] Em tradução livre "Princípios Justos de Informação"
[209] Donega, Danilo. Donega, Danilo. Página 103.
[210] BRASIL. Constituição (1988). Brasília, Distrito Federal, Brasil: Senado Federal.
[211] Bittencourt, Illa Barbosa; Veiga, Ricardo Macellaro. Direito ao Esquecimento. Revista Direito Mackenzie, v.8(n.2), p. 51 - 52, 2014
[212] Bittencourt, Illa Barbosa; Veiga, Ricardo Macellaro. Página 52.

A privacidade é aquilo que as pessoas fazem no ambiente familiar, entre amigos próximos, nas atividades de lazer, ou em atividades religiosa, ou seja, é o que a pessoa faz e fala nas atividades particulares porque detém confiança.[213]

O Art. 20 do Código Civil brasileiro coloca que:

> "Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais."[214]

Deve-se entender também o conceito de intimidade, que por sua vez, é mais restrito e consiste naquilo que a pessoa tem com ela mesma, que não tem obrigação de exteriorizar ou compartilhar no seu ambiente familiar ou privado ou com os seus.[215]

Esses dois conceitos estão espelhados nos artigos 20 e 21 do Código Civil, onde, para fins de tutela, deverão ser compreendidos duas interpretações em relação a vida privada de cada cidadão. O *locus privado*, que tem como alicerce o princípio da inviolabilidade e a proteção plena, e em seguida o *locus público*, onde a proteção da vida privada é relativizada conforme o interesse público. Ou seja, o *locus público*, tem permissão para violar a esfera da privacidade de cada cidadão, porém os direitos em relação a esta continuam resguardados conforme seus interesses. Onde, para os autores, mesmo que a pessoa seja uma figura pública, a invasão de sua privacidade, seja por meio de fotos e/ou perseguição não podem ocorrer, a ponto de tornar a vida em sociedade dessas figuras insuportável.[216]

O direito ao esquecimento, mesmo das figuras públicas, deve existir a partir da invasão da vida privada assegurado no artigo 21 do Código Civil brasileiro, ao demonstrar um prejuízo grande para a prosseguir no quotidiano atingido.[217]

---

[213] Bittencourt, Illa Barbosa; Veiga, Ricardo Macellaro. Página 52.
[214] BRASIL. Código Civil. Brasília, Distrito Federal, Brasil, de 10 de Janeiro de 2002.
[215]Bittencourt, Illa Barbosa; Veiga, Ricardo Macellaro. Página 52.
[216] Bittencourt, Illa Barbosa; Veiga, Ricardo Macellaro. Páginas 52 - 53.
[217] Bittencourt, Illa Barbosa; Veiga, Ricardo Macellaro. Páginas 52 - 53.

Na IV Jornada de Direito Civil, que tiveram como coordenador geral do evento Ruy Rosado de Aguiar Júnior, foi aprovado o Enunciado 531, com título "A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento.", em relação ao artigo 11 do Código Civil. Como justificativa colocaram que:

> "Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-recluso à ressocialização. Não atribui a ninguém o direito de apagar factos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos factos pretéritos, mais especificamente o modo e a finalidade com que são lembrados".[218]

Com as constantes evoluções tecnológicas, segundo Poliana Bozégia Moreira, a internet, trouxe uma capacidade de armazenamento ilimitada, fazendo com que as informações fiquem disponíveis quase infinitamente. Até certo ponto este aspeto é positivo, no sentido em que a internet é uma fonte inesgotável de conhecimento, mas que, no entanto, quando colide com os direitos fundamentais à privacidade e intimidade, pode tornar-se um grande problema para os indivíduos envolvidos.[219]

Para se divulgar um conteúdo na internet não é preciso revelar sua identidade, há uma grande facilidade de circulação e de manutenção de informações. A qualquer momento estão disponíveis, mesmo depois de decorrido um grande lapso temporal. É factual que qualquer informação pode ser publicada sem nenhum crivo sobre sua veracidade.[220]

[218] Justiça Federal. Enunciados Aprovados na VI Jornada de Direito Civil. 2017. Disponível em <http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/enunciados-vi-jornada/view>.
[219] Moreira, Poliana Bozégia. Direito ao Esquecimento. Revista de Direito da Universidade Federal de Viçosa, Vol. 7(nº 2), p. 296, 2015.
[220] Moreira, Poliana Bozégia. Páginas 296 – 297.

Em razão disso, o instituto do direito ao esquecimento, já abrangido no âmbito da proteção constitucional da privacidade, vem ganhando importância, ressurgindo como uma das principais discussões no campo do direito digital.[221]

Na opinião de Alexandre Veronese e Noemy Melo a primeira fonte da proteção de dados no Brasil está relacionada com as informações pessoais armazenadas em sistemas de registros estatais, regulamentado através da Lei n.º 8.159, de 8 de janeiro de 1991. Segundo os autores trata-se de legislação antiga e que ainda está em vigor.[222]

Hoje a discussão da proteção de dados no Brasil, passa por entender que o problema advém das capacidades tecnológicas associados ao uso da internet. Para o autor João Carlos Zanon, o direito ao esquecimento é definido como:

> "A proteção de dados pessoas resguarda a pessoa de não ser discriminada pelas suas crenças religiosas, suas opiniões políticas e filosóficas, por sua etnia, condições de saúde ou orientação sexual; proteger os dados pessoais significa, também, evitar que o indivíduo seja impedido de acessar bens e serviços, a princípio só oferecidos àqueles com boas credenciais; conferir proteção aos dados pessoais implica, ainda, livrar-se de etiquetas e chancelas. Portanto, com a proteção aos dados pessoais, busca-se, sobretudo, a não discriminação, a não exclusão e a promoção da liberdade. [...] Tutela o livre desenvolvimento da personalidade e a dignidade humana"[223]

A proteção de dados interconecta-se com o direito de imagem e com a liberdade de expressão, assegurando esses direitos na esfera da internet, ao contrário do que se concretizou na Europa, sendo aplicado a proteção de qualquer dado que possa identificar uma pessoa, seja ela natural ou jurídica.[224]

A compreensão da relevância jurídica da internet, segundo Dias e Bolesina, não é uma questão temporal, mas sim material. Ou seja, embora a compreensão jurídica da Internet dê seus primeiros passos, mais ou menos, a partir de 1996, ela é somente

[221] Moreira, Poliana Bozégia. Página 297.
[222] Veronese, Alexandre; Melo, Noemy. O Projeto de Lei 5.276/2016 em contraste com o novo regulamento Europeu (2016/679 UE). Revista de Direito Civil Contemporâneo, Vol. 14, p. 75, 2018.
[223] Zanon, João Carlos. Direito à proteção dos dados pessoais. Revista dos Tribunais, p.151, 2013.
[224] Idem

considerada, passando a integrar habitualmente os debates jurídicos, após mais de uma década. Por um lado, a compreensão jurídica da internet introduzir-se como factor hermenêutico, isso é, como um artefacto que deve ser avaliado na interpretação do Direito, que já fora reconhecido. Por outro lado, a compreensão jurídica da internet aparece como elemento na elaboração de novas legislações, especialmente a partir de 2010, as quais, ironicamente, foram e são chamadas de vanguardistas.[225]

As legislações criadas no Brasil até então regulam parcialmente a temática da proteção dos dados pessoais, porém, nenhuma o faz de modo contundente e específico. A pretensão protetiva aparece mais como um dever acessório ou um anexo legislativo do que como o objetivo central, seguindo com a cultura pós-violatória e punitiva brasileira.[226]

Assim, todas essas legislações, principalmente a Constituição Federal e o Código Civil, são bastante elementares no assunto. A grande questão é que ao passo que a Europa se dedica diretamente ao tema há mais de cinco décadas; os EUA, ao seu modo, há quase duas décadas, alguns países sul-americanos, como Uruguai e Argentina, há cerca de uma década lidam com a proteção de dados pessoais, o Brasil conta com tímidos avanços indiretos. O tema da proteção de dados pessoais nunca contou com força suficiente para se inserir diretamente na agenda política brasileira.[227]

O cenário brasileiro, porém, obteve uma significativa mudança ao aprovar no dia 14 de agosto de 2018, a Lei n.º 13.709, batizada como a Lei Geral de Proteção de Dados Pessoais.

O anteprojeto dessa lei foi articulado no âmbito da plataforma virtual "Pensando o Direito", em paralelo com outras legislações como o próprio Marco Civil da Internet e o Estatuto da Juventude, por exemplo, na qual estava aberto a todos o debate e a submissão de contribuições e críticas ao texto originalmente proposto.

Tecnicamente, a proposta começou a ser pensada ainda em 2005, tendo o debate público nascido em 2010 e se intensificado no ano de 2015. Em julho de 2015, o tempo

[225] Dias, Felipe da Veiga; Bolesina, Iuri. Direito à Proteção de Dados Pessoais no Brasil e os Traços Centrais de uma Autoridade Local de Proteção. E-Civitas - Revista Científica do Curso de Direito do UNIBH, Volume X (número 1), p.4, 2017.
[226] Dias, Felipe da Veiga; Bolesina, Iuri. Página 6.
[227] Dias, Felipe da Veiga; Bolesina, Iuri. Páginas 6 - 7.

de contribuições foi encerrado, e na sequência, o anteprojeto foi remetido e submetido ao legislativo federal, passando a tramitar sob o "Projeto de Lei n. 5.276/2016".

João Carlos Zanon escreveu sobre o projeto:

> "Afora os trabalhos legislativos em curso no Congresso nacional, vem sendo preparado pelo Ministério da Justiça (MJ), em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas do Rio de Janeiro (CTS/FGV-Rio), um anteprojeto de lei de proteção de dados pessoais. O texto preliminar começou a ser formulado em 2005 [...]".[228]

A plataforma virtual "Pensando Direito" esclareceu que:

> "O Anteprojeto de Lei de Proteção de Dados Pessoais foi elaborado pela Senacon, em conjunto com a Secretaria de Assuntos Legislativos do Ministério da Justiça, após a realização de dois debates públicos, realizados via internet. O primeiro em 2010 e o segundo no primeiro semestre de 2015. No total foram mais de 2.000 contribuições dos setores público e privado, academia e organizações não-governamentais. Durante os últimos cinco anos também foram realizadas inúmeras reuniões técnicas, seminários e discussões por diversos órgãos e entidades".[229]

Na justificativa do Projeto de Lei 5.276/16 é discutido que:

> "A proposta visa assegurar ao cidadão o controle e a titularidade sobre suas informações pessoais, com fundamento na inviolabilidade da intimidade e da vida privada, na liberdade de expressão, comunicação e opinião, na autodeterminação informativa, no desenvolvimento econômico e tecnológico, bem como na livre iniciativa, livre concorrência e defesa do consumidor. O avanço da tecnologia da informação amplia

[228] Zanon, João Carlos. Direito à proteção dos dados pessoais. Revista dos Tribunais, p. 174, 2013.
[229] O Direito Pensando. Conheça a nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais. Disponível em <http://www.pensando.mj.gov.br/>

> enormemente o potencial de coleta, processamento e utilização de dados pessoais, o que representa, por um lado, uma oportunidade de geração de novos conhecimentos e serviços, mas, por outro, pode acarretar graves riscos aos direitos da personalidade do cidadão, ao acesso a serviços e bens [...]".[230]

O texto do Anteprojeto de Lei de Proteção de Dados pessoais foi, originalmente, apresentado ao Congresso Nacional abrangendo o objetivo de proteção de dados pessoais. A denominação de "Projeto de Lei n. 5.276/2016" declara em seu preâmbulo que "dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural".[231]

O desafio do Brasil era aprovar essa legislação que deveria ser aplicável tanto à esfera pública quando para às relações privadas. Mesmo essa lei tendo sido aprovada, o Brasil está atrasado na regulamentação da proteção de dados pessoais em comparação a outros ordenamentos jurídicos, como o Regulamento (UE) 2016/679 na UE, e as leis dos países vizinhos, como o Chile, Lei 19.628/1999 e a Argentina através da Lei 25.326/2000.[232]

A lei está estruturada em 56 artigos, dispostos em nove capítulos, sendo eles: 1) das disposições preliminares; 2) dos requisitos para o tratamento de dados pessoais; 3) dos direitos do titular; 4) do tratamento de dados pessoais pelo poder público; 5) da transferência internacional de dados; 6) dos agentes de tratamentos de dados pessoais; 7) da segurança e das boas práticas; 8) da fiscalização; 9) das disposições finais e transitórias. Segundo Zanon, colocando-se em paralelo com as legislações europeias que tratam do assunto, perceber-se-á dali a sua inspiração e influência direta.[233]

Nas razões e justificações do projeto de lei de proteção de dados pessoais, seus requerentes esclarecem que o projeto como um todo, mais vincada na sua organização, suas projeções e o seu momento de implementação estão voltados para atingir não apenas a discrepância do estabelecido e a falta de uma legislação específica sobre o tema, como

[230] Aragão, Eugênio José Guilherme de; Gaetani, Francisco. Fundamentação do Projeto de Lei de Proteção de Dados Pessoais – PL 5276-2016, 2016.
[231] Dias, Felipe da Veiga; Bolesina, Iuri. Página 8.
[232] Veronese, Alexandre; Melo, Noemy. Páginas 75 - 76.
[233] Zanon, João Carlos. Direito à proteção dos dados pessoais. Revista dos Tribunais, p. 76, 2013.

também o atual desequilíbrio de poder em favor dos responsáveis pelo tratamento dos dados pessoais e em desfavor dos titulares desses dados.

