**DEPARTAMENTO DE DIREITO**

**MESTRADO EM DIREITO**

**ESPECIALIDADE EM CIÊNCIAS JURÍDICAS**

**UNIVERSIDADE AUTÓNOMA DE LISBOA**

**"LUÍS DE CAMÕES"**

# AS NOVAS TECNOLOGIAS COMO FATORES DE INIBIÇÃO À PRIVACIDADE

Dissertação para a obtenção do grau de Mestre em Direito

Autor: José Carlos Viana Mendes Neto

Orientador: Prof. Doutor Armando Reis Dias Ramos

Número do candidato: 20151896

**Junho de 2021**

**Lisboa**

## AGRADECIMENTOS

Em primeiro lugar agradeço a Deus pela saúde e proteção nesses tempos difíceis.

Agradeço aos meus pais que ajudaram financeiramente para a conclusão desse projeto.

Ao meu falecido avô, Dr. José Carlos Viana Mendes que sempre me perguntava o dia em que seria mestre.

Minhas tias, Solange e Alessandra Mendes que desde criança me deram e me dão o suporte para chegar até onde estou.

Ao meu orientador Professor Doutor Armando Reis Dias Ramos que sempre foi solícito e atencioso em me orientar da melhor forma possível.

À Universidade Autónoma de Lisboa e a todos os que fazem parte da Instituição, pelo acolhimento quando estive em Portugal.

## RESUMO

A tecnologia quase sempre desempenha um papel importante na sociedade e cada vez mais está adentrando a vida das pessoas de tal forma que os recursos tecnológicos se tornaram quase que indispensáveis para o bom andamento das atividades cotidianas sociais. A era tecnológica nos trouxe facilidades e benefícios incontáveis e são facilmente perceptíveis e presentes no cotidiano das pessoas. No que diz respeito ao direito à privacidade, compreende-se que este seria pertencente ao gênero classificado como direitos fundamentais e está alicerçado juridicamente na Constituição brasileira, bem como na Constituição portuguesa e nas leis da União Europeia. A presente pesquisa objetivou analisar a influência da tecnologia e o direito à privacidade: autoexposição da vida pessoal e íntima dos usuários. Tratou-se de um estudo de revisão de literatura, nos quais foram utilizadas as bases de dados: Artigos jurídicos publicados, dissertações e teses em pós-graduação em direito, livros de juristas notáveis e o Google Scholar. Mediante o cruzamento dos descritores: Direito à Privacidade. Videovigilância. Tecnologia. Titulares de dados. Foram usadas publicações dos últimos anos dos quais estivessem em inglês, português ou espanhol. Com o advento da videovigilância e da *internet*, cada vez mais se percebe a necessidade vital de normatizações que possam atuar de maneira a defender esse direito, tendo em vista que o fluxo de informações é armazenado e transmitido numa velocidade de grande magnitude tal que, pode ocasionar diversos conflitos entre a supressão da privacidade e imagem. Os direitos a personalidade são intransmissíveis e irrenunciáveis e é comum cada vez mais pessoas as pessoas fiquem vulneráveis fazendo uso dessas novas tecnologias. O Direito Digital vem então equilibrar, nesse caso, o direito à segurança, o direito à informação e o direito à privacidade, por mais difícil que seja.



**Palavras-chave:** Direito à Privacidade. Videovigilância. *Internet*. Tecnologia. Titulares de dados.

## ABSTRACT

Technology almost always plays an important role in society and is increasingly entering people's lives in such a way that technological resources have become almost indispensable for the smooth running of everyday social activities. The technological age has brought us countless facilities and benefits and they are easily noticeable and present in people's daily lives. With regard to the right to privacy, it is understood that this would belong to the genre classified as fundamental rights and is legally based on the Brazilian Constitution, as well as on the Portuguese Constitution and on the laws of the European Union. This research aimed to analyze the influence of technology and the right to privacy: self-exposure of users' personal and intimate lives. It was a literature review study, in which the following databases were used: Published legal articles, dissertations and postgraduate theses in law, books by notable jurists and Google Scholar. By crossing the descriptors: Right to Privacy. Video surveillance. Technology. Data Holders. Publications from recent years were used, in English, Portuguese or Spanish. With the advent of video surveillance and the internet, the vital need for regulations that can act in a way to defend this right is increasingly perceived, given that the flow of information is stored and transmitted at such a high speed that it can cause several conflicts between deletion of privacy and image. Personality rights are non-transferable and non-waivable and it is common for more and more people to gain by making use of these new technologies. The Digital Law then comes to balance, in this case, the right to security, the right to information and the right to privacy, however difficult it may be.



**Keywords**: Right to Privacy. Video surveillance. Internet. Technology. Data subjects.

## ÍNDICE

## 1. - INTRODUÇÃO

A tecnologia quase sempre desempenha um papel importante na sociedade e cada vez mais está adentrando a vida das pessoas de tal forma que os recursos tecnológicos se tornaram quase que indispensáveis para o bom andamento das atividades cotidianas sociais. Diante desse contexto já se discute acerca da existência de uma nova geração de direitos e liberdades, os recursos da tecnologia bem como o surgimento da *internet* estariam enquadrados. Esses sendo vistos como direitos de quarta geração, onde seriam inseridos aqueles direitos no quais fazem referência ao campo da manipulação genética, da bioética e novas tecnologias relacionadas ao processo da comunicação (PAESANI, 2014).

A era tecnológica nos trouxe facilidades e benefícios incontáveis e são facilmente perceptíveis e presentes no cotidiano das pessoas. O uso de dispositivos móveis (*notebooks*, *tabletes*) dentre outros aparatos tecnológicos, só evidenciam a imparável cultura da informação, onde a fluidez e rapidez são as suas principais características. Nessa conjuntura, surge a discussão sobre a utilidade e o propósito do uso exacerbado de instrumentos tecnológicos e as consequências da transmissão da informação. Mesmo assim, é notório a facilidade do acesso a qualquer tipo de conteúdo, o que traz muitas vantagens para a sociedade, principalmente pela quebra de fronteiras temporais e espaciais, garantindo comodidade aos usuários. (CARVALHO; PEDRINI, 2019).

Há também um crescimento exponencial do uso de sistemas de videovigilância, onde prevê tecnologia suficiente para captura de dados, imagens e sons de transeuntes em espaços públicos, fazendo com que esses dados sejam tratados por outras pessoas com finalidades definidas em lei.

Trazendo essas informações para a temática da privacidade com que essas informações são manuseadas/tratadas, bem como na liberdade de expressão em volta as questões correlacionadas a informação e a difusão da mesma, a privacidade acaba sendo vista atualmente como algo que está diretamente relacionado quatro categorias: direito de ser deixado só; resguardo contra interferências alheias; Segredo ou sigilo; Controle sobre informações e dados pessoais (LEONARDI, 2012).

Compreende-se que o direito à privacidade seria pertencente ao gênero classificado como direitos fundamentais e está alicerçado juridicamente na CRFB/88, no art. 5°, inciso X, e na Constituição da República Portuguesa em seu artigo 26º, nº 1.

No âmbito da sistematização constitucional, dar-se a garantia não apenas ao direito

quanto à intimidade, vida privada e a honra, colorados do direito à privacidade, mas também ao que diz respeito a proteção devido a situações que possam violar moralmente ou materialmente o indivíduo.

Segundo Branco e Mendes (2015) no contexto do direito à privacidade está o controle de informações e conceitos sobre si mesmo. Sendo assim o núcleo básico do que se refere ao direto a vida privada relaciona-se ao controle de informações a respeito de seu próprio ser. Para Silva (2010), o que pode violar esse tipo de direito não está relacionado apenas a aspectos íntimos do indivíduo, mas também se relaciona a outros setores da vida humana, tais como aspectos sociais, profissionais, comerciais etc. Destaca-se que os direitos no que concerne à privacidade vem ganhando novos rumos atualmente. De acordo com Paesani (2014, p. 43), "direito reconhecido ao indivíduo de exercer o controle sobre o uso dos próprios dados pessoais inseridos num arquivo eletrônico".

Partindo dessa contextualização a presente pesquisa objetivou analisar se a privacidade ainda é protegida com o advento das novas tecnologias, principalmente quanto aos sistemas de videovigilância e o uso da *internet.* A privacidade está sendo esquecida ou apenas está se adequando às novas tecnologias? A legislação de Portugal e Brasil está acompanhando as mudanças sociais?

O estudo em questão foi realizado abordando o uso do sistema de videovigilência e o uso da *internet* em relação aos direitos à personalidade, em especial o direito à vida privada e a imagem, traçando as principais leis, opiniões de juristas e casos concretos no Brasil, Portugal e no mundo. No decorrer dos capítulos seguintes abordou-se diversos fatores que fazem com que o direito a personalidade seja suprimido, em especial o direito à imagem, a privacidade e o direito ao esquecimento.

Tratou-se de um estudo de revisão de literatura, nos quais foram utilizadas as bases de dados: Livros de juristas referente aos assuntos, artigos, monografias e dissertações e o Google Scholar. Mediante o cruzamento dos descritores: Direito à Privacidade. Videovigilância. Uso da *Internet*. Tecnologia. Titulares de dados. Foram usadas publicações dos últimos anos das quais estivessem em inglês, português ou espanhol. Publicações essas que estivesses de acordo com os objetivos proposto pelo estudo em questão.

## 2. - VIDEOVIGILÂNCIA

### 2.1 - Videovigilância em Portugal

Portugal é acobertado de leis que cercam e regulam o uso de câmeras em determinados locais, sejam públicos ou privados além dos casos que são obrigatórios a instalação desse meio tecnológico, como farmácias, postos de combustíveis, sociedades financeiras, instituições crediárias, lojas de exposição ou compra de metais preciosos, dentre outros sítios em que a lei alcança como forma de limitar atividades infratoras, bem como proteger bens e pessoas. Serviços de segurança privada e autoproteção, forças de segurança nos locais públicos, Estradas de Portugal (EP), concessionárias rodoviárias e serviço de taxi são respaldadas em lei[1] o uso da videovigilância.

Com o objetivo de facilitar a solução de crimes ou mesmo impedir a prática, a Lei nº 9/2012 que assegura a utilização dos meios de gravação de imagem e seu tratamento pela força Policial de Segurança Pública e a Guarda Nacional, em seu artigo 2º os autoriza apenas se a finalidade for proteger instalações com interesse para defesa ou segurança, proteger edifícios e instalações públicas bem como seus acessos, proteger a segurança das pessoas e bens, públicos ou privados, e prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência, proteger e reprimir infrações rodoviárias, prevenir atos terroristas, proteger áreas florestais e prevenir incêndios florestais.

O tratamento do material gravado tanto em áudio quanto em imagem é de competência da força de segurança responsável pela área de sua abrangência, conforme o disposto na Lei nº 67/98 de acordo com o nº 2 do artigo 2º da Lei nº 1/2005 que foi atualizada pela Lei nº 9/2012.

A instalação de câmeras fixas também é regulada pela lei, abrangendo equipamentos portáteis nos termos do nº 1 do artigo 7º da Lei nº 1/2005, atualizada pela Lei nº 9/2012, depende de autorização prévia do membro do Governo que é responsável pela força ou serviço de segurança, conforme artigo 3º, nº 1 e depende de parecer da Comissão Nacional de Proteção de Dados (CNPD) em até 60 dias da data do recebimento do pedido, conforme disposto no nº 2 do mesmo artigo.

Este pedido é valido apenas se a autoridade máxima competente da força nacional ou o presidente da câmara municipal o fizerem e devem ser observados para tanto o artigo 5º e

[1] Lei n.º 34/2013 / Lei n.º 9/2012/ Lei n.º 51/2006 / Lei n.º 33/2007.

alíneas da mesma lei, portanto deve constar no pedido os elementos como: os locais públicos de observação das câmeras, as características técnicas do equipamento utilizado, a identificação dos agentes que irão proceder o tratamento e conservação do dados, quando não responsáveis pelo sistema, as motivações para a existência da necessidade da instalação do sistema de vigilância por vídeo, os procedimentos de informação aos cidadãos sobre a existência do sistema na localidade, os mecanismos tendentes para assegurar o uso correto dos dados registrado, o período de conservação dos dados, com respeito pelos princípios da adequação e da proporcionalidade, face ao fim a que os mesmos se destinam e o comprovativo de aprovação, de capacidade ou de garantia de financiamento da instalação do equipamento utilizado e das respetivas despesas de manutenção.

Ainda no artigo 5º, o nº 3 preleciona sobre a decisão de autorização para uso que deverá constar os locais públicos objetos de observação por câmeras, as limitações e condições de uso do sistema, a proibição de captação de áudio, salvo quando ocorra perigo concreto para segurança de bens e pessoas, o espaço físico que será sujeito à gravação, bem como os requisitos do equipamento e, por fim, a duração da autorização que será de no máximo 2 anos suscetível de renovação por iguais períodos, mediante comprovação da manutenção dos fundamentos invocados para a sua concessão ou da existência de novos fundamentos, conforme nº 5 do artigo em análise. A autorização também poderá sofrer revogação ou suspensão, caso haja decisão fundamentada pelo poder público, conforme nº 6.