Sendo assim, a proposta possui três áreas. A primeira é criar um ordenamento legislativo com previsões específicas; a segunda é incitar a elaboração de mecanismos e articulações, institucionais ou não, que ataquem e diminuam, ou eventualmente eliminem, a distância entre os responsáveis pelo tratamento de dados pessoais e os titulares dos dados pessoais; e, a terceira e última, fomentar parâmetros e meios de controle e limitação do uso dos dados pessoais. Tudo isso integrando, simultaneamente, a proteção dos direitos dos titulares e o uso lícito, de boa-fé e transparente dos tratadores de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) foi aprovada no dia 14 de agosto de 2018, dispondo sobre a proteção de dados pessoais e alterando a Lei n.º 12.965, de 23 de abril de 2014, nomeada de Marco Civil da Internet. A LGPD teve o veto presidencial em alguns pontos, sendo o principal em relação a criação da Autoridade Nacional de Proteção de Dados, que seria um órgão especial vinculado ao Ministério da Justiça. Na mensagem oficial do veto foi apenas explicado que a criação dessa autoridade era inconstitucional, conforme publicado: "Os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1.º, II, 'e', cumulado com o artigo 37, XIX da Constituição.".

Porém, o mesmo presidente, que estava em exercício na época, a três dias de terminar seu mandato editou a Medida Provisória n.º 869, de 27 de dezembro de 2018, publicado no Diário Oficial no dia 28 de dezembro de 2018, a qual criou a Autoridade Nacional de Proteção de Dados (ANPD), que passa a ser órgão da administração pública federal, integrante da Presidência da República.

No artigo 55-J da Medida prevê as funções da ANPD, que são:

> Art. 55-J. Compete à ANPD:
>
> I - zelar pela proteção dos dados pessoais; II - editar normas e procedimentos sobre a proteção de dados pessoais; III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos; IV - requisitar

informações, a qualquer momento, aos responsáveis pelo tratamento e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos responsáveis pelo tratamento; XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XVI - elaborar relatórios de gestão anuais acerca de suas atividades.

É bastante criticável que a ANPD tenha sido desenhada de forma genérica e não como uma entidade estatal nos moldes de uma agência reguladora. Segundos Veronese & Melo, existe o risco de que esse órgão seja apenas um conselho na estrutura de um Ministério, o que colocaria em potencial risco a sua necessária independência. A criação de um comitê consultivo, conforme o artigo 55-C da Medida Provisória n.º 869, tende a ser um factor criador de confusão.[234]

Um avanço que se apresentou em 2019 na legislação brasileira foi a PROPOSTA DE EMENDA À CONSTITUIÇÃO (PEC) N° 17, DE 2019[235], proposto pelo Senador Eduardo Gomes (MDB/TO) como primeiro signatário e mais 28 senadores para acrescentar o inciso X/1-A, ao art. 5.º e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

A PEC propõe um acréscimo no art. 5.º da Constituição Federal com o inciso XII-A que prevê que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais.".

A PEC ainda propõe a inclusão do inciso XXX no art. 22.º da Carta Magna, que prevê "Compete privativamente à União legislar sobre:", passando a união a legislar também sobre "XXX- proteção e tratamento de dados pessoais.".

Como justificativa os autores da PEC colocaram que:

> "…países de todo o planeta já visualizaram a importância e imprescindibilidade de se regular juridicamente o tratamento de dados dos cidadãos. É o caso dos membros da União Europeia, que, hoje, já contam com a segunda e moderna versão regulatória sobre o assunto, chamado de Regulamento Geral de Proteção de Dados. O RGPD entrou em vigor em 25 de maio de 2018, gerando um impacto de nível global, sobretudo em face de milhares de empresas que ofertam serviços ao mercado europeu".

[234] Veronese, Alexandre; Melo, Noemy. Página 91.
[235] Senado Federal. Proposta de Emenda à Constituição N° 17. Senador Eduardo Gomes (MDB/TO), de 21 de fevereiro de 2019.

O projeto da PEC buscou na nova legislação europeia inspiração para trazer a proteção já vivenciada na UE desde 1995 com as devidas atualizações para a realidade brasileira, observando que na União a proteção de dados e tudo que ela prevê é um direito fundamental do cidadão dos Estados-Membros.

Na justificativa os autores também suscitaram a autodeterminação informacional, ao colocar que “Foi o caso de Portugal: sua Constituição, adotada em 1976, assegura o direito e a garantia pessoal de utilização da informática, estabelecendo, também, normas específicas de acesso e tratamento de dados pessoais.”.

Os autores afirmam também que “além de instituir o direito fundamental à proteção de dados pessoais, também disciplinar questão tormentosa: a competência constitucional para legislar sobre o tema.”.

E concluem dizendo que “o ideal, tanto quanto se dá com outros direitos fundamentais e temas gerais relevantes, é que a União detenha a competência central legislativa. Do contrário, pode-se correr o risco de, inclusive de forma inconstitucional, haver dezenas - talvez milhares- de conceitos legais sobre o que é "dado pessoal" ou sobre quem são os "agentes de tratamento" sujeitos à norma legal.”.

Em votação no senado, ocorrida no dia 02 de julho de 2019, foi aprovada, em dois turnos como manda o rito da PEC, com 64 votos favoráveis no primeiro turno e 62 no segundo. Nenhum senador votou contra o texto.

O projeto ainda será votado na Câmara do Deputados e aprovada em dois turnos com o mínimo de três quintos dos votos dos membros da casa, ou seja, 308 deputados para posteriormente estar presente na Constituição Federal. Porém esse projeto mostra que o Brasil, inspirado na autodeterminação informacional juntamente com o Regulamento Geral de Proteção de Dados da União Europeia, propôs projeto a sua Constituição para assegurar como direito fundamental a todo cidadão brasileiro a Proteção de Dados, trazendo uma segurança semelhante ao que existe hoje na União Europeia.

3.1. Caso “Massacre da Candelária”

O Caso do Massacre da Candelária é o primeiro processo que chegou ao Superior Tribunal de Justiça sobre o direito ao esquecimento. Diferente dos processos do TJUE

esse processo está relacionado com o direito de imagem de uma pessoa combinado com danos morais em face da liberdade de imprensa de um programa televisivo de investigação. Já existe uma nova jurisprudência no decorrer desse capítulo que foi o primeiro processo sobre desindexação.

Segundo o próprio acórdão, Jurandir Gomes de França ajuizou ação de reparação de danos morais em favor da TV Globo Ltda. (Globo Comunicações e Participações S/A). Esta estação informou participação de Jurandir Gomes de França como coautor/participante da sequência de homicídios ocorridos em 23 de julho de 1993, na cidade do Rio de Janeiro, conhecidos como "Massacre da Candelária", mas que, a final, submetido a júri, foi absolvido da autoria pela unanimidade dos membros do Conselho de Sentença.[236]

Então a TV Globo procurou-o com o intuito de uma entrevista no programa televisivo "Linha Direta - Justiça", posteriormente transmitido, tendo sido recusada a realização da entrevista e mencionado o desinteresse do autor em ter sua imagem apresentada em contexto nacional. Porém, em junho de 2006, foi transmitido, tendo sido o autor apontado como um dos envolvidos no massacre, do qual a sua participação não fora provada.

O autor contesta a exposição pública, reacendendo na comunidade onde reside a imagem de participante no massacre e o ódio social, ferindo, assim, o seu direito à paz, anonimato e privacidade pessoal, com prejuízos diretos também dos seus familiares. Esta situação, afirma Jurandir Gomes de França prejudicou de enormemente a sua vida profissional, encontrando-se ainda desempregado, além de ter sido obrigado a desfazer-se de todos os seus bens e abandonar a comunidade por temer pela própria vida devido a "justiceiros" e traficantes e também para proteger a segurança dos seus familiares.

Por entender que a exposição de sua imagem e nome no referido programa foi ilegítima e causou-lhe intenso abalo moral, requereu uma indeminização no valor de 300 (trezentos) salários mínimos brasileiros.

O Juiz de Direito da 3ª Vara Civil do Rio de Janeiro, em primeira instância, segundo o próprio acórdão, avaliando, de um lado, o interesse público da notícia acerca

[236] Superior Tribunal de Justiça. Recurso Especial nº 1.334.097, de 22 de maio de 2013.

de "evento traumático da história nacional" e que repercutiu "de forma desastrosa na imagem do país junto à comunidade internacional", e, de outro, o "direito ao anonimato e ao esquecimento" do autor, entendeu por bem mitigar o segundo, julgando improcedente o pedido indemnizatório.

Porém, em segunda instância, a decisão tomada pela 3ª Vara Civil do Rio de Janeiro, a decisão foi reformada, conforme a ementa da decisão:

> Apelação. Autor que, acusado de envolvimento na Chacina da Candelária, vem a ser absolvido pelo Tribunal do Júri por unanimidade. Posterior veiculação do episódio, contra sua vontade expressa, no programa Linha Direta, que declinou seu nome verdadeiro e reacendeu na comunidade em que vivia o autor o interesse e a desconfiança de todos. Conflito de valores constitucionais. Direito de Informar e Direito de Ser Esquecido, derivado da dignidade da pessoa humana, prevista no art. 1.º, III, da Constituição Federal.
>
> I - O dever de informar, consagrado no art. 220 da Carta de 1988, faz-se no interesse do cidadão e do país, em particular para a formação da identidade cultural deste último.
>
> II - Constituindo os episódios históricos patrimônio de um povo, reconhece-se à imprensa o direito/dever de recontá-los indefinidamente, bem como rediscuti-los, em diálogo com a sociedade civil.
>
> III - Do Princípio Constitucional da Dignidade da Pessoa Humana, e do direito que tem todo cidadão de alcançar a felicidade, restringe-se a informação, contudo, no que toca àqueles que, antes anônimos, foram absolvidos em processos criminais e retornaram ao esquecimento.
>
> IV - Por isto, se o autor, antes réu, viu-se envolvido em caráter meramente lateral e acessório, em processo do qual foi absolvido, e se após este voltou ao anonimato, e ainda sendo

possível contar a estória da Chacina da Candelária sem a menção de seu nome, constitui abuso do direito de informar e violação da imagem do cidadão a edição de programa jornalístico contra a vontade expressamente manifestada de quem deseja prosseguir no esquecimento.

V - Precedentes dos tribunais estrangeiros. Recurso ao qual se dá provimento para condenar a ré ao pagamento de R$ 50.000,00 a título de indenização.

Foram posteriormente opostos embargos infringentes, que por maioria, foram rejeitados com a seguinte ementa:

"Embargos Infringentes. Indemnizatória. Matéria televisivo jornalística: "chacina da Candelária". Pessoa acusada de participação no hediondo crime e, alfim, inocentada. Uso não consentido de sua imagem e nome. Conflito aparente entre princípios fundamentais de Direito: Informação "vs" Vida Privada, Intimidade e Imagem. Direito ao esquecimento e direito de ser deixado em paz: sua aplicação. Proteção da identidade e imagem de pessoa não-pública. Dados dispensáveis à boa qualidade jornalística da reportagem. Dano moral e dano à imagem: distinção e autonomia relativa. Indenização. Quantificação: critérios.

1. Trata-se de ação indemnizatória por dano moral e à imagem, fundada não em publicação caluniosa ou imprecisa, mas no só revolver de factos pretéritos que impactaram drasticamente a esfera da vida privada do autor - acusado que fora, injustamente, de participação na autoria de crime de inglória lembrança, a "chacina da Candelária". Por isto mesmo, não aproveita à ré a alegação de cuidado com a verdade dos factos e sua não distorção - alegação que, conquanto veraz, não guarda relação com a causa de pedir.

2. Conquanto inegável seja o interesse público na discussão aberta de factos históricos pertencentes à memória coletiva, e de todos os pormenores a ele relacionados, é por outro lado contestável a necessidade de revelarem-se nome completo e imagem de pessoa envolvida, involuntariamente, em episódio tão funesto, se esses dados já não mais constituem novidade jornalística nem acrescem substância ao teor da matéria vocacionada a revisitar factos ocorridos há mais de década. Não é leviano asseverar que, atendido fosse o clamor do autor de não ter revelados o nome e a imagem, o distinto público não estaria menos bem informado sobre a Chacina da Candelária e o desarranjado inquérito policial que lhe sucedeu, formando uma vergonha nacional à parte.

3. Recorre-se ao juízo de ponderação de valores para solver conflito (aparente) de princípios de Direito: no caso, o da livre informação, a proteger o interesse privado do veículo de comunicação voltado ao lucro, e o interesse público dos destinatários da notícia; e o da inviolabilidade da intimida- de, da imagem e da vida privada. A desfiguração eletrônica da imagem do autor e o uso de um pseudônimo (como se faz, em observância a nosso ordenamento, para proteção de menores infratores) consistiria em sacrifício mínimo à liberdade de expressão, em favor de um outro direito fundamental que, no caso concreto, merecia maior atenção e preponderância.

4. Das garantias fundamentais à intimidade e à vida privada, bem assim do princípio basilar da dignidade da pessoa humana, extraíram a doutrina e a jurisprudência de diversos países, como uma sua derivação, o chamado "direito ao esquecimento", também chamado pelos norte-americanos de "direito de ser deixado em paz". Historicamente, a construção desses conceitos jurídicos fez- se a bem da ressocialização de autores de atos delituosos, sobretudo quando libertados ou em vias de o serem. Se o direito ao esquecimento beneficia os que já pagaram por

crimes que de facto cometeram, com maior razão se deve observá-lo em favor dos inocentes, involuntariamente tragados por um furacão de eventos nefastos para sua vida pessoal, e que não se convém revolver depois que, com esforço, a vítima logra reconstruir sua vida.