Quanto aos requisitos e características mínimas necessárias para o uso dos equipamentos de videovigilância, o membro do Governo responsável pela administração interna as definirá, consultada a CNPD. O artigo 3º, nº 7, a CNPD no exercício de suas atribuições poderá formular recomendações e dispensar expressamente a existência de certas medidas de segurança, garantido que se mostre o respeito pelos direitos, liberdades e garantias dos titulares dos dados. Os princípios da proporcionalidade, idoneidade/adequação são observados, disposto nº 1 e 2 do artigo 7º, no tocante a conservação, utilização e registro de imagens ou sons, para manutenção de ordem pública, prevenção de crimes e a manutenção da segurança (UNIÃO EUROPEIA, 2016).

Da mesma forma o nº 3 consta a preocupação caso direitos pessoais sejam atingidos. Sistemas de videovigilância que estejam em desacordo com o artigo 7º, nº 6 e 7 serão vedados, pois é expressamente proibido quando imagens de interiores de casas e edifícios habitáveis são gravadas, salvo com o consentimento do proprietário, e que de alguma forma esteja infringindo o direito à vida privada ou intimidade das pessoas, por gravação de áudio. Caso em um desses casos seja violado, seja por captação de imagem ou áudio, os dados

deverão ser imediatamente apagados pelo usuário do sistema.

Em alguns casos excepcionais, quando existe urgência pela ameaça à segurança, à ordem pública e à defesa do Estado, poderá o dirigente da força estatal fundamentar que se proceda a instalação de câmeras de vídeo, sem prejuízo de autorização no prazo de 72 horas, conforme artigo 7º, nº 5. O responsável do governo que tutela serviço relacionados à segurança e força deve ser comunicado imediatamente. Nesse contexto, caso a gravação flagre algum delito cometido, a força de segurança competente em administrar o uso dos recursos de vídeo ou áudio, deverá fazer a auto notícia, remetendo as provas ao Ministério Público no prazo mais rápido possível ou no máximo em até 72 horas, conforme artigo 8º, nº 1. Em casos que o prazo em questão se estingue, a participação dos fatos poderá ser feita eletrônica ou verbalmente, expedindo-se o mais rápido possível. O Ministério Público deverá ser comunicado quando houver decisão autorizativa na utilização do sistema de videovigilência e decisão de urgência de instalação, conforme artigo 8º, nº 3.

Quanto as gravações, deverão ser conservadas no período máximo de 30 dias a partir de dia que foram capturadas, observado o sigilo por quem esteja com o acesso sob pena de responsabilização criminal, conforme artigo 9º, nº 1 e 2. Interessados que aparecerem em gravações ou tenham sua voz por elas captadas, podem requerer o apagamento dos dados armazenados, salvo quando tais dados sejam relevantes para investigação criminal, ou constituírem perigo para a defesa do Estado ou segurança pública, ou caracterizarem fatos que ofereçam ameaça à direitos de terceiros, conforme preleciona o artigo 10, nº 1 e 2. A força de segurança ou agentes competentes para o manuseio dos dados colhidos do sistema de videovigilância deverão seguir os princípios pertencentes da Lei nº 9/2012, sob pena de responsabilidade criminal.

O artigo 13º da referida lei, traz questões à título de regime especial a utilização de câmeras para controle rodoviário e proteção florestal, tendo em vista prevenir infrações nas estradas portuguesas, bem como alertar possíveis focos de incêndio em áreas de preservação, autorizado o uso pelas forças de segurança além de gravação em tempo real e sistemas de localização via satélite. Concessionárias rodoviárias também dispõem de sistemas de localização para melhor eficaz da gestão viária. A referida autorização trouxe facilidade na fiscalização das autoridades judiciárias e forças de segurança e deverão ser utilizados de acordo com os princípios relativos à proteção de dados pessoais e seu tratamento, de forma a assegurar, conforme nº 2 do artigo 13º e alíneas da Lei nº 9/2012.

A decisão que autoriza o uso do sistema deverá ser crivada pela CNPD e pela Autoridade Nacional da Proteção Civil, de acordo com o artigo 15º, nº 5, alíneas “a” e “b”.

Em conjunto com a referida lei em análise, o RGPD também ratifica preceitos da revogada Lei nº 67/98, e os coloca de maneira mais atual e eficaz perante as novas tecnologias. Cita-se, portanto, o artigo 23º do Regulamento 2016/679, que trouxe expressamente limitações, através de medida legislativa, aos direitos do titular de dados que são: direito à transparência das informações, das comunicações e das regras para exercício dos direitos, direito à informação e acesso aos dados pessoais, direito à retificação e apagamento e o direito de oposição e decisões individuais automatizadas.

Percebe-se então a ratificação legal que o Regulamento tomou para si da Lei nº 9/2012, estabelecendo claramente limites ao direito do titular dos dados quando se tratar de matérias relacionadas à segurança pública, à defesa, à segurança do Estado, à defesa dos processos judiciais, dentre outras restrições importantes que inevitavelmente transpõem, em alguma medida, direitos à privacidade.

Portanto, é certo que a legislação atual se preocupa de modo incisivo com a questão da videovigilância e eventuais conflitos jurídicos, possibilitando ao titular dos dados que foram capturados, o passo a passo para pleitear os direitos estabelecidos no ordenamento jurídico, principalmente os direitos à imagem, à intimidade e à vida privada.

### 2.2 - A instalação de equipamentos em Portugal

Conforme já explanado, a instalação da videovigilância no espaço público português é um grande aliado no combate ao crime e prevenção de acidentes, possuindo amplo regimento legal. Atos terroristas, monitoramento para segurança de pessoas e bens também se enquadram a favor do uso desse tipo de tecnologia. Portanto, a prática do sistema em determinadas regiões portuguesas pelas forças de segurança (PSP e GNR) está ficando cada vez mais comum, tendo em vista os preceitos norteadores previsto na Lei nº 9/2012.

Ainda assim, percebe-se argumentos contrários à utilização do sistema, tendo em vista a possível quebra de princípios fundamentais e a desconfiança no tratamento de dados pelas forças de segurança, mesmo com a atualização da lei. Como explanado anteriormente, a norma legal estabelece diversas regras e informações no que diz respeito aos limites do tratamento de dados, além de informar de maneira clara os procedimentos cabíveis aos titulares dos dados, caso requeiram o acesso. Será possível encontrar um ponto de equilíbrio entre a defesa do direito à privacidade e a prevenção de crimes e segurança de bens e pessoas?

A tarefa do Estado é garantir uma série de direitos, e ambos estão aqui inseridos. O direito à privacidade e a segurança compõe uma balança que para uns, um lado pende mais, e

para outros, ambos os lados podem ter a mesma medida. As leis, portanto, têm o papel garantidor para a sociedade, visto que sem elas, não se pode haver ordem. É importante que a norma seja atualizada sempre que possível tendo em vista as inúmeras facetas tecnológicas que todos os anos facilitam a vida dos cidadãos.

O uso do sistema de videovigilância, quando observado os princípios constantes na lei, notadamente aumenta a sensação de segurança das pessoas, em especial em zonas com maior índice de criminalidade ou maiores risco de acidentes, fazendo com que circulem livres, sem o receio de assaltos, furtos, agressões etc. Da mesma forma, permite o tratamento das imagens capturadas para prevenir e detectar a prática do ilícito, bem como a identificação do autor de forma clara e objetiva, tomando medidas cabíveis e eficazes de maneira rápida para melhor andamento do processo judicial, impossibilitando dados maiores à vítima. Conforme visto, a auto de notícia é concretizado de forma mais célere, pois as provas já estarão em mãos do OPC para prosseguimento da fase de inquisitória, instrução e julgamento.

A autorização das forças de segurança para o uso do sistema é o melhor instrumento de trabalho relacionado ao controle social, pois além da agilidade, barateia os serviços de envio de meios para a ocorrência, sendo assim vantajoso ao Estado. Além do controle da criminalidade, proporciona o monitoramento em estradas portuguesas e áreas de preservação contra acidentes e incêndios, resguardando direitos de propriedade e integridade física.

### 2.3 - Confronto com direitos, liberdades e garantias

O conceito da videovigilância abrange de forma técnica um sistema de controle de imagens e/ou sons captados por câmeras durante um determinado período de tempo e em determinada área. Segundo *The Police Fundation* (2014), é um sistema de câmeras posicionadas em locais estratégicos para o monitoramento de atividades em lugares predeterminados. O que há em comum nesses dois conceitos é a capacidade de transmissão ou gravação de áudio e/ou imagem em tempo real ou não, para presente ou posterior análise em salas com pessoas especializadas. Essas características demonstram facilidade dos agentes estatais em controlar, fiscalizar, garantir segurança ou gerir melhor eventos de qualquer tipo.

Segundo Bacelar Gouveia (2016, p. 357), os direitos fundamentais são “posições jurídicas ativas das pessoas integradas no Estado-Sociedade, exercidas por contraposição ao Estado - Poder, positivadas no texto constitucional”. Portanto são posições jurídicas sagradas que deverão ser garantidas, respeitadas e protegidas contra qualquer ameaça, seja do Estado, pessoas jurídicas privadas ou civis.

A Constituição Portuguesa preleciona no capítulo I, título II uma série de direitos, liberdades e garantias, previstos nos artigos 24º ao 79º. O direito à liberdade e a segurança está impresso no artigo 27, nº 1 e o direito à intimidade e vida privada no artigo 26º, nº 1. À nível internacional, tem-se a Declaração Universal dos Direitos do Homem que preleciona no artigo 12º o direito à intimidade e a vida privada, a Convenção Europeia dos Direitos do Homem afirma em seu artigo 8º o direito ao respeito da vida íntima e familiar, e o Pacto Internacional de Direitos Civis e Políticos, no mesmo sentido, no artigo 17º.

À nível da República Portuguesa, a Constituição estabelece no artigo 26º, nº 1, e artigo 34º e 35º os direitos relativos à inviolabilidade domiciliar, de correspondência e proteção dos dados pessoais. O Código Penal também ratificou em seus artigos 190º a 198º. O direito de personalidade está no Código Civil em seu artigo 80º e conforme as palavras de David Festas (2004, s/p) "pode ser visto a nível estrutural como o direito de impedir o acesso a informações relativas à vida privada e de impedir a divulgação dessas mesmas informações". Ainda na Declaração Universal dos Direitos do Homem tem-se o direito relativos à liberdade nos artigos 1º, 3º, 9º, 13º, 18º, 19º e 20º, no Pacto Internacional de Direitos Civis e Políticos nos artigos 9º e 14º e na Convenção Europeia dos Direitos do Homem no artigo 5º.

No Estado português o direito à liberdade anda de mãos dadas com o direito à segurança e se concretiza nos artigos 27º, nº 1 e 3 da Constituição. Os artigos 28º, 29º, 30º, 31º, 32º e 33º proíbe a prisão arbitrária por qualquer força de segurança, salvo quando há condenação criminal. A legislação portuguesa aborda as possibilidades de prisão quando envolver flagrante delito, prisão preventiva, condenação criminal, medidas protetivas ao menor infrator e internação aos portadores de doenças psíquicas, nos termos da Lei penal e processual penal. Esses casos serão admitidos após decisão judicial ou autoridade pública, observados os princípios da proporcionalidade e igualdade sendo garantido aos cidadãos recursos à prisão manifestamente ilegal.

O direito à imagem é também previsto na Constituição Portuguesa no artigo 26º, nº 1 e o direito à personalidade, previsto no Código Civil no artigo 79º, nº1 e no Código Penal no artigo 199º. Portanto, visa proteger de abusos as pessoas que tenham sua imagem veiculada de maneira indevida nos meios de comércio ou exposta sem a sua autorização. Conforme nº 2 do 79º, "não é necessário o consentimento da pessoa retratada quando assim o justifiquem [...] exigências de polícia ou de justiça, [...] ou quando a reprodução da imagem vier enquadrada na de lugares públicos ou de factos de interesse público ou que hajam decorrido publicamente" (DECRETO-LEI n.º 47344, 1966, s/p).

Para Cordeiro (2016, p. 194) "a imagem permite a imediata identificação de uma

pessoa de que se trate. O destino que se dê à imagem é, de certo modo, um tratamento dado à própria pessoa. A imagem faz, assim, a sua aparição no palco dos bens de personalidade [...] proteger a imagem [...] equivale a tutelar a intimidade e a tranquilidade de cada um".

A mitigação dos direitos mencionados acima, ou seja, direito à vida privada, à liberdade e à imagem, se torna factual ao analisar outros direitos que da mesma forma são garantidos. Mais uma vez o Declaração Universal dos Direitos Humanos (1948, s/p) afirma em seu artigo 3º, o direito à segurança pessoal, portanto "todas as pessoas têm direito à vida, à liberdade e à segurança pessoal" e o artigo 5º da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. A Carta Maior portuguesa em seu artigo 27º, nº 1, garante o direito à liberdade como já explanado nos parágrafos anteriores.

Porém, é razoável pensar em liberdade quando os cidadãos agem de forma livre, segura e sabem que desfrutam da sensação de segurança, sem medo ou receio de sofrer ameaça por terceiros ou contra o seu patrimônio. O Estado como garantidor desse direito, deve tomar medidas para que a segurança seja eficaz de maneira que os cidadãos e seus bens estejam protegidos e livres de qualquer dano. É aqui que a prevenção criminal demonstra total importância para que o plano de segurança estatal seja confiável, sendo criteriosas as regras para atuação administrativas, econômicas e judiciárias do Estado.