5. Analisado como sistema que é, nosso ordenamento jurídico, que protege o direito de ressocialização do apenado (art. 748 do CPP) e o direito do menor infrator (arts. 17 e 18 do ECA), decerto protegerá também, por analogia, a vida privada do inocente injustamente acusado pelo Estado.

6. O direito de imagem não se confunde com o direito à honra: para a violação daquele, basta o uso não consentido da imagem, pouco importando se associada ou não a um conteúdo que a denigra. Não sendo o autor pessoa pública, porque a revelação de sua imagem já não traz novidade jornalística alguma (pois longínqua a data dos factos), o uso de sua imagem, a despeito da expressa resistência do titular, constitui violação de direito a todos oponível, violação essa que difere da ofensa moral (CF. art. 5.º, V, da CF).

7. Tomando em linha de conta a centralidade do princípio da dignidade da pessoa humana, a severidade dos danos decorrentes da exibição do programa televisivo na vida privada do autor (relançado na persona de "suspeito" entre as pessoas de sua convivência comunal), e o conteúdo punitivo-pedagógico do instituto da indenização por dano moral, a verba aparentemente exagerada de R$ 50.000,00 se torna adequada - tanto mais em se tratando do veículo de comunicação de maior audiência e, talvez, de maior porte econômico.

Desprovimento do recurso”

Em Recurso Especial ao STJ, o Relator Ministro Luis Felipe Salomão em seu voto refere que muito embora tenham as instâncias ordinárias reconhecido que a reportagem

se mostrou legítima com a realidade, a aceitação do homem médio brasileiro a noticiários dessa categoria é propícia a reacender a desconfiança geral acerca da índole do autor, que, certamente, não teve reforçada sua imagem de inocente, mas sim a de autor.

Neste caso, permitir nova veiculação do facto com a indicação precisa do nome e imagem do autor, significaria a autorização de uma segunda ofensa ao seu decoro, só porque a primeira já ocorrera, porquanto, como bem reconheceu o acórdão recorrido, além do crime em si, o inquérito policial consubstanciou uma reconhecida "vergonha" nacional.

Completando seu voto com a seguinte sentença:

> "Os valores sociais ora cultuados conduzem a sociedade a uma perceção invertida dos factos, o que gera também uma conclusão às avessas: antes de enxergar um inocente injustamente acusado, visualiza um culpado acidentalmente absolvido.
>
> Por outro lado, o quantum da condenação imposta nas instâncias ordinárias (R$ 50.000,00) não se mostra exorbitante, levando-se em consideração a gravidade dos factos, assim também a sólida posição financeira da recorrente, circunstância que me faz manter o acórdão também nesse particular.
>
> Diante do exposto, nego provimento ao recurso especial.
>
> É como voto."

Para Poliana Bozérgia Moreira, ficou demonstrado no voto que apesar do direito à informação ter papel de destaque no atual ordenamento jurídico, este não é amplo e irrestrito, encontrado limitações no também fundamental princípio da dignidade da pessoa humana.[237]

Alguns episódios tornaram-se marcantes e constituem a própria identidade cultural do país, devendo ser recontados a fim de que se entenda a história da nação. No entanto, há que se conservar a identidade daqueles que foram absolvidos. Hoje é possível notar que a informação deixou de ser só um direito e passou a ser utilizada como uma

[237] Moreira, Poliana Bozégia. Página 310.

atividade lucrativa, em que não é privilegiado o direito à privacidade da pessoa objeto da informação, mas sim a busca do dinheiro que a aquela notícia renderá para quem a veicula.[238]

Sendo assim, há que se determinar limites ao direito de informação, proporcionando uma harmonização com os direitos decorrentes da privacidade do indivíduo, levando-se em consideração as especificidades do caso concreto para se verificar qual direito prevalecerá naquela situação.[239]

A TV Globo Ltda posteriormente ainda intentou Agravo de Instrumento contra a decisão publicada pelo STJ, com Instrução do então Ministro Joaquim Barbosa. O recurso não foi admitido com o Ministro a afirmar que "declinadas no julgado as razões do *decisum*, está satisfeita a exigência constitucional.", conforme pode ser visto na seguinte ementa:

> "Agravo de instrumento de decisão que inadmitiu RE, a, contra acórdão do Tribunal Superior do Trabalho, assim do: "ANTECIPAÇÃO DA GRATIFICAÇÃO NATALINA. CONVERSÃO EM URV. APLICAÇÃO DA LEI N.º 8.880/94. O art. 24 da Lei n.º 8.880/94, que instituiu a URV, dispõe que nas deduções de antecipações de décimo terceiro salário ou de gratificação natalina deve ser considerado o valor da antecipação, em URV ou equivalente em URV, na data do efetivo pagamento. Embargos não conhecidos. "Alega-se violação dos artigos 5.º, II, XXXV, XXXVI e LV; 7o, VI; e 93, IX, da Constituição Federal. O acórdão recorrido limitou-se a aplicar a legislação infraconstitucional pertinente ao caso. A pretensa ofensa aos dispositivos constitucionais tidos como violados, se houvesse, seria indireta ou reflexa: incide, mutatis mutandis, a Súmula 636.Não há falar em negativa de prestação jurisdicional ou violação dos princípios compreendidos nos artigos 5.º, XXXV e LV, e 93, IX, da Constituição Federal. A jurisdição foi prestada, no caso, mediante decisão suficientemente motivada, não

[238] Moreira, Poliana Bozégia. Página 310.
[239] Moreira, Poliana Bozégia. Página 310.

> obstante contrária à pretensão do recorrente, tendo o Tribunal a quo, como se observa do acórdão proferido, justificado suas razões de decidir: "o que a Constituição exige, no preceito invocado, é que a decisão seja fundamentada, não, que a fundamentação seja correta: declinadas no julgado as razões do decisum, está satisfeita a exigência constitucional."(RE 140.370, Sepúlveda Pertence, 1a T, DJ 21.5.1993).Nego provimento ao agravo. Brasília, 2 de agosto de 2004.Ministro SEPÚLVEDA PERTENCE - Relator
>
> (STF - AI: 400336 RJ, Relator: Min. JOAQUIM BARBOSA, Data de Julgamento: 02/08/2004, Data de Publicação: DJ 27/08/2004 PP-00095)”

A TV Globo Ltda intentou novo Agravo Regimental em Relação ao Agravo de Instrumento, afirmando ofensa indireta ou reflexiva à Constituição Federal, conforme o enunciado 279 da Súmula do STF. Em Instrução pelo Ministro Joaquim Barbosa, o agravo teve seu provimento negado em decisão unânime pela 2ª Turma do STF, conforme ementa:

> “EMENTA: AGRAVO REGIMENTAL EM AGRAVO DE INSTRUMENTO. RESPONSABILIDADE CIVIL DO ESTADO. DANO MORAL POR RICOCHETE. OFENSA INDIRETA OU REFLEXA À CONSTITUIÇÃO. ENUNCIADO 279 DA SÚMULA/STF. Agravo regimental a que se nega provimento.
>
> (STF - AI: 400336 RJ, Relator: Min. JOAQUIM BARBOSA, Data de Julgamento: 24/05/2011, Segunda Turma, Data de Publicação: DJe-108 DIVULG 06-06-2011 PUBLIC 07-06-2011 EMENT VOL-02538-01 PP-00071)”

A TV Globo Ltda intentou novo Recurso Extraordinário com Agravo (ARE/789246), com Instrução do Ministro Celso de Mello, sob a defesa de que “a

agravante ao deduzir o apelo extremo em questão, sustentou que o Tribunal "*a quo*" teria transgredido preceitos inscritos na Constituição da República".[240]

Porém em sua decisão, reconheceu que o caso em questão se encaixa no caso de repercussão geral, de Instrução do Ministro Dias Toffoli dos processos ARE 833.248/RJ, posteriormente substituído pelo RE 1.010.606/RJ.

Por fim o Ministro Celso de Mello proferiu que: "Isso significa que se impõe, quanto ao Tema n.º 786, nos termos do art. 328 do RISTF, na redação dada pela Emenda Regimental n.º 21/2007, a devolução dos presentes autos ao Tribunal de origem."

Sendo assim, o primeiro processo sobre o direito ao esquecimento não foi ainda julgado pelo STF, que colocou esse processo à espera de sentença para o processo reconhecido como repercussão geral, o processo do Caso Aída Curi.

Em nada, este caso, reflete a ideia de direito ao esquecimento que já está previsto no Regulamento 2016/679 do Parlamento e do Conselho Europeu. O processo ainda está ligado ao direito de imagem em relação ao direito de impressa, o que está também em discussão no caso a seguir que é de repercussão geral, segundo o STF.

3.2. Caso "Aída Curi"

O caso Aída Curi foi o segundo processo sobre o direito ao esquecimento que chegou ao STJ. Foi considerado Repercussão Geral para o STF e não foi ainda julgado. A discussão decorre do mesmo problema do processo descrito anteriormente.

No dia 14 de julho de 1958, no bairro de Copacabana na cidade do Rio de Janeiro, Aída Curi, à data com 18 anos de idade, foi arrastada até o topo do Edifício Rio Nobre por dois rapazes que foram ajudados pelo porteiro a abusar sexualmente da mesma.[241]

[240] Supremo Tribunal Federal. ARE 789246 - Recurso Extraordinário com Agravo, 2015. Disponível em <http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4510026>.
[241] Moreira, Poliana Bozégia. Página 310.

Segundo a perícia, Aída foi submetida a pelo menos trinta minutos de tortura e luta corporal com os três agressores, até desmaiar. Para encobrir o crime, os mesmos atiraram a jovem do terraço do prédio tentando simular um suicídio.

Este crime foi um dos mais célebres nos jornais policiais da época devido à forte comoção gerada na população. E em razão desta popularidade, foi um dos crimes também apresentados no programa televisivo Linha Direta.

Por causa da apresentação no programa televisivo da TV Globo Ltda, os irmãos da vítima intentaram uma ação de indeminização por danos morais, materiais e à imagem contra a estação de televisão, alegando que o crime teria sido esquecido com o passar do tempo e que a exibição do programa trouxe à tona todo a amargura que sentiram na época do facto, reabrindo as antigas feridas da família. Sustentaram também que comunicaram previamente à cadeia de televisão de que não autorizavam a nova exposição do crime, e em razão disso, houvera enriquecimento ilícito da cadeia de televisão, com a exploração da tragédia familiar, obtendo lucros com audiência e publicidade.

Tanto para a primeira e segunda instância, o pedido foi improcedente. Em ambas as decisões o facto foi identificado já como público, e que a cadeia de televisão utilizando do programa em questão, executou apenas o papel de informar.

A família então intentou Recurso Especial para o STJ, que sob Instrução do Ministro Luis Felipe Salomão, o mesmo Instrutor do Caso da Candelária envolvendo também o Programa Linha Direta, a 4ª Turma do STJ negou o provimento do recurso e concordou com o que fora julgado nas instâncias anteriores, conforme ementa:

> “RECURSO ESPECIAL. DIREITO CIVIL-CONSTITUCIONAL. LIBERDADE DE IMPRENSA VS. DIREITOS DA PERSONALIDADE. LITÍGIO DE SOLUÇÃO TRANSVERSAL. COMPETÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA. DOCUMENTÁRIO EXIBIDO EM REDE NACIONAL. LINHA DIRETA-JUSTIÇA. HOMICÍDIO DE REPERCUSSÃO NACIONAL OCORRIDO NO ANO DE 1958. CASO "AIDA CURI". VEICULAÇÃO, MEIO SÉCULO DEPOIS DO FACTO, DO NOME E IMAGEM DA VÍTIMA. NÃO CONSENTIMENTO DOS FAMILIARES. DIREITO AO

ESQUECIMENTO. ACOLHIMENTO. NÃO APLICAÇÃO NO CASO CONCRETO. RECONHECIMENTO DA HISTORICIDADE DO FACTO PELAS INSTÂNCIAS ORDINÁRIAS. IMPOSSIBILIDADE DE DESVINCULAÇÃO DO NOME DA VÍTIMA. ADEMAIS, INEXISTÊNCIA, NO CASO CONCRETO, DE DANO MORAL INDENIZÁVEL. VIOLAÇÃO AO DIREITO DE IMAGEM. SÚMULA N. 403/STJ. NÃO INCIDÊNCIA.

1. Avulta a responsabilidade do Superior Tribunal de Justiça em demandas cuja solução é transversal, interdisciplinar, e que abrange, necessariamente, uma controvérsia constitucional oblíqua, antecedente, ou inerente apenas à fundamentação do acolhimento ou rejeição de ponto situado no âmbito do contencioso infraconstitucional, questões essas que, em princípio, não são apreciadas pelo Supremo Tribunal Federal.

2. Nos presentes autos, o cerne da controvérsia passa pela ausência de contemporaneidade da notícia de factos passados, a qual, segundo o entendimento dos autores, reabriu antigas feridas já superadas

quanto à morte de sua irmã, Aida Curi, no distante ano de 1958. Buscam a proclamação do seu direito ao esquecimento, de não ter revivida, contra a vontade deles, a dor antes experimentada por ocasião da morte de Aida Curi, assim também pela publicidade conferida ao caso décadas passadas.