Expõe António Sousa (2003, p. 49) "a prevenção orienta-se a um fim futuro, que consiste em impedir que um perigo surja ou se concretize em dano". Ainda conforme Marcello Caetano (1996, p. 268) "evitar que os perigos se convertam em danos – eis o campo onde se desenvolve o modo de agir administrativamente que se chama polícia. Por último, consoante Germano Marques da Silva (1993, p. 53) "o que importa à coletividade, [...], não é tanto punir os que transgridem, mas evitar, pelo adequado uso dos meios legais de dissuasão, que transgridam". A função estatal enquanto garantidor da ordem pública é estabelecer normas e critérios que visem a não sucessão de crimes através de órgãos administrativos, traçando mecanismos para a prevenção. Nesse ínterim, a investigação criminal é efetuada graças aos recursos que o poder público oferece aos órgãos de segurança, facilitando a análise criminal.

Esses são os principais direitos fundamentais para interesse desse trabalho e estão inseridos na lei no contexto português e no contexto internacional. Entretanto, é natural que existam colisões entre eles, principalmente quando se investiga o trabalho de prevenção criminal do Estado, aliado ao direito à segurança e limitando alguns aspectos fundamentais dos direitos à imagem, liberdade, vida privada e intimidade. Vieira de Andrade (2010, p. 303) diz que "os direitos, liberdades e garantias não são absolutos nem ilimitados, [...] os direitos

liberdades e garantias cedem, em termos proporcionais, perante outros e encontram-se limitados internamente e externamente [...]. Internamente, pois encontram-se restringidos pelas situações de conflito, entre diferentes valores, que representam as diversas facetas da dignidade humana e externamente, pois devem conciliar as suas exigências naturais com as imposições próprias da vida em sociedade: a ordem pública, a autoridade do Estado, a segurança nacional."

Percebe-se que a colisão no âmbito da videovigilância é devida pelo fato de que a Constituição assegura concorrentemente dois ou mais direitos fundamentas em um mesmo contexto. Ainda, Vieira de Andrade (2010, p. 312) aduz que "a esfera de proteção de um direito é constitucionalmente protegida em termos de intersectar a esfera de outro direito ou de colidir com uma outra norma ou princípio constitucional."

Como então solucionar esses conflitos? Qual o lado da balança do direito pesará mais?

A doutrina majoritária orienta a observância de alguns princípios e critérios para a solução dos conflitos entre direitos. Um deles é o princípio da harmonização ou concordância prática que parte da ideia que todos os princípios são de "igual valor" (CANOTILHO, 1983, p. 507), ou seja, devem coexistir na mesma situação com equilíbrio e proporcionalidade, não sendo necessário a supressão total de um para eficácia de outro. Vieira de Andrade (2010, p. 312) é claro quando "um método e processo de legitimação das soluções que impõe a ponderação ou [...] um *balancing ad-hoc* – de todos os valores constitucionais aplicáveis, para que não se ignore nenhum deles, para que a Constituição seja preservada na medida do possível", bem como "a solução dos conflitos e colisões entre direitos, liberdades e garantias [...], não pode, porém, ser resolvida através de uma referência abstrata, com o mero recurso à ideia de uma ordem hierárquica dos valores constitucionais" (ANDRADE, 2010, p. 312).

Outro critério que deve ser levando em conta para a solução de conflitos, é o princípio da prevalência do interesse superior, que se traduz em proteger o bem jurídico de maior valor em detrimento do bem jurídico de menor valor. O artigo 335º do Código Civil português também estabelece o critério quando a colisão for de direitos iguais ou da mesma espécie "devem os titulares ceder na medida do necessário para que todos produzam igualmente o seu efeito, sem maior detrimento para qualquer das partes," e quando forem direitos diferentes e espécies diferentes "prevalece o que deva considerar-se superior" (DECRETO-LEI n.º 47344, 1966, s/p).

Entretanto, como todos os direitos investigados até aqui estão consolidados na Constituição, é de difícil análise as hierarquias entre eles, necessitando especialmente de alguma situação concreta para a devida ponderação. Vieira de Andrade (2010, p. 303) refere

que “não sendo a ordem de valores constitucionais hierárquica, a solução para a colisão de direitos terá que passar pela tentativa de harmonizar da melhor maneira os preceitos divergentes, em função das circunstâncias concretas em que se põe o problema”.

Essa problemática não será solucionada meramente com a análise do artigo 335º do Código Civil português, pois é evidente que a construção dos direitos fundamentais é mais complexa, além do nível de afetação que eles exercem sobre determinado bem jurídico. Parece razoável a proporcionalidade na aplicação dos direitos e a necessidade, tendo em vista que a limitação de um direito sobre o outro trará melhor solução dependendo do caso, bem como o sacrifício parcial de direitos para salvar bem jurídico mais valoroso.

De forma resumida, pode-se dizer que o resultado para o conflito de direitos é o uso do juízo de ponderação “das formas ou modos de exercício específicos dos direitos, nas circunstâncias do caso concreto, tentando encontrar e justificar a solução mais conforme à ordem constitucional” (ANDRADE, 2010, p. 305). Assim, a doutrina vigente afirma a utilização desses métodos para o melhor juízo valorativo, destacando critérios de proporcionalidade e necessidade, que transportará à prevalência de um direito fundamental em detrimento a um outro ou até o sacrifício de um sobre um outro. Nesse último caso, conforme do Código Civil e o Código Penal português, a prevalência do interesse superior e o princípio da prevalência do interesse preponderante.

Vieira de Andrade (2010, p. 306) afirmou que a solução do conflito é “uma atividade simultaneamente de interpretação e de restrição ou condicionamento – de delimitação restritiva ou condicionadora, mas que parece dever integrar-se na competência do juiz e, em geral, dos aplicadores da Constituição”.

Com base no que foi dito, o legislador português estabeleceu regras capazes de solucionar os conflitos de direitos, embora a mera interpretação ofereça brechas, pois não apresentou critérios de aplicação, causando de certo modo insegurança jurídica. Por isso é de suma importância a avaliação do caso concreto, observada devidamente o conselho doutrinário e a extensão dos preceitos constitucionais em relação à aplicabilidade de princípios como a proporcionalidade e necessidade, além das condições e atitudes das pessoas envolvidas.

### 2.4 - O Novo RGPD – 2016/679 UE

O Regulamento Geral de Proteção de Dados aprovado pelo Regulamento 2016/679 EU do Conselho do Parlamento Europeu, estabelece normas de proteção, tratamento e

circulação de dados pessoais, que revogou a Diretiva 95/46/CE, que transpôs a Lei 67/98 (Lei de Proteção de Dados), e que é elaborada seguindo a Agenda Digital para a comunidade europeia, viabilizando mudanças desde o ano de 2012.

O regulamento traz a garantia para o consumidor nas transações comerciais digitais, visando a proteção dos dados do titular, proatividade e responsabilidade das instituições que usam a base de dados de terceiros, exigência à segurança e amparo aos direitos dos titulares desses dados.

Comparado à antiga Diretiva revogada, o Regulamento continua a ratificar os conceitos e aplicações de dados pessoais, consentimento, responsável pelo tratamento e entidade subcontratante, tratamento, autoridade de controlo etc. Entretanto há inovações pertinentes no que diz respeito ao direito à pseudonimização e anonimização, à violação de dados desde a concepção, à consulta prévia, ao registro das operações de tratamento, aos responsáveis para a proteção de dados, dentre outras.

O objetivo do Regulamento é "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." (nº 2) (UNIÃO EUROPEIA, 2016, p. 1).

Seu foco principal é destinado à tríade de autores, composta pelo titular dos dados, pela autoridade de controle (CNPD), vinculada ao Comité Europeu de Proteção de Dados, e o responsável pelo tratamento. Conforme o RGPD, o titular dos dados é "considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular." (UNIÃO EUROPEIA, 2016, p. 33).

O responsável pelo tratamento descrito no artigo 4º, nº 7 é "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais." (UNIÃO EUROPEIA, 2016, p. 33). Portanto, é a pessoa que conduz a maneira de como os dados serão tratados, o tempo disponível para tratamento, os tipos de dados analisados, a causa que deu motivo ao tratamento, observados os princípios previstos no artigo 5º, as obrigações previstas no artigo 24º e seguintes e os direitos dos titulares previstos nos artigos 12º e seguintes.

Outra novidade importante e que muda o disposto na Lei nº 9/2012, é a necessidade de

comunicação prévia à CNPD para o tratamento de dados, que poderá ser feita posteriormente. Isso só foi possível graças ao conjunto de princípios relativos à responsabilidade de tratamento que automaticamente transfere ao responsável pelos dados a exigência normativa, conforme previstos no artigo 5º, nº 2 e o artigo 24º. Sendo mais claro, o nº 89 diz que a Diretiva 95/46/CE previu a obrigação prévia de notificar entidades de controle, ou seja, a CNPD, para tratamento de dados. Portanto, "esta obrigação originou encargos administrativos e financeiros, e nem sempre contribuiu para a melhoria da proteção de dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades." (nº 89) (UNIÃO EUROPEIA, 2016, p. 17).

A entidade subcontratante também recebe seu conceito legal previsto no artigo 4º nº 8 sendo a "pessoa singular ou coletiva, agência ou outro organismo que trate dados pessoais por conta do responsável pelo tratamento de dados" (UNIÃO EUROPEIA, 2016, p. 33). Antes da Lei em questão, o titular não poderia aduzir responsabilidade ao subcontratante, salvo se este estivesse sob contrato do responsável pelos dados. Agora o titular tem aval normativo para exigir obrigações ao subcontratante, visto que é diretamente responsável, tendo em voga o artigo 79º e seguintes. As obrigações do subcontratante são em conjunto com a CNPD, a luz do artigo 28º, o que leva ao responsável pelo tratamento a sua contratação somente se estiver de acordo com os princípios da RGPD, previsto no nº 5 do artigo 28º.

A CNPD, caracterizada no Regulamento como entidade de controle nos artigos 51º e seguintes, possui como principais atribuições a execução do regulamento, cooperação com autoridades, condução de investigação, orientação, gestão de reclamações, sensibilização dos responsáveis pelo tratamento, aconselhamento, cumprimento de sanções, dentre outras previstas no artigo 57º e 58º. Também é legitimada a emitir recomendações por escrito e auxiliar o responsável pelo tratamento, conforme artigo 36º, nº 8. Compete que torne pública uma lista do tipo de tratamentos operados "em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados" (UNIÃO EUROPEIA, 2016, p. 53). Promove em conjunto com o Estado, Comité e a Comissão, códigos de conduta, criação de procedimentos de certificação em matéria de proteção de dados e acredita organismos de certificação, conforme artigos 40.º a 42.º e 58.º n.º 3.

Passando aos direitos dos titulares de dados, o RGPD ratifica a Diretiva quanto aos direitos de informação, acesso, retificação e oposição nos termos dos artigos 13º, 14º, 15º, 16º

e 21º. A mudança foi o surgimento de novos institutos jurídicos com a função de proteger e estabelecer mais limites a favor dos titulares dos dados, que são os direitos ao apagamento ou esquecimento, à limitação do tratamento, à portabilidade dos dados, à decisões individuais automatizadas e à comunicação de uma violação de dados pessoais, nos termos dos artigos 17º, 18º, 20º, 22º e 34º. O responsável pelo tratamento deverá facilitar que todos esses direitos sejam exercidos pelo titular, agindo com a devida transparência, ficando a cargo do responsável a gestão e controle de eventuais pedidos para revista, conforme o artigo 12º.

A prática dos direitos narrados será gratuita, salvo quando manifestamente excessivos, repetitivos ou sem fundamento que o justifiquem, sendo possível que o responsável recuse o pedido de acordo com a regra descrita em lei, ou seja, quando for demonstrado o conteúdo manifestamente infundado ou excessivo. O prazo para a apreciação do pedido é de um mês da dada o seu recebimento e será prorrogado por dois meses quando se tratar de matéria complexa. Independente da fundamentação do tratamento, o direito à informação (artigos 13º e 14º), direito à ao acesso dos dados (artigo 15º), direito à retificação (artigo 16º). Caso os dados pessoais sejam recolhidos na presença do titular, o responsável para o tratamento faculta-lhe algumas informações como a identidade e o contato dos demais responsáveis que irão tratar os dados, a finalidade e o fundamento jurídico do tratamento. São esses os requisitos mínimos para o direito à transparência, conforme artigo 5º, nº 1.

Quanto a confirmação dos dados que serão tratados, o titular deve ter conhecimento de quais serão os dados e de que forma se conduzirá o tratamento, bem como a sua licitude, finalidade, período de tratamento etc. Poderá facultar ao titular "o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais" (63) (UNIÃO EUROPEIA, 2016, p. 12).

O direito à retificação garante ao titular reparações dos seus dados pessoas perante o responsável do tratamento sem demora injustificada, "o titular dos dados tem o direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional" (UNIÃO EUROPEIA, 2016, p. 43), nos termos do artigo 16º.