3. Assim como os condenados que cumpriram pena e os absolvidos que se envolveram em processo-crime (REsp. n. 1.334/097/RJ), as vítimas de crimes e seus familiares têm direito ao esquecimento - se assim desejarem -, direito esse consistente em não se submeterem a desnecessárias lembranças de factos passados que lhes causaram, por si, inesquecíveis feridas. Caso contrário, chegar-se-ia à antipática e desumana solução de

reconhecer esse direito ao ofensor (que está relacionado com sua ressocialização) e retirá-lo dos ofendidos, permitindo que os canais de informação se enriqueçam mediante a indefinida exploração das desgraças privadas pelas quais passaram.

4. Não obstante isso, assim como o direito ao esquecimento do ofensor - condenado e já penalizado - deve ser ponderado pela questão da historicidade do facto narrado, assim também o direito dos ofendidos deve observar esse mesmo parâmetro. Em um crime de repercussão nacional, a vítima - por torpeza do destino - frequentemente se torna elemento indissociável do delito, circunstância que, na generalidade das vezes, inviabiliza a narrativa do crime caso se pretenda omitir a figura do ofendido.

5. Com efeito, o direito ao esquecimento que ora se reconhece para todos, ofensor e ofendidos, não alcança o caso dos autos, em que se reviveu, décadas depois do crime, acontecimento que entrou para o domínio público, de modo que se tornaria impraticável a atividade da imprensa para o desiderato de retratar o caso Aida Curi, sem Aida Curi.

6. É evidente ser possível, caso a caso, a ponderação acerca de como o crime tornou-se histórico, podendo o julgador reconhecer que, desde sempre, o que houve foi uma exacerbada exploração mediática, e permitir novamente essa exploração significaria conformar-se com um segundo abuso só porque o primeiro já ocorrera. Porém, no caso em exame, não ficou reconhecida esse artifício ou o abuso antecedente na cobertura do crime, inserindo-se, portanto, nas exceções decorrentes da ampla publicidade a que podem se sujeitar alguns delitos.

7. Não fosse por isso, o reconhecimento, em tese, de um direito de esquecimento não conduz necessariamente ao dever de indenizar. Em matéria de responsabilidade civil, a violação de direitos encontra-se na seara da ilicitude, cuja existência não

dispensa também a ocorrência de dano, com nexo causal, para chegar-se, finalmente, ao dever de indenizar. No caso de familiares de vítimas de crimes passados, que só querem esquecer a dor pela qual passaram em determinado momento da vida, há uma infeliz constatação: na medida em que o tempo passa e vai se adquirindo um "direito ao

esquecimento", na contramão, a dor vai diminuindo, de modo que, relembrar o facto trágico da vida, a depender do tempo transcorrido, embora possa gerar desconforto, não causa o mesmo abalo de antes.

8. A reportagem contra a qual se insurgiram os autores foi ao ar 50 (cinquenta) anos depois da morte de Aida Curi, circunstância da qual se conclui não ter havido abalo moral apto a gerar responsabilidade civil. Nesse particular, fazendo-se a indispensável ponderação de valores, o acolhimento do direito ao

esquecimento, no caso, com a consequente indenização, consubstancia desproporcional corte à liberdade de imprensa, se comparado ao desconforto gerado pela lembrança.

9. Por outro lado, mostra-se inaplicável, no caso concreto, a Súmula n. 403/STJ. As instâncias ordinárias reconheceram que a imagem da falecida não foi utilizada de forma degradante ou desrespeitosa. Ademais, segundo a moldura fática traçada nas instâncias ordinárias - assim também ao que alegam os próprios recorrentes -, não se vislumbra o uso comercial indevido da imagem da falecida, com os contornos que tem dado a jurisprudência para franquear a via da indenização.

10. Recurso especial não provido.

Acórdão

Vistos, relatados e discutidos estes autos, os Ministros da QUARTA TURMA do Superior Tribunal de Justiça acordam, na

conformidade dos votos e das notas taquigráficas a seguir, por maioria, negar provimento ao recurso especial, nos termos do voto do Senhor Ministro Relator. Votaram vencidos os Srs. Ministros Maria Isabel Gallotti e Marco Buzzi. Os Srs. Ministros Raul Araújo Filho e António Carlos Ferreira, votaram com o Sr. Ministro Relator.

Informações Adicionais

(VOTO VENCIDO)

É devida indenização pela veiculação de foto de vítima fatal de crime por emissora de televisão em programa com finalidade comercial, independentemente da comprovação de prejuízo, na hipótese em que seus familiares recusaram expressamente essa divulgação, ainda que o facto criminoso tenha ocorrido há mais de cinquenta anos e, à época, tenha suscitado forte interesse coletivo. Isso porque a conduta da emissora incide na proibição de exposição ou utilização da imagem para fins comerciais sem autorização e contra a expressa vontade da família da vítima, inserta no artigo 20, parte final, do CC, o que dá ensejo à indenização independentemente de comprovação de prejuízo, conforme a Súmula 403 do STJ. Acrescente-se que o facto de o crime haver suscitado forte interesse coletivo à época em que ocorreu não é suficiente para mitigar o direito da vítima e de seus familiares de não ter a imagem da vítima divulgada, considerando a proteção legal à intimidade e à privacidade do morto e o sentimento comum de que as famílias não desejam ver seus mortos expostos em mídia televisiva. Ademais, o dever de informar não equivale a uma autorização de explorar economicamente um facto de há muito sucedido, que não envolveu pessoas notórias. Assim, eternizar uma informação desprovida de interesse público ou histórico viola o direito ao esquecimento a que tem a família da vítima do crime."

Os irmãos de Aída Curi interpuseram Recurso Extraordinário ao STF, que foi considerado Repercussão Geral, e sob Instrução do Ministro Dias Toffoli, e que ainda será julgado, mas não tem data para acontecer, conforme ementa:

> "DIREITO CONSTITUCIONAL. VEICULAÇÃO DE PROGRAMA TELEVISIVO QUE ABORDA CRIME OCORRIDO HÁ VÁRIAS DÉCADAS. AÇÃO INDEMNIZATÓRIA PROPOSTA POR FAMILIARES DA VÍTIMA. ALEGADOS DANOS MORAIS. DIREITO AO ESQUECIMENTO. DEBATE ACERCA DA HARMONIZAÇÃO DOS PRINCÍPIOS CONSTITUCIONAIS DA LIBERDADE DE EXPRESSÃO E DO DIREITO À INFORMAÇÃO COM AQUELES QUE PROTEGEM A DIGNIDADE DA PESSOA HUMANA E A INVIOLABILIDADE DA HONRA E DA INTIMIDADE. PRESENÇA DE REPERCUSSÃO GERAL.
>
> **Decisão:** O Tribunal, por maioria, reputou constitucional a questão, vencido o Ministro Marco Aurélio. Não se manifestou a Ministra Cármen Lúcia. O Tribunal, por maioria, reconheceu a existência de repercussão geral da questão constitucional suscitada, vencido o Ministro Marco Aurélio. Não se manifestou a Ministra Cármen Lúcia."

O caso mantém ainda o debate, principalmente em relação ao direito ao esquecimento e a liberdade de imprensa. No dia 12 de junho de 2017, em audiência pública do STF, teve como tema o direito ao esquecimento e o ponto de partida foi o Caso Aída Curi.

O Ministro Instrutor Dias Toffili explicou que a família da vítima argumenta que sofreu "massacre" de órgãos de imprensa na época e diz que os familiares ficaram estigmatizados. Eles declaram que, depois de mais de 50 anos, foi transmitido um

programa que explorou a imagem real de Aída Curi, com cenas impactantes de violência.[242]

No processo, segundo Toffoli, a TV Globo Ltda esclareceu que o conteúdo debatido no programa se limita a factos públicos e históricos e que grande parte do programa foi composta por arquivos da época, além de material de livros sobre o caso. A empresa interpreta que é direito de todos o acesso à história e estabelece que os direitos de imagem não se sobrepõem ao direito coletivo da sociedade de ter acesso a factos históricos, segundo a instrução do ministro.

Em entrevista ao Jornal Folha de São Paulo, o Ministro Luis Felipe Salomão, do STJ e Instrutor dos Casos da Candelária e de Aída Curi, disse que: "O direito ao esquecimento não é espécie de censura". Completou dizendo que: “a discussão em curso atualmente versa sobre se é possível retirar conteúdo da Internet e em que medida, como se faz na Europa, mas sem impedir publicação”.[243]

O Advogado do Google Brasil Guilherme Sanchez, na mesma entrevista, afirmou que: "o alcance e a dimensão da internet potencializam e aprofundam a tensão entre a liberdade de informação e outros direitos", e completou dizendo que: "O Brasil não é um país de direitos absolutos e a liberdade de expressão não é um direito absoluto. Só que o nível de liberdade e autonomia do nosso povo e a qualidade da nossa democracia tem relação direta com o apreço que nós temos pela liberdade de informar e de nos expressarmos.".[244]

A então Presidente, e hoje, Ministra do STF, Cármen Lúcia, afirmou sobre o Direito ao Esquecimento que: "Nós encontraremos, com certeza, o equilíbrio que é virtuoso para deixar que a liberdade garanta a dignidade, mas que a liberdade de um não se sobreponha à de todos os outros de tal maneira que nós não tenhamos mais condições de saber qual é a nossa história". E completou em entrevista à Folha de São Paulo que: "

[242] Folha de São Paulo. Em debate no STF, especialistas divergem sobre direito a esquecimento. 12 de junho de 2017. Disponível em <http://www1.folha.uol.com.br/poder/2017/06/1892422-em-debate-no-stf-especialistas-divergem-sobre-direito-a-esquecimento.shtml>.
[243] Folha de São Paulo. Para ministro do STJ, direito ao esquecimento é diferente de censura. 07 de novembro de 2017. Disponível em <http://www1.folha.uol.com.br/poder/2017/11/1933401-para-ministro-do-stj-direito-ao-esquecimento-e-diferente-de-censura.shtml>.
[244] Idem

É preciso reconhecer que, para que eu tenha futuro, é preciso que eu tenha passado. Ter passado é ter identidade, e um povo não vive sem identidade.".[245]

3.3. Caso "Xuxa Meneghel"

O caso Xuxa Meneghel foi o primeiro processo a chegar ao STJ sobre o direito ao esquecimento, em relação à desindexação do motor de pesquisa, conforme esse direito foi estabelecido na UE. Foi o primeiro que envolveu internet e o motor de pesquisa em face do direito ao esquecimento de um utilizador. Cabe uma comparação a Deliberação 536/2016 da Comissão Nacional de Proteção de Dados de Portugal, pois trata-se de uma figura pública que tem sua imagem e sua vida pessoal afetada por ligações de seu nome a pesquisa na internet.

Em outubro de 2010, segundo Erik Noleta Kirk Palma Lima, Xuxa Meneghel intentou ação visando obrigar o provedor Google a remover da sua página de internet os resultados relativos à pesquisa pela expressão "xuxa pedófila" ou ainda qualquer outra que associasse o nome da apresentadora a uma prática criminosa qualquer. Foi deferido para que o Google não disponibilizasse aos seus utilizadores aqueles resultados.[246]

O Google intentou então Recurso Especial no STJ, onde a 3ª Turma, sob Instrução da Ministra Nancy Andrighi, por unanimidade votou a favor para o provimento do recurso, pelos motivos de que é tecnicamente impossível de ser cumprida, derivando assim a incompatibilidade da multa cominatória fixada, com clara violação do art. 461, § 4.º, do CPC. Porém, conforme a instrutora, mesmo que se quisesse adequar os termos da mencionada decisão, objetivando a sua exequibilidade, exigindo da vítima a indicação dos URLs, implicaria ausência de interesse de agir da recorrida. Adicionalmente ao indicado acima, a instrutora verificou que no julgamento, de uma forma mais ampla, o descabimento de se impor aos provedores de pesquisa qualquer restrição nos resultados das buscas realizadas por seus sistemas, sob pena de afronta ao direito constitucional de informação, conforme ementa:

> "CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO

[245] Folha de São Paulo. STF encontrará 'equilíbrio' ao julgar direito ao esquecimento, diz Cármen. 28 de agosto de 2017. Disponível em <http://www1.folha.uol.com.br/poder/2017/08/1911849-stf-encontrara-equilibrio-ao-julgar-direito-ao-esquecimento-diz-carmen.shtml>.
[246] Lima, Erik Noleta Kirk Palma. Direito ao esquecimento: Discussão europeia e sua repercussão no Brasil . Revista de Informação Legislativa, Ano 50(Número 199), p. 277, 2013.

SERVIÇO. INDIFERENÇA. PROVEDOR DE PESQUISA. FILTRAGEM PRÉVIA DAS BUSCAS. DESNECESSIDADE. RESTRIÇÃO DOS RESULTADOS. NÃO-CABIMENTO. CONTEÚDO PÚBLICO. DIREITO À INFORMAÇÃO.

1. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei n.º 8.078/90. 2. O facto de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração", contido no art. 3.º, § 2.º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. 3. O provedor de pesquisa é uma espécie do gênero provedor de conteúdo, pois não inclui, hospeda, organiza ou de qualquer outra forma gerencia as páginas virtuais indicadas nos resultados disponibilizados, se limitando a indicar links onde podem ser encontrados os termos ou expressões de busca fornecidos pelo próprio usuário. 4. A filtragem do conteúdo das pesquisas feitas por cada usuário não constitui atividade intrínseca ao serviço prestado pelos provedores de pesquisa, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não exerce esse controle sobre os resultados das buscas. 5. Os provedores de pesquisa realizam suas buscas dentro de um universo virtual, cujo acesso é público e irrestrito, ou seja, seu papel se restringe à identificação de páginas na web onde determinado dado ou informação, ainda que ilícito, estão sendo livremente veiculados. Dessa forma, ainda que seus mecanismos de busca facilitem o acesso e a consequente divulgação de páginas cujo conteúdo seja potencialmente ilegal, facto é que essas páginas são públicas e compõem a rede mundial de computadores e, por isso, aparecem no resultado dos sites de pesquisa. 6. Os provedores de pesquisa não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente

da indicação do URL da página onde este estiver inserido. 7. Não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1.º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa. 8. Preenchidos os requisitos indispensáveis à exclusão, da web, de uma determinada página virtual, sob a alegação de veicular conteúdo ilícito ou ofensivo – notadamente a identificação do URL dessa página – a vítima carecerá de interesse de agir contra o provedor de pesquisa, por absoluta falta de utilidade da jurisdição. Se a vítima identificou, via URL, o autor do ato ilícito, não tem motivo para demandar contra aquele que apenas facilita o acesso a esse ato que, até então, se encontra publicamente disponível na rede para divulgação. 9. Recurso especial provido.

A requerente Xuxa ainda interpôs Embargos de Declaração, no recurso acima apresentado, ao qual os Ministros da 3.º Turma acordaram por unanimidade a rejeição do provimento dos Embargos, sob Instrução da Ministra Nancy Andrighi, conforme ementa:

> "PROCESSO CIVIL. EMBARGOS DE DECLARAÇÃO NO RECURSO ESPECIAL. IRRESIGNAÇÃO DA PARTE. EFEITOS INFRINGENTES. IMPOSSIBILIDADE.
>
> 1. A atribuição de efeitos modificativos aos embargos declaratórios é possível apenas em situações excecionais, em que sanada a omissão, contradição ou obscuridade, a alteração da decisão surja como consequência lógica e necessária. 2. Não há previsão no art. 535 do CPC, quer para reabertura do debate, quer para análise de questões não abordadas nos acórdãos recorridos, notadamente quando fundados os embargos de declaração no mero inconformismo da parte. 3. Embargos de declaração no recurso especial rejeitados.

Com a rejeição do recurso, Xuxa interpôs então Reclamação ao STF com medida cautelar, Rcl 15955, que em decisão unanime pelo Ministro Instrutor Celso de Mello foi colocado que: "**nego seguimento** à presente reclamação, **restando prejudicado**, *em consequência*, **o exame** do pedido de medida liminar.". Houve posteriormente Agravo Regimental a decisão do Ministro Instrutor, que "A Turma, por votação unânime, **negou** provimento ao recurso de agravo, **nos termos** do voto do Relator. Ausente, justificadamente, o Senhor Ministro Dias Toffoli. Presidência do Senhor Ministro Celso de Mello. **2ª Turma**, 15.09.2015.".

Por fim, Xuxa interpôs Agravo Regimental na Reclamação, em relação a decisão do Ministro Celso de Mello, que também foi relator deste agravo, e por unanimidade novamente, a Segunda Turma do STF negou o provimento concordando com o voto do relator, conforme ementa:

> **"Reclamação** – **arguição de ofensa** *ao postulado da reserva de plenário* (**cf**, art. 97) – **súmula vinculante n.º 10/stf** – **inaplicabilidade** a situações **que configurem** simples "*crise de legalidade*" – **inexistência**, *no caso, de juízo* (**ostensivo ou disfarçado**) *de inconstitucionalidade* **de qualquer** ato estatal – **julgamento pelo órgão reclamado** que se efetuou **em face** *do ordenamento infraconstitucional – contencioso de mera legalidade* – **inviabilidade** da reclamação – **precedentes** – **recurso de agravo improvido**.

Ao contrário da Deliberação n.º 536/2016 da Comissão Nacional de Proteção de Dados e do Acórdão Google Spain, de 2014, o STJ afirmou que "Os provedores de pesquisa não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, nem os resultados que apontem para uma foto ou texto específico, independentemente da indicação do URL da página onde este estiver inserido." Ainda "não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1.º, da CF/88, sobretudo considerando que a internet representa, hoje, importante veículo de comunicação social de massa.".

Ou seja, já fora consolidado na Europa o direito ao esquecimento, mesmo de pessoa pública, quando é atingido sua vida pessoal, de forma a prejudicar seu quotidiano. No processo presente as palavras que são ligadas ao nome da autora da ação com o resultado da pesquisa no motor de pesquisa não possuem correlação e o filme fora proibido a circulação, por meio judicial, antes mesmo desse processo chegar ao STJ.[247]

3.4. Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709)

A Lei 13.709, de 14 de agosto de 2018, veio alterar a Lei 12.965/14, conhecida como Marco Civil da Internet no Brasil. Esta lei dispõe especificamente sobre o tratamento de dados no Brasil.

Logo no seu primeiro artigo descreve que a Lei "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.".

No seu artigo 4.º, como o 23.º do RGPD, enumera as limitações ou as exclusões de incidência, como pode ser visto:

> Art. 4.º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
>
> II - realizado para fins exclusivamente:
>
> a) jornalístico e artísticos; ou
>
> b) acadêmicos, aplicando-se a esta hipótese os artigos 7.º e 11.º desta Lei;
>
> III - realizado para fins exclusivos de:

[247] Tribunal de Justiça do Rio de Janeiro. Processo nº 0019930-53.2010.8.19.0000, de 05 de maio de 2010.

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1.º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2.º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3.º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4.º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado.

O artigo 5.º, prevê a finalidade da lei, onde se vê pela primeira vez a palavra exclusão, como previsto que "XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado".

A Seção 3, titulada "Da Responsabilidade e do Ressarcimento de Danos", descreve sobre a exclusão do dado e sua responsabilidade. É previsto que:

> Art. 42. O responsável pelo tratamento ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1.º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do responsável pelo tratamento, hipótese em que o operador se equipara ao responsável pelo tratamento, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os responsáveis pelo tratamento que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

No entanto, o artigo 43 da mesma lei retira a responsabilidade dos agentes de tratamentos em três circunstâncias. A primeira é a não realização do tratamento de dados pessoais que lhes é atribuído; a segundo é que embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; por fim se o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Para Alexandre Veronese e Noemy Melo, a lei brasileira segue a moldura europeia, porém, utiliza-se de termologias menos claras e está redigido de uma forma

confusa, em comparação com o regulamento europeu. Os autores também afirmam que a lei brasileira possui um tamanho menor do que a norma europeia.[248]

Veronese e Melo ainda suscitam que o artigo 3.º da Lei deixa claro que ele é aplicável ao Poder Público e às empresas, porém, ao comparar com o regulamento europeu, a lei não reflete as obrigações que as empresas devem ter, e afirmam que essa falta de detalhe revela a ausência de vontade política de promover uma proteção mais radical no Brasil.[249]

A falta de incidência para o tratamento de dados de áreas específicas, como os previstos no regulamento europeu, sobre documentos públicos, identificação nacional, relações de trabalho e atividades religiosas, previstos nos artigos 86.º, 87.º, 88.º e 90.º do RGPD, respetivamente. A principal crítica fica para a falta de debate do tratamento de dados pessoais em questões criminais, que na EU foi fixado através da Diretiva 2016/680.[250]

A Lei Geral de Proteção de Dados apresenta o termo chamado "eliminação". No artigo 16 da Lei n.º 13.709, conhecida como Lei Geral de Proteção de Dados coloca a expressão "Os dados pessoais serão eliminados após o término de seu tratamento", com exceções previstas nos artigos 16 e 18 da mesma lei. Essa eliminação equipara ao direito ao apagamento previso na Diretiva 95/46 da EU, porém sem os aparos e a evolução do conceito que o acórdão Google e o RGPD trouxeram na Europa.

3.5. REsp n.º 1660168 – Superior Tribunal de Justiça

O REsp n.º 1660168 foi o primeiro processo que o STJ reconheceu como Repercussão Geral no Superior Tribunal de Justiça sobre o direito ao esquecimento como desindexação de motores de pesquisa na internet.

O processo foi iniciado no Rio de Janeiro por Denise Pieri Nunes, que requeria a desindexação, nos resultados das aplicações de pesquisa mantidas pelo "Yahoo!" e pelo Google, de notícias relacionadas às suspeitas de fraude no XLI Concurso da Magistratura do Estado do Rio de Janeiro. Na ação, a requerente alega que a indexação desses conteúdos seria a causa de danos à sua dignidade e à sua privacidade e, assim, requer a

[248] Veronese, Alexandre; Melo, Noemy. Página 89.
[249] Veronese, Alexandre; Melo, Noemy. Página 92.
[250] Veronese, Alexandre; Melo, Noemy. Página 94.

filtragem dos resultados de pesquisas que utilizem seu nome como parâmetro, a fim de desvinculá-la das mencionadas reportagens, conforme o voto da Ministra Instrutora Nancy Andrighi.[251]

O Tribunal de Justiça do Rio de Janeiro, em ação interposta por Denise Pieri Nunes, deu provimento ao pedido em que os mecanismos de pesquisas deveriam filtrarem os resultados, ou seja, desindexarem os resultados que teriam menção a recorrida, conforme ementa:

> "AÇÃO DE OBRIGAÇÃO DE FAZER C/C TUTELA ANTECIPADA. PROVEDOR DE PESQUISA. RELAÇÃO DE CONSUMO. ART. 3º, § 2.º, DO CDC. INTEPRETAÇÃO AMPLA INCLUINDO O GANHO INDIRETO DO FORNECEDOR. PRECEDENTE DO STJ (REsp 1192208). IMPLANTAÇÃO DE FILTRO POR PALAVRA-CHAVE COM ESCOPO DE EVITAR A ASSOCIAÇÃO DO NOME DA AUTORA A NOTÍCIAS QUE ENVOLVAM SUPOSTA FRAUDE NO XLI CONCURSO DA MAGISTRATURA DESTE ESTADO.
>
> SENTENÇA DE IMPROCEDÊNCIA. APELAÇÃO.
>
> 1- PEDIDO DE PROSSEGUIMENTO DA EXECUÇÃO PROVISÓRIA, AUTUADA SOB O NÚMERO 0412290.91.2011.8.19.0001, RELATIVA ÀS ASTREITES, PREJUDICADO COM BASE EM DOIS FUNDAMENTOS: AUSÊNCIA DE IMPUGNAÇÃO DA REVOGAÇÃO DA TUTELA ANTECIPADA PROVISÓRIA DECORRENTE DA SENTENÇA DE IMPROCEDÊNCIA E A NÃO INTERPOSIÇÃO DE RECURSO CONTRA A SENTENÇA DE EXTINÇÃO PROFERIDA NAQUELES AUTOS, ACARRETANDO A COISA JULGADA MATERIAL.

[251] Superior Tribunal de Justiça. **Recurso Especial Nº 1.660.168** - RJ (2014/0291777-1).

2- ILEGITIMIDADE PASSIVA DA MICROSOF INFORMÁTICA JÁ REFUTADA POR ESTE ÓRGÃO JULGADOR. EMBORA A QUESTÃO DA LEGITIMIDADE PASSIVA SEJA MATÉRIA DE ORDEM PÚBLICA, NÃO PODE SER OBJETO DE NOVA APRECIAÇÃO NESTA SEARA RECURSAL, SOB PENA DE MITIGAÇÃO EXACERBADA DA COISA JULGADA FORMAL.

3- PRELIMINAR DE IMPOSSIBILIDADE JURÍDICA DO PEDIDO SOB A ALEGADA NECESSIDADE DE AVALIAÇÃO FÁTICA DO CUMPRIMENTO DA ORDEM JUDICIAL E DE FALTA DE INTERESSE DE AGIR DIANTE DA INUTILIDADE DO PROVIMENTO JUDICIAL. QUESTÕES QUE SE CONFUNDEM COM O MÉRITO.

4- IMPOSSIBILIDADE TÉCNICA DE IMPLANTAÇÃO NÃO OBJETIVAMENTE COMPROVADA. DOCUMENTOS ACOSTADOS PELA AUTORA COMPROVANDO QUE OS APELADOS POSSUEM MEIOS DE PROCEDER À EXCLUSÃO DE RESULTADOS DO SISTEMA DE PESQUISAS DOS CHAMADOS "BUSCADORES" NOS MOLDE PLEITEADOS. DOCUMENTOS NÃO REFUTADOS.

5- DIREITO À INTIMIDADE E PRIVACIDADE X DIREITO À INFORMAÇÃO. PREVALÊNCIA DO DIREITO À IMAGEM, À PERSONALIDADE E AO ESQUECIMENTO, COM VISTA A EVITAR O EXERCÍCIO DA LIVRE CIRCULAÇÃO DE FACTOS NOTICIOSOS POR TEMPO IMODERADO.

6- ALEGAÇÃO DA YAHOO DA NECESSIDADE DE A AUTORA INDICAR AS URL'S A SEREM BLOQUEADAS. INDEFERIMENTO PELO JUÍZO DE PISO, CONFIRMADO POR ESTE ÓRGÃO JULGADOR. COISA JULGADA FORMAL.

> 7- PLEITO DE TUTELA RECURSAL. DEFERIMENTO. PRESENÇA DOS REQUISITOS DO ARTIGO 273 DO CPC. RISCO IMINENTE DE PERECIMENTO OU DE DANO AO DIREITO, PROVA INEQUÍVOCA E VEROSSIMILHANÇA DA ALEGAÇÃO.
>
> PROVIMENTO PARCIAL DO RECURSO.” [252]

A instrutora então prosseguiu para o seu voto, onde ela fez um capítulo sobre o direito ao esquecimento. Para a instrutora, o acórdão recorrido tem toda a fundamentação no direito ao esquecimento e obrigaria, assim, as recorrentes a filtrarem o conteúdo dos resultados de buscar que contenham o nome da recorrida, relacionadas às notícias de possível fraude em concurso para a magistratura no Rio de Janeiro.