No entanto, existe direitos peculiares que estão previsto no RGPD, pois dependem de outros aspectos, como por exemplo o fundamento do tratamento. São constituídos por: direitos ao esquecimento (artigo 17º), direito à limitação de tratamento (artigo 18º), direito à portabilidade (artigo 20º), direito à oposição (artigo 21º), direito relacionados à decisão individual automatizada (artigo 22º) e o direito à notificação (artigo 36º).

O direito ao esquecimento ou apagamento dos dados, apenas pode ser exercido se previstas as motivações contidas nas alíneas do artigo 17º, alíneas "a" a "f", ou seja, os dados

deixaram de ser necessários para a finalidade que motivou a sua recolha e tratamento; titular retira o consentimento em que se baseia o tratamento e se não existir outro fundamento jurídico para o referido tratamento; o titular opõe-se ao tratamento e não existem interesses legítimos prevalecentes; os dados pessoais foram tratados ilicitamente; os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; e os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação.

Porém o Regulamento estabelece situações previstas no artigo 17º, nº 3, alíneas "a" a "e", em que esse direito é reconhecido, tendo em vista a continuidade do tratamento para casos do exercício da liberdade de expressão e informação, para o cumprimento de uma obrigação legal imposta pela União ou Estado-Membro e exercício da função ou autoridade pública, para motivos de interesse público relativos à saúde pública, à investigação científica, histórica ou fins estatísticos e para fins processuais.

A limitação do tratamento é direito do titular dos dados, conforme artigo 18º, sendo permitido o acesso com o seu consentimento, salvo para efeitos declaratórios, defesa de direitos em processos judiciais, defesa de terceiros ou a coletividade ou por motivo de interesse público. Portanto, o nº 67 assevera que "para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio *web* dos dados aí publicados" (UNIÃO EUROPEIA, 2016, p. 13). Em se tratando de ficheiros automatizados, o tratamento deverá ser feito de forma técnica para impedir que os dados possam ser tratados por outros meios e impeça a sua alteração.

A portabilidade quando é exercida pelo titular, permite a transferência dos seus dados para outro responsável, quando houver consentimento ou por meio de um contrato e for realizado por meios automatizados (artigo 20º). Portanto, o titular dos dados deverá, "ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável" (nº 68) (UNIÃO EUROPEIA, 2016, p. 12). Quando se tratar de dados de mais de um indivíduo, o responsável do tratamento deverá tomar providências para não afetar dados de terceiros ou infringir desnecessariamente direitos.

O direito à oposição traduz que o titular é legítimo para se opor a qualquer momento ao tratamento por motivos relacionados com a sua situação particular que deverá

imediatamente o responsável pelos dados cessar a operação, “a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial” (artigo 21º nº 1) ou “salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.” (artigo 21º, nº 6) (UNIÃO EUROPEIA, 2016, p. 45-46).

O titular não ficará vulnerável a nenhuma decisão exclusiva do tratamento automatizado de dados, incluindo a definição de perfis, que haja efeitos em na esfera jurídica ou que o afete em algum grau semelhante. O direito não é aplicável nos casos em que “for necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento, for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou for baseada no consentimento explícito do titular dos dados” (artigo 22º, nº 2) (UNIÃO EUROPEIA, 2016, p. 45-46). O responsável pelo tratamento deverá prezar por medidas adequadas para salvaguardas os direitos, garantias e interesse do titular, inclusive designar a intervenção humana por parte do responsável para fins de opinar ou contestar a decisão, conforme previsto no artigo 22º, nº 3.

O RGPD trouxe outro princípio, em seu número 74, o da responsabilidade proativa o qual “deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares” (UNIÃO EUROPEIA, 2016, p.14).

Tal princípio exige ao responsável pelo tratamento adotar medidas técnicas, organizadas e adequadamente seguras, aderir a políticas protetivas, registrar todas as atividades que serão tratadas, avaliar previamente o impacto do tratamento, notificar caso haja violação de dados, obrigatoriedade de provar o cumprimento de suas obrigações.

Quanto a medidas técnicas e organizativas e de segurança, o responsável pelo tratamento deverá tomar medidas que dizem respeito à pseudominização e cifragem de dados pessoais, assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes

dos sistemas e dos serviços a serem tratados, ser capazes de reestabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico, processo que teste, aprecie e avalie regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento, avaliar o nível de segurança adequado, tendo em conta os riscos apresentados pelo tratamento, cumprir o código de conduta ou um procedimento de certificação previstos nos artigos 40º e 42º, para demonstração do cumprimento das obrigações.

Percebe-se que o Regulamento impõe a elaboração de um código de conduta elaborados pelos legitimados por lei ao tratamento de dados, ou seja, aos que exercem a atividade. O código deverá ser apresentado perante a CNPD e esta fará a análise determinando a validade ou não do mesmo. A CNPD e o organismo farão a supervisão do cumprimento do código. Também prevê a obrigatoriedade de uma política de proteção no momento do tratamento, caso haja defeitos, redução da quantidade de tratamentos, extensão de tratamentos, período de conservação e acessibilidade.

A obrigação de registro para as atividades de tratamento, englobam empresas ou organismos que tenham mais de 250 trabalhadores, quando eminência de perigo para os direitos e garantias do titular de dados e quando o mérito do tratamento não envolver assuntos sensíveis, infrações ou condenações criminais. Para comprovação desses fatos, haverá um registro por escrito ou eletrônico. É obrigatória disponibilizar à CNPD, informações relativas ao nome, contatos de responsáveis, destinatários, categorias de titulares e dados, transferências internacionais, prazos para apagamento, localização dos dados e características do suporte.

As obrigações do EDP consistem nas funções de informar e aconselhar sobre suas obrigações aos trabalhadores e responsáveis, está de acordo com as regras do Regulamento, lei nacional e políticas do responsável (sensibilização, auditorias) e dar parecer no que diz respeito a avaliação de impactos, quando lhe é solicitado e atuar junto à autoridade de controle. Além disso, sua atividade é o essencial ao poder público, visto que é responsável pelo tratamento de grande quantidade de dados sensíveis, condenações ou infrações criminais, e nos casos que a lei obriga. É obrigado o sigilo e a confidencialidade das suas atividades.

A avaliação prévia de impactos é obrigatória quando se tratar do uso de novas tecnologias, em casos de tratamento automatizado de pessoas singulares e seus aspectos pessoais, tendo como base decisões que podem produzir efeitos jurídicos relevantes ou que afetem sua reputação “ou na sequência do tratamento de categorias especiais de dados pessoais, de dados biométricos ou de dados sobre condenações penais e infrações ou medidas

de segurança conexas." (nº 91) (UNIÃO EUROPEIA, 2016, p. 18). Se um tratamento ter algum risco de impactar direitos e liberdades de pessoas singulares, o responsável pelo tratamento deve proceder a uma avaliação de impactos. "A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados." (nº 4, artigo 35º) (UNIÃO EUROPEIA, 2016, p. 53).