Porém a Ministra instrutora acredita que no recurso em julgamento, figuram como recorrentes três provedores de aplicação de buscas, Google, Yahoo!, recorrentes no processo e Bing, interessada no processo, não detêm propriamente a informação que se quer ver esquecida, quem detêm a informação é quem noticiou, os provedores seriam apenas “meio” de chegar a essa informação.

Andrighi continua seu voto citando o acórdão Google, do TJUE, em 2014, onde ela menciona que o referido tribunal decidiu que:

> “I. Um provedor de aplicação de buscas deve ser considerado responsável pelos dados pessoais, nos termos da legislação europeia;
>
> II. A responsabilidade existe mesmo quando o servidor do provedor de aplicação de buscas se encontra fora do território europeu;
>
> III. Preenchidos os requisitos legais, um provedor de aplicação de buscas é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as conexões a outras páginas web publicadas por terceiros

[252] Superior Tribunal de Justiça. **Recurso Especial Nº 1.660.168** - RJ (2014/0291777-1)

> e que contenham informações sobre essa pessoa, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita;
>
> IV. O indivíduo, ao exercer seu direito ao esquecimento, não pode causar prejuízo a outra pessoa. Em princípio, esse direito prevalece sobre o interesse econômico do buscador e sobre o interesse público em acessar a informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse caso se houver razões especiais (por exemplo, se o requerente houver desempenhado relevante papel na vida pública).”

A Ministra instrutora faz ainda a ressalva que a lei europeia é muito distante das leis brasileiras, mesmo sendo um importante precedente. Porém, ela afirma que a ausência de uma lei geral que disponha sobre a proteção de dados pessoais dos cidadãos brasileiros. Deste modo, cumpre traçar algumas considerações sobre a jurisprudência pátria a esse respeito.

Como precedentes no próprio tribunal, a Ministra Andrighi com o Enunciado 531 da VI Jornada de Direito Civil, já referido anteriormente nesse trabalho, continuou seu raciocínio definindo o que seria direito ao esquecimento para o STJ, baseando em vários julgamentos da Quarta e Quinta Turmas do Tribunal (HC 256.210/SP, Sexta Turma, julgado em 03/12/2013, DJe 13/12/2013; REsp 1335153/RJ, Quarta Turma, julgado em 28/05/2013, DJe 10/09/2013; e REsp 1334097/RJ, Quarta Turma, julgado em 28/05/2013, DJe 10/09/2013), definindo como:

> “direito de não ser lembrado contra sua vontade, especificamente no tocante a factos desabonadores, de natureza criminal, nos quais se envolveu, mas que, posteriormente, fora inocentado”.

A Ministra Andrighi cita os ensinamentos de François Ost, segundo o qual o direito ao esquecimento deve atuar para proteger a vida privada de todo o indivíduo:

> “Em outras hipóteses, ainda, o direito ao esquecimento, consagrado pela jurisprudência, surge mais claramente como uma das múltiplas facetas do direito a respeito da vida privada. Uma vez que, personagem pública ou não, fomos lançados diante da

> cena e colocados sob os projetores da atualidade – muitas vezes, é preciso dizer, uma atualidade penal –, temos o direito, depois de determinado tempo, de sermos deixados em paz e a recair no esquecimento e no anonimato, do qual jamais queríamos ter saído. Em uma decisão de 20 de abril de 1983, Mme. Filipachi Cogedipresse, o Tribunal de última instância de Paris consagrou este direito em termos muito claros: "[...] qualquer pessoa que se tenha envolvido em acontecimentos públicos pode, com o passar do tempo, reivindicar o direito ao esquecimento; a lembrança destes acontecimentos e do papel que ela possa ter desempenhado é ilegítima se não for fundada nas necessidades da história ou se for de natureza a ferir sua sensibilidade; visto que o direito ao esquecimento, que se impõe a todos, inclusive aos jornalistas, deve igualmente beneficiar a todos, inclusive aos condenados que pagaram sua dívida para com a sociedade e tentam reinserir-se nela. (OST, François. O Tempo do direito. Tradução Élcio Fernandes. Bauru, SP: Edusc, 2005, p. 160-161)"

A Ministra ressalta o Marco Civil da Internet, quem em seu art. 7.º, I e X, preenche parcialmente a falta de legislação sobre o assunto no Brasil, principalmente em relação ao direito ao esquecimento. O artigo coloca que:

> Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; 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.

A instrutora continua seu voto citando que na hipótese de provedores de aplicações de pesquisa na internet, ou seja, os mecanismos de pesquisa, existe uma disponibilização de ferramentas que, por meio de algoritmos e de indexação, auxiliam o utilizador a encontrar páginas de internet ou outros recursos, de acordo com os

argumentos de pesquisa inseridos no serviço de busca, seguindo o julgamento da Terceira Turma da mesma Corte:

> Essa provedoria de pesquisa constitui uma espécie do gênero provedor de conteúdo, pois esses sites não incluem, hospedam, organizam ou de qualquer outra forma gerenciam as páginas virtuais indicadas nos resultados disponibilizados, se limitando a indicar links onde podem ser encontrados os termos ou expressões de busca fornecidos pelo próprio usuário. (REsp 1.316.921/RJ, Terceira Turma, julgado em 26/06/2012, DJe 29/06/2012).

Baseado no Código de Defesa do Consumidor, pela prestação de serviços desses motores de pesquisa, e no Marco Civil da Internet, onde prevê que a responsabilidade deve ficar restrita à natureza da atividade por eles desenvolvida, a Ministra afirma que, "os provedores de pesquisa devem garantir o sigilo, a segurança e a inviolabilidade dos dados cadastrais de seus usuários e das buscas por eles realizadas, bem como o bom funcionamento e manutenção do sistema. Por outro lado, tem-se que a filtragem de conteúdo das pesquisas feitas por cada usuário não é uma atividade intrínseca ao serviço prestado afastando-se a aplicação do art. 14º do CDC".

Em relação aos autos, a Ministra então decidiu que a autora do processo não tinha fundamentos normativos no ordenamento jurídico pátrio capaz de imputar à recorrente a obrigação de implementar o direito ao esquecimento da recorrida. Essa obrigação deve recair diretamente sobre aquele que mantém a informação no ambiente digital, dando então a causa aos recorrentes Google e Yahoo!, reformando a decisão do TJRJ.

O Ministro Ricardo Villas Bôas Cueva seguiu o voto da instrutora, explanando que apesar de ser possível vislumbrar legitimidade no requerido da autora de ver seu nome dissociado da narrativa de factos que a prejudicam, ocorridos no passado, para o ministro não há como negar que para a satisfação plena dessa pretensão o provimento jurisdicional ora pretendido não se revela necessário e, além disso, não é completamente eficaz.

Para ele o conteúdo cuja eventual manutenção na internet por tempo indeterminado se revelaria, em tese, ofensivo ao direito da autora de ser esquecida não é

de responsabilidade das recorrentes, ou seja, dos mecanismos de pesquisa, mas de terceiros provedores, que para o Ministro, mesmo diante da procedência do pedido autoral, publicações digitais relacionando o nome da autora com a suspeita de fraude no concurso permanecerão na internet e poderão ser facilmente encontradas por quem quer que seja, inclusive a partir da simples utilização do nome da autora como parâmetro de pesquisa em serviços dessa natureza oferecidos por outros provedores de aplicações.

O Ministro ainda suscita a necessidade de que para um URL ser eliminado, conforme o art. 19, §1.º, do Marco Civil da Internet, Lei n.º 12.965/2014, "sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material".

Afirmando então que o Tribunal já possui jurisprudência consolidada, sendo incontroverso, que essa responsabilização por conteúdo gerado por terceiros exigiria, em virtude da necessidade de se permitir a localização inequívoca do material ao provedor de aplicação, a indicação do URL da página a ser por ele eventualmente excluído.

Sendo assim o Ministro decidiu que os mecanismos de pesquisa, recorrentes no processo, não podem ser obrigados a executar monitorização prévia das informações que constam nos resultados de pesquisas.

O Ministro Marco Aurélio Bellizze, juntamente com os Ministros Moura Ribeiro e Paulo De Tarso Sanseverino votaram a favor da recorrida, ou seja, a favor do direito ao esquecimento, e foram os votos vencedores.

O Ministro Bellizze, em seu voto, esclareceu que o direito brasileiro tutela a proteção de dados dos cidadãos, seja com base na Constituição Federal, ao estabelecer o *habeas data* como instrumento jurídico de garantia da proteção aos dados pessoais (art. 5.º, LXXI, CRFB), seja por meio da Lei n. 9.507/1997, que regula o direito de acesso a informações e disciplina o rito processual do *habeas data*, além de legislações esparsas, como o Código de Defesa do Consumidor e o Marco Civil da Internet.

Ele complementa dizendo que as regras em vigor no território nacional brasileiro, não são tão distintas daquelas em que se apoiou o TJUE para normalizar a incidência da diretiva de proteção de dados aos aplicativos de busca, reconhecendo se referir a tratamento de dados a organização dos resultados exibidos.

O Ministro também coloca que a Diretiva 95/46 “não se endereça diretamente a disputas e regulamentos aplicáveis à realidade da internet, ainda incipiente à época de sua publicação, em 23 de novembro de 1995.”.

A divergência do Ministro acontece ao reconhecer que o Marco Civil da Internet estabelece a proteção aos registrados, previsto na Seção II do Capítulo II da Lei, havendo então a base legal sobre a qual apoiar eventual pretensão de obtenção da restrição de tratamento de dados.

Para ele o entendimento do Marco Civil não é de impor aos provedores de aplicação, principalmente aqueles que são dedicados exclusivamente à disponibilização de ferramenta de pesquisa, como os motores de pesquisa, não se pode colocar o ônus de retirar conteúdo inserido por terceiros, muito menos de lhes imputar a função de um “verdadeiro censor digital”, expressão usada pelo Ministro, que completou que o Poder Judiciário deve assegurar a apreciação de casos concretos excecionais em que se denote a ausência de razoabilidade na exibição dos resultados das pesquisa.

O Ministro elucidou que o próprio Google explica como funciona a sua pesquisa, ao referir:

> “(…) esse serviço tem por essência o rastreamento e a indexação de triliões de páginas disponíveis na web, possibilitando a localização e organização, segundo critérios internos de classificação e relevância das páginas já indexadas e organizadas em sua base de dados (sistema PageRank). Essa indexação, a princípio, é passível de futuras atualizações. Contudo, de modo geral, o sistema trabalha apenas acrescentando à base de dados as páginas novas localizadas por seu sistema de varredura.”

Para o Ministro não se pode afirmar que os resultados um dia existentes serão necessariamente excluídos, pelo facto de que algumas páginas pesquisadas novamente, conforme o mesmo disse em seu voto:

> “(…) algumas páginas serão varridas novamente – segundo uma periodicidade que variará de acordo com um sistema exclusivo de ranking das páginas, que toma em consideração a quantidade de

> vezes que ela é mencionada na rede por outros usuários e o volume de consultas e acessos –, porém, outras páginas, por sua ínfima relevância no meio virtual, serão ignoradas em novas varreduras, mantendo-se íntegro o resultado atrelado na base de dados do Google Search aos argumentos de pesquisa inseridos pelos internautas."

Ou seja, para o Ministro Marco Aurélio Bellizze, não se trata de impugnar as pesquisas que pretendessem colocar como resultado notícias vinculadas a fraudes em concursos, ou mesmo, o nome da autora da ação e outros critérios que a ligasse a concursos públicos ou fraudes. O Ministro coloca que "a manutenção desses resultados acaba por alimentar o sistema, uma vez que, ao realizar a pesquisa pelo nome da recorrida e se deparar com a notícia, o cliente terá acesso ao conteúdo – até movido por curiosidade despertada em razão da exibição do URL – reforçando, no sistema automatizado, a confirmação da relevância da página catalogada.".

Sendo assim, o Ministro Marco Bellize acredita ser imprescindível a atuação do Poder Judiciário para assegurar à pessoa em causa, a quebra dessa vinculação eterna pelos motores de pesquisa e desindexar os dados pessoais do resultado cujo já fora superado, classificando, assim, a essência do direito ao esquecimento como: "não se trata de efetivamente apagar o passado, mas de permitir que a pessoa envolvida siga sua vida com razoável anonimato, não sendo o facto desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca.".

O Ministro Bellizze salienta ainda que aqueles que pesquisem sobre fraudes em concursos públicos não teriam sua pesquisa impedida, mas livraria o nome da recorrida de permanecer acessível, seja a pesquisa com o nome dela ou apenas de termos ligados ao caso.

O Ministro finaliza seu raciocínio afirmando a existência de uma via conciliadora entre o livre acesso à informação e do legítimo interesse individual, evitando uma pesquisa direcionada a informações sobre a recorrida como critério de pesquisa exclusivo, não tendo como resultado a indicação de um noticiário de uma década, impedindo a mesma de superar o momento descrito no processo.

O Ministro Moura Ribeiro inicia seu raciocínio referindo que a determinação de que as notícias em questão fossem atualizadas, passando a constar a absolvição da autora, para o mesmo, seria medida suficiente e que atenderia simultaneamente aos interesses de todas as partes, porém o mesmo afirma a falta desse pedido no processo.

Para o Ministro Ribeiro a desindexação seria a segunda melhor solução, e para confirmar o seu pensamento cita Ingo Wolfgang Sarlet em seu voto, descrevendo o direito ao esquecimento como:

> "o direito ao esquecimento não se reduz ao direito de requerer o cancelamento de informações previsto no artigo 7.º da Lei do Marco Civil da Internet (e nem ao direito ao cancelamento consagrado no artigo 17 do novo Regulamento Europeu de Proteção de Dados), mas abarca (ou deveria, no nosso entender, da literatura brasileira majoritária e da posição prevalente no mundo europeu ocidental) um direito à desindexação em face dos provedores de pesquisa. (Vale a pena relembrar o que estamos fazendo com o direito ao esquecimento. Disponível em https://www.conjur.com.br/2018-jan-26/direitos-fundamentais-vale-p ena-relembrar-fizemos-direito-esquecimento, consultado aos 20/1/2018).".

O Ministro Moura Ribeiro segue então com a concordância ao voto do Ministro Marco Aurélio Bellizze, considerando juridicamente possível o pedido feito na exordial, ou seja, sendo possível a desindexação dos resultados pretendidos.

O Ministro então suscita o acórdão Google Spain, afirmando:

> "Ora, o Tribunal de Justiça Europeu, como se percebe, imputou aos mecanismos de busca a mesma responsabilidade que agora se quer ver a eles imputada neste processo, rechaçando a tese da impossibilidade técnica do pedido. Se, no caso espanhol, a desindexação se mostrou viável, a argumentação da inviabilidade técnica do procedimento não se sustenta.".

Sendo assim, o Ministro Moura Ribeiro termina seu voto acompanhando o Ministro Marco Aurélio Bellizze sobre a possibilidade da desindexação conforme pedido na inicial.

Por fim, o último voto e de desempate partiu do Ministro Paulo De Tarso Sanseverino, que iniciou seu raciocínio afirmando que mesmo antes da Lei Brasileira do Marco Civil ter sua edição, o STJ já vinha admitindo o direito ao esquecimento para casos em que os factos veiculados através da televisão, trazendo o caso descrito anteriormente do Massacre da Candelária.

Para ele, no processo relacionado com o Massacre da Candelária, tem importância indiscutível pois suscitou a discussão sobre o direito ao esquecimento como verdadeira faceta de dois direitos fundamentais, o da dignidade da pessoa humana e o direito a privacidade, mas limitando o último em aplicação a conteúdos caluniosos e difamatórios.

O Ministro coloca também a regulamentação através do Marco Civil da Internet dos direitos e deveres dos utilizadores de internet, prevendo a:

> "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" (inciso I do art. 7.º). Além disso, o legislador tratou também do próprio direito ao esquecimento, ao elencar, dentre eles, o direito à "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" (inciso X do art. 7.º).".

O Ministro Sanseverino continuou seu raciocínio suscitando que seus colegas citaram o acórdão Google Spain, e afirmou que a partir deste acórdão foi reconhecido o direito ao esquecimento em favor dos cidadãos da UE. O Ministro complementa com a citação sobre o RGPD, que prevê expressamente em seu artigo 17 o direito ao esquecimento.

Para o Ministro “a legislação brasileira, bem como o direito comparado, portanto, possuem normas que, ao meu ver, tutelam o direito do usuário/cidadão no tratamento de seus dados pessoais, não encontrando a pretensão óbice no ponto.”.

Para ele o pedido do processo em questão, não versa sobre a retirada de páginas da internet em que constem notícias sobre a suposta fraude ocorrida no concurso descrito, mas sim o reconhecimento de seu direito de evitar que pesquisas pelo nome da autora, sem qualquer outro critério que vincule a pesquisa a fraude, apresente como resultados relevantes tais notícias.

O Ministro afirma então que “na tensão que se coloca entre o direito fundamental à informação e as liberdades públicas dos cidadãos, ao meu ver, o primeiro deve ceder.”. Terminando seu voto seguindo os dois ministros anteriores para a desindexação dos resultados.

Sendo assim o Recurso Especial n.º 1660168 terminou com a seguinte ementa:

> “RECURSO ESPECIAL. DIREITO CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. 1. OMISSÃO, CONTRADIÇÃO OU OBSCURIDADE. AUSÊNCIA. 2. JULGAMENTO EXTRA PETITA. NÃO CONFIGURADO. 3. PROVEDOR DE APLICAÇÃO DE PESQUISA NA INTERNET. PROTEÇÃO A DADOS PESSOAIS. POSSIBILIDADE JURÍDICA DO PEDIDO. DESVINCULAÇÃO ENTRE NOME E RESULTADO DE PESQUISA. PECULIARIDADES FÁTICAS. CONCILIAÇÃO ENTRE O DIREITO INDIVIDUAL E O DIREITO COLETIVO À INFORMAÇÃO. 4. MULTA DIÁRIA APLICADA. VALOR INICIAL EXORBITANTE. REVISÃO EXCEPCIONAL. 5. RECURSO ESPECIAL PARCIALMENTE PROVIDO.
>
> 1. Debate-se a possibilidade de se determinar o rompimento do vínculo estabelecido por provedores de aplicação de busca na

internet entre o nome do prejudicado, utilizado como critério exclusivo de busca, e a notícia apontada nos resultados.

2. O Tribunal de origem enfrentou todas as questões postas pelas partes, decidindo nos estritos limites da demanda e declinando, de forma expressa e coerente, todos os fundamentos que formaram o livre convencimento do Juízo.

3. A jurisprudência desta Corte Superior tem entendimento reiterado no sentido de afastar a responsabilidade de buscadores da internet pelos resultados de busca apresentados, reconhecendo a impossibilidade de lhe atribuir a função de censor e impondo ao prejudicado o direcionamento de sua pretensão contra os provedores de conteúdo, responsáveis pela disponibilização do conteúdo indevido na internet. Precedentes.

4. Há, todavia, circunstâncias excecionalíssimas em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo.

5. Nessas situações excecionais, o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o facto desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca.

6. O rompimento do referido vínculo sem a exclusão da notícia compatibiliza também os interesses individual do titular dos dados pessoais e coletivo de acesso à informação, na medida em que viabiliza a localização das notícias àqueles que direcionem sua pesquisa fornecendo argumentos de pesquisa relacionados ao facto noticiado, mas não àqueles que buscam exclusivamente pelos dados pessoais do indivíduo protegido.

7. No caso concreto, passado mais de uma década desde o facto noticiado, ao se informar como critério de busca exclusivo o nome da parte recorrente, o primeiro resultado apresentado permanecia apontando link de notícia de seu possível envolvimento em facto desabonador, não comprovado, a despeito da existência de outras tantas informações posteriores a seu respeito disponíveis na rede mundial.

8. O arbitramento de multa diária deve ser revisto sempre que seu valor inicial configure manifesta desproporção, por ser irrisório ou excessivo, como é o caso dos autos.

9. Recursos especiais parcialmente providos. ACÓRDÃO Vistos, relatados e discutidos estes autos, acordam os Ministros da Terceira Turma do Superior Tribunal de Justiça, na conformidade dos votos e das notas taquigráficas a seguir, por maioria, dar parcial provimento aos recursos especiais, nos termos do voto do Sr. Ministro Marco Aurélio Bellizze, que lavrará o acórdão. Vencidos os Srs. Ministros Nancy Andrighi e Ricardo Villas Bôas Cueva. Votaram com o Sr. Ministro Marco Aurélio Bellizze (Presidente) os Srs. Ministros Paulo de Tarso Sanseverino e Moura Ribeiro.

Brasília, 08 de maio de 2018 (data do julgamento).

MINISTRO MARCO AURÉLIO BELLIZZE, Relator”

Sendo assim, pela diferença de um voto, os Ministros com votos contrários ao da Ministra instrutora sentenciaram pela primeira vez no Brasil a favor da desindexação de uma informação dos mecanismos de busca, fundamentando e indo de acordo com o Acórdão Google Spain, de 2014, e concretizando no Brasil o que na Europa já está descrito no RGPD, o reconhecimento do direito ao esquecimento como desindexação.

CONCLUSÃO

O direito ao esquecimento (ou à desindexação) surge a partir da decisão do TJUE no acórdão Google Spain ao reconhecer que os resultados apresentados pelos motores de busca são fruto de tratamento de dados pessoais. Com isso o direito ao apagamento, que fora inspirado na autodeterminação informacional e regulado a partir da Diretiva 95/46, começa a ser aplicado como um direito à desindexação exercido contra os motores de busca.

Fica claro com o advento do RGPD que o legislador europeu utilizou o termo "esquecimento" de forma porventura equivocada – e que o termo mais adequado seria desindexação – pois a redação da legislação europeia é a confirmação do que fora respondido ao tribunal espanhol na questão prejudicial do acórdão Google.

O RGPD reafirmou a possibilidade da aplicação extraterritorial da legislação europeia para a proteção de dados. Como o RGPD revogou a Diretiva 95/46, cabe agora ao TJUE, que foi questionado sobre a aplicação da desindexação no Caso da CNIL, responder à questão prejudicial tendo em conta os desenvolvimentos do novo padrão normativo, ainda que os questionamentos tenham sido feitos com base na diretiva então em vigor.

Como a proteção de dados é reconhecido como um direito fundamental na UE através da legislação europeia e da jurisprudência do TJUE, como no Acórdão Lindqvist, cabe ao TJUE reconhecer e responder a CNIL no sentido de que a aplicação da desindexação de informações nos motores de busca deve ser feita de forma global, a fim de atingir todos os domínios dos motores de busca.

O que já fora praticado pelo mesmo tribunal, ao reconhecer no Acórdão Schrems, que a partir de um país não ter a mesma proteção jusfundamental que é assegurada no território dos Estados-Membros, para o tratamento de dado, mesmo fora do território da União deve ser usado a legislação europeia ou o dado não pode ser enviado a países terceiros.

A aplicação deve ser global para proteger o direito fundamental, pois trata-se de uma aplicação da legislação a empresas que tratam dados para fins lucrativos, e que atuam

de forma global, sendo que seus endereços locais são fictícios e todos subsidiários do endereço principal, o "*.com*".

Sendo assim cabe ao TJUE assegurar, indo contrario a opinião do Advogado-Geral, como no Acórdão Google, um direito amplo e fundamental de forma global em face de empresas que atuam em todo o mundo tratando dados para o seu próprio lucro.

Cabe ressaltar que ao procurar informações em um motor de busca as informações que aparecem como resultado não necessariamente estão armazenadas no país em que é feita a pesquisa, podendo estar-se a aceder a um *data center* localizado no estrangeiro. Isto corrobora a ideia que a desindexação seja aplicada a todos os domínios.

Em relação ao Brasil, o direito ao esquecimento foi entendido primeiramente como um direito amplo e ligado à imagem das pessoas, como foi apresentado nos primeiros processos que chegaram ao STJ. Com a promulgação da Lei Geral de Proteção de Dados o legislador brasileiro se inspirou na legislação da UE e previu o direito à eliminação do dado pessoal quando a sua finalidade ou o tempo de armazenamento tenha expirado – incorporando, desta forma, o conceito de apagamento já previsto na Diretiva 95/46 e atualmente no RGPD.

O STJ, em recente decisão, consagrou o direito ao esquecimento como desindexação, tal como previsto no RGPD e decidido pelo TJUE – reconhecendo, pela primeira vez no Brasil, o direito à deslistagem ou à desassociação a uma cidadã brasileira que teve a sua vida privada prejudicada por um resultado de pesquisa apresentado no Google quando buscava seu nome.

Além disso, em votação recente no Senado Federal, foi aprovada a PEC 17/2019 tendente a instituir no Brasil, no rol do artigo 5.º da Constituição Federal, o direito fundamental à proteção de dados – o que integra também o direito à eliminação e o direito à desindexação. Essa PEC ainda precisa ser votada pela Câmara dos Deputados, mas o avanço recente na legislação e na jurisprudência mostra que o Brasil está a seguir o caminho traçado na UE para reconhecer a proteção de dados – e, no que releva para esta dissertação, o direito à desindexação – como um direito fundamental do cidadão brasileiro.

BIBLIOGRAFIA

Alessi, Stefania. Eternal Sunshine: The Right to be Forgotten in the European Union after the 2016 General Data Protection Regulation. Emory International Law Review, Volume 32, 145-171, 2017.

Assembleia Geral da ONU. Declaração Universal dos Direitos Humanos. Paris, 1948.

Bittencourt, Illa Barbosa; Veiga, Ricardo Macellaro. Direito ao Esquecimento. Revista Direito Mackenzie, v.8(n.2), 45-58, 2014

Botelho, Catarina Santos. Novo ou velho direito? – O Direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global. AB INSTANTIA, 5(7), 49-71, 2017.

BRASIL. Código Civil. Brasília, Distrito Federal, Brasil, de 10 de Janeiro de 2002.

BRASIL. Constituição (1988). Brasília, Distrito Federal, Brasil: Senado Federal.

Brougher, Jordan D.. The Right to be Forgotten: Applying European Privacy Law to American Eletronic Health Records. Indiana Health Law Review, 510-545, 2016.

Bundesverfassungsgericht (BVerfG). Volkszählungsurteil - BVerfGE 65 de 15 de dezembro de 1983.

Bundesverfassungsgericht. BVerfGE 35, 202 – Lebach, de 5 de junho de 1973. Disponível em < https://germanlawarchive.iuscomp.org/?p=62>.

Burri, Mira; Schär, Rahel. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. Journal of Information Policy, Volume 6, 479-511, 2014.

Calvão, Filipa Urbano. O Direito Fundamental à Proteção dos Dados Pessoais e a Privacidade 40 Anos Depois. Jornadas nos quarenta anos da Constituição da República Portuguesa – Impacto e Evolução, Manuel Afonso Vaz, Catarina Santos Botelho,Luís Heleno Terrinha, Pedro Coutinho (Coord.), Universidade Católica Editora, 2017.

Camargo, Coriolano Almeida; Santos, Cleórbete. Direito Digital: novas teses jurídicas. Rio de Janeiro, Lumen Juris, 2018.

Canotilho, J.J. Gomes; Moreira, Vital. Constituição da República Portuguesa Anotada: artigos 1º a 107º. Volume I, 4º edição revista. Coimbra Editora, 2007.

Castro, Caratina Sarmento e. A Jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspectivas para o direito ao esquecimento na Europa. Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos. Volume 1, Almedina, 1047 – 1070, 2016.

Castro, Catarina Sarmento e. 40 anos de "Utilização da Informática": O artigo 35.º da Constituição da República Portuguesa. e-Pública, Lisboa , v. 3, n. 3, p. 42-66,

dez. 2016 . Disponível em <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S2183-184X2016000300004&lng=pt&nrm=iso>.

CNIL. Right to Delisting: Google Informal Appeal Rejected, de 21 de setembro de 2015, disponível em <https://www.cnil.fr/fr/node/15814>.

Cofone, Ignacio. Google v. Spain: A Right to Be Forgotten? Chicago-Kent Journal of International and Comparative Law, Volume 15(No. 1), 1 – 11, 2015.

Commission Nationale de l'Informatique et des Libertés. Decision No. 2016-054 - Restricted Committee issuing Google Inc. with a financial penalty, de 10 de março de 2016.

Commission Nationale de l'Informatique et des Libertés. Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X, 10 de março de 2016.

Conselho da Europa, Comité de Ministros (1973), Resolução (73) relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor privado, de 26 de setembro de 1973;

Conselho da Europa, Comité de Ministros (1974), Resolução (74) relativa à proteção da privacidade e das pessoas singulares perante os bancos eletrónicos de dados no setor público, 20 de Setembro de 1974.

Conselho da Europa. Alterações à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (STCE n.º 108) que permitem a adesão das Comunidades Europeias, adotadas pelo Comité de Ministros em Estrasburgo, em 15 de junho de 1999; artigo 23.º, n.º 2, da Convenção 108 na redação em vigor.

Conselho da Europa. Convenção Europeia dos Direitos do Homem, STCE n.º. 005, 1950

Conselho da Europa. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, Conselho da Europa, STCE n.º 108, 1981.

Conselho da Europa. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo, 2014.

Conselho da Europa. Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, STCE n.º 181, 2001.

Corrado, John. Not Forgetting Just Obscuring: American and European Attempts to Maintain Privacy in the Digital Age. Cardozo Journal of Internactional and Comparative Law, Volume 1, 307 – 337, 2018.

Cuijpers, Colette; Purtova, Nadezhda; Kosta, Eleni. Data Protection Reform and the Internet: The Draft Data Protection Regulation. Tilburg Law School Research Paper No. 03/2014, 2014.

Curtiss, Tiffany. Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies. Washington Journal of Law, Technology & Arts, 97-121, 2016.

Daugirdas, Kristina; Mortensen, Julian Davis. European Union and United States Conclude Agreement to Regulate Transatlantic Personal Data Transfers. American Journal of International Law, Volume 110, Issue 2, 360-368, 2016.

De Alcantara, Larissa Kakizaki. Big Data e Internet das Coisas: Desafios de Privacidade e da Proteção de Dados no Direito Digital. São Paulo: Bok2, 2017.

Demchak, Chris; Dombrowski, Peter. Cyber Westphalia: Asserting State Prerogatives in Cyberspace. Georgetown Journal of International Affairs, 29-38, 2013.

Dias, Felipe da Veiga; Bolesina, Iuri. Direito à Proteção de Dados Pessoais no Brasil e os Traços Centrais de uma Autoridade Local de Proteção. E-Civitas - Revista Científica do Curso de Direito do UNIBH, Volume X (número 1), 2017.

Donega, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. Espaço Jurídico Journal of Law, v. 12(n. 2), 91 – 108, 2011.

Eoyang, Mieke. Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance. Journal of National Secutity Law & Policy, 259 – 281, 2017.

Fleischer, Peter. Reflecting on the Right to be Forgotten. Google Blog. Disponível em <https://blog.google/topics/google-europe/reflecting-right-be-forgotten>.

Frosio, Giancarlo F.. The Right to be Forgotten: Much ado about nothing. Colorado Techlogy Law Journal, 308 – 336, 2017

Gilbert, Francoise. GDPR: EU General Data Protection Regulation. Orange County Lawyer, Volume 60, 23-26, 2018.

Gömann, Merlin. The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement. Common Market Law Review, Volume 54(Issue 2), 567-590, 2017.

Google. Transparency Report - Perguntas Frequentes sobre as solicitações de remoção da pesquisa em conformidade com a privacidade europeia. Disponível em <https://support.google.com/transparencyreport/answer/7347822?hl=pt-BR>.

Google. Transparency Report - Remoções da pesquisa em cumprimento da legislação europeia sobre privacidade. Disponível em <https://transparencyreport.google.com/eu-privacy/overview>.

Google. Transparency Report - Solicitações de remoções da pesquisa em conformidade com a privacidade europeia. Disponível em <https://www.google.com/transparencyreport/removals/europeprivacy/>.

Grupo de Trabalho do Artigo 29.º. 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" C-131/12, 2014.

Hall, Holly Kathleen. Restoring Dignity and Harmony to United States-European Union Data Protection Regulation. Communication Law and Policy, Volume 23, 125-157, 2018.

Justiça Federal. Enunciados Aprovados na VI Jornada de Direito Civil. 2017. Disponível em <http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/enunciados-vi-jornada/view>.

Keller, Daphne. The Center for Internet and Society. Stanford Law School, 2015. Disponível em <http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law>.

Kitain, Jessica. Beware of Wearables: Protecting Privacy in a Data-Collecting World. Drexel Law Review Online, 1 – 29, 2016.

Kuhn, McKenzie L.. 147 Million Social Security Numbers for Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches. Iowa Law Review, Volume 104, 418-445, 2018.

Lode, Sarah L.. "You Have the Data" . . . The Writ of Habeas Data and other Data Protection Rights: Is the United States Falling Behind? Indiana Law Journal & Supplement, Volume 94, 41-63, 2018.

Martial-Braz, Nathalie. O direito das pessoas interessadas no tratamento de dados pessoais: anotações da situação na França e na Europa. Revista de Direito, Estado e Telecomunicações, v. 10(n. 1), 85-108, 2018.

Mayer-Schönberger, Viktor. Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press; Edição: Revised ed. for Kindle, 25 de julho de 2011.

McAllister, Craig. What About Small Businesses? The GDPR and its Consequences for Small, U.S.-Based Companies. Brooklyn Journal of Corporate, Financial & Commercial Law, 187 – 211, 2017.

Mirada, Jorge; Medeiros, Ruy. Constituição Portuguesa Anotada. Volume I, 2º ed., Revista – Lisboa: Universidade Católica Editora, 2017.

Mitchell-Rekrut, Cooper. Search Engine Liability under the Libe Data Regulation Proposal: Interpreting Third Party Responsibilities as Informed by Google Spain. Georgetown Journal of International Law, Volume 45, 2014.

Moniz, Graça Canto. Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD. UNIO - EU Law Journal, Vol. 4(Nº. 2), 119 – 131, 2018.

Moreira, Poliana Bozégia, Direito ao Esquecimento. Revista de Direito da Universidade Federal de Viçosa, Vol. 7(nº 2), 293 – 317, 2015.

Nunziato, Dawn Carla. The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten. University of Pennsylvania Journal of International Law, Volume 39, 1014 – 1064, 2018.

O Direito Pensando. Conheça a nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais. Disponível em <http://www.pensando.mj.gov.br/>

Parlamento Europeu e do Conselho. Directiva 95/46/CE. Luxemburgo, 24 de outubro de 1995. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>.

Parlamento Europeu e o Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Disponível em < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>.

Peguera, Miquel. The Shaky Ground of the Right to Be Delisted. Vanderbilt Journal of Entertainment and Technology Law, Volume 18, Issue 3, 509-561, 2016.

Prorok, Christine. “The Right to be Forgotten” in the EU’s General Data Protection Regulation. The Michigan Journal of International Law. The Michigan Journal of International Law, 2016

Safari, Beata A. Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. Seton Hall Law Review, Volume 47, 809-848, 2017.

Senado Federal. Proposta de Emenda à Constituição N° 17. Senador Eduardo Gomes (MDB/TO), de 21 de fevereiro de 2019.

Shapiro-Barr, Jeremy. The GDPR's Impact in the U.S.: Considerations for the U.S. Health Lawyer. Journal of Health & Life Sciences Law, Vol.12 (No. 1), 2018.

Silveira, Alessandra. Direitos humanos fundamentais originariamente protegidos offline mas exercidos online – e a recíproca, é verdadeira?. Direito & solidariedade, Elisaide Trevisam/Lívia Gaigher Bósio Campello (coords.), Editora Juruá, Curitiba, 2017

Silveira, Alessandra; Marques, João. Do Direito a Estar Só ao Direito ao Esquecimento. Considerações Sobre a Proteção de Dados Pessoais Informatizados no Direito da União Europeia: Sentido, Evolução e Reforma Legislativa. Revista da Faculdade de Direito - UFPR, Vol. 61(n.º 3), 91 – 118, 2016.

Silvestre, Gilberto Fachetti; Borges, Carolina Biazatti; Benevides, Nauani Schades. The Procedural Protection of Data De-Indexing in Internet Search Engines: The

Effectiveness in Brazil of the So-Called “Right To Be Forgotten” Against Media Companies. Revista Jurídica, [S.l.], v. 1, n. 54, 25 - 50, mar. 2019.

Souza, Bernardo de Azevedo e. Direito, Tecnologia e Práticas Punitivas. Porto Alegre: Canal Ciências Criminais, 2016.

Superior Tribunal de Justiça. Recurso Especial nº 1.334.097, de 22 de maio de 2013.

Swire, Peter; Kennedy-Mayo, DeBrae. How Both the EU and the U.S. are "Stricter" than each other for the Privacy of Government Requests for Information. Emory Law Journal, Volume 66, 617-667, 2017.

Taylor, Rachel C.. Intelligence-Sharing Agreements & International Data Protection: Avoiding a Global Surveillance State. Washington University Global Studies Law Review, 731-759, 2018.

The City University of New York. Maximilian Schrems, Initiator of Europe v. Facebook. The US v. Europe v. Facebook: Digital Divisions?. New York, 2016.

Tribunal de Justiça da União Europeia. Acórdão C-131/12 - Conclusões do Advogado-Geral Niilo Jääskinen, 25 de junho de 2013.

Tribunal de Justiça da União Europeia. Acórdão C-131/12 - Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, 2014.

Tribunal de Justiça da União Europeia. Acórdão C-362/14 - Maximillian Schrems contra Data Protection Commissioner, de 06 de outubro de 2015.

Tribunal de Justiça da União Europeia. Acórdão C-507/17 - Request for a preliminary ruling from the Conseil d’État (France) lodged on 21 August 2017 — Google Inc. v Commission nationale de l’informatique et des libertés (CNIL), 2017.

Tribunal de Justiça da União Europeia. Acordão Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González – Processo C-131/12, 13 de maio de 2014. Disponível em < http://curia.europa.eu/juris/document/document.jsf?text=&docid=153853&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=8125412>.

Tribunal de Justiça da União Europeia. Acórdão Lindqvist, de 6 de novembro de 2003, proc. C-101/01. Disponível em < https://curia.europa.eu/jcms/jcms/j_6/pt/>.

Tribunal de Justiça da União Europeia. Caso C-136/17 - Conclusions De L’avocat Général M. Maciej Szpunar, de 10 de janeiro de 2019.

Tribunal de Justiça da União Europeia. Comunicado de Imprensa n.º 2/19. Luxemburgo,10 de janeiro de 2019. Disponível em <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002pt.pdf>

Tribunal de Justiça da União Europeia. O advogado-geral M. Szpunar propõe ao Tribunal de Justiça que limite à escala da União Europeia a supressão de hiperligações a

que os operadores de motores de busca são obrigados a proceder, de 10 de janeiro de 2019.

U.S.-EU Safe Harbor Framework. Testimony of Edward M. Dean, Deputy Assistant Secretary for Services, International Trade Administration, U.S. Department of Commerce, 2015. Disponível em < https://docs.house.gov/meetings/IF/IF16/20151103/104148/HHRG-114-IF16-20151103-SD012.pdf>.

Van Alsenoy, Brendan; Koekkoek, Marieke. Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'. International Data Privacy Law, Volume 5(Issue 2), 105–120, 2015.

Veronese, Alexandre; Melo, Noemy. O Projeto de Lei 5.276/2016 em contraste com o novo regulamento Europeu (2016/679 UE). Revista de Direito Civil Contemporâneo, Vol. 14, 71-99, 2018.

Warren, Samuel D.; Brandeis, Louis D.. The Right to Privacy. Harvard Law Review, Vol. IV (Nº. 5), 15 de Dezembro de 1890. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

Zanon, João Carlos. Direito à proteção dos dados pessoais. Revista dos Tribunais, 2013.