A CNPD deve ser consultada antes da avaliação de riscos sobre a proteção de dados pelo responsável do tratamento, emitindo orientações escritas no prazo de 8 semanas, prorrogáveis por mais 6 semanas. A consulta deve ser eivada de elementos como a repartição de responsabilidades, finalidades e meios do tratamento, medidas garantistas para defesa de direitos dos titulares, contatos do encarregado dos dados e avaliação de impactos (nº 3, art. 36º).

No caso de, mesmo observados todos os requisitos da RGPD, ocorrer violação dos dados, o responsável pelo tratamento "notifica desse facto a autoridade de controlo competente [...], sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso." (artigo 33º) (UNIÃO EUROPEIA, 2016, p. 52). No texto da notificação deve ser escrito o tipo de violação, os titulares atingidos bem como os seus contatos, demonstração dos impactos e possíveis reparações. Nos casos mais graves de violação, deve ser informado do fato o titular em caráter de urgência, sem demora injustificada e numa linguagem direta.

Na comunicação ao titular, deve ser apresentadas as características da violação, contatos dos responsáveis pelo tratamento, descrição dos procedimentos e possível reparação do dano causado. Porém, há situações que essa comunicação pode ser suprimida no caso de execução de medidas adequadas, como a cifragem, a adoção de meios que anulem o risco, ou mesmo a comunicação por si só apresente um nível desproporcional. A Administração Pública Portuguesa foi pautada pelo Governo português quanto as orientações técnicas para o novo RGPD, prevista na Resolução do Conselho de Ministros nº 41 (2018, p. 1425), conforme preleciona:

> 1 — Aprovar os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado, os quais constam do anexo à presente resolução e que dela faz parte integrante. 2 — Recomendar a aplicação dos requisitos técnicos a que se refere o número anterior também nas redes e sistemas de informação do setor empresarial do Estado. 3 — Determinar que cada serviço e entidade da

> Administração direta e indireta do Estado deve avaliar a conformidade dos requisitos técnicos das redes e sistemas de informação em uso com as finalidades e princípios de segurança que se pretendem alcançar com os requisitos estabelecidos no anexo à presente resolução. 4 — Determinar que os requisitos referidos no anexo à presente resolução devem ser implementados no prazo máximo de 18 meses após a data de entrada em vigor da presente resolução.

Por fim, o novo RGPD veio trazer diversas obrigações para empresas ou entidades pública ou privada que tenham em mãos a responsabilidade de tratamento de dados pessoais. Devem observar princípios e garantias, no exercício de suas funções e visa cumprir todos os preceitos e normas estabelecidos no Regulamento, proteger os dados pessoais criando medidas técnicas e seguras, nomear o responsável de tratamento, estabelecer critérios razoáveis de competência para os responsáveis do tratamento, dentre outros. Porém, o artigo 2º, nº 2, alínea "d" estabelece que o Regulamento não se aplica caso "efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública." (UNIÃO EUROPEIA, 2016, p. 32).

Assim, o RGPD estabeleceu mais autonomia às forças de segurança quanto a não obrigatoriedade de notificação ao CNPD. Em matéria de investigação criminal é aplicado a Diretiva 2016/680, conforme seu artigo 1º, nº 1, tendo em vista "à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública" (UNIÃO EUROPEIA, 2016, p. 4).

## 3 - O USO DA INTERNET

### 3.1 – Exposição de dados na internet

Por muito tempo, a população mundial buscou meios capazes de facilitar a tomada de decisões e execuções de tarefas de maneira automatizada. Essa necessidade foi suprida com a chegada do computador e vem sendo aprimorada todos os anos novas habilidade e novas ações. Tendo em vista as vantagens que o computador trouxe, pessoas do mundo inteiro já não conseguem "viver" sem a presença de um simples relógio inteligente (*smartwatch*), quando mais sem a presença de um celular (*smartphone*). Tudo isso graças à inúmeras

vantagens que a tecnologia trouxe que felizmente (ou infelizmente?) tornaram pessoas escravas e dependentes dela.

No Brasil existem cerca de 10 milhões de internautas com conhecimento cada vez mais avançado em tecnologia, e esse número cresce exponencialmente todos os dias. Alguns estudos mostram o mercado negro de cursos para crimes virtuais no Brasil e, para analisar e mapear o submundo dos cibercrimes na Rússia e na China, a Trend Micro lança o estudo "*The Brazilian Underground Market*", com um panorama dos problemas de segurança digital no Brasil. De acordo com alguns estudos, o submundo dos cibercrimes do país é o único que possui treinamentos para pessoas que queiram entrar nesse mundo (ROSSINI, 2004).

Segundo o *Norton Cyber Security*, o Brasil foi o segundo país que mais recebeu denúncias de crimes cibernéticos. No mundo, cerca de 62 milhões de pessoas foram vítimas, gerando um prejuízo aproximado de 22 bilhões de dólares (BRASIL, 2020).

Entretanto, pondera-se que para encontrar o responsável pelos crimes cibernéticos é necessária uma quebra de sigilo, ou seja, faz-se imprescindível rastrear a localidade através da máquina usada para cometer o ato ilícito e, assim, autuar o culpado, por meio de provas eletrônicas e de uma perícia técnica, uma vez que somente dessa maneira as provas são aceitas e incluídas ao processo (WENDT; JORGE, 2014).

As estruturas sociais são totalmente dependentes da *internet*, sendo esta o principal instrumento que alimenta e expande o planeta. Essencialmente importante, ela traz inúmeras facilidades e meios que facilitam o processamento de informações, armazenamento de dados e propagação de conteúdos com grande rapidez e agilidade. Afirma Lima (2016, p. 10):

> Os avanços tecnológicos mais intensamente percebidos a partir da década de 1970 resultam no desenvolvimento do computador e da *internet*, que no decorrer da década de 1990 avançam na sua popularização e hoje representam uma realidade crescente na vida das pessoas. Essa realidade tem imposto significativas mudanças nos hábitos, comportamentos sociais e até mesmo na maneira das pessoas se relacionarem. A busca pela informação e interação imediata faz dos indivíduos seres cada vez mais conectados que passam a construir uma espécie de *second life* no espaço virtual. A convergência de tecnologias, a virtualização do mundo e o indivíduo conectado impulsionam a sociedade, que se personifica como uma sociedade digital.

Com o surgimento das redes sociais, em meio ao "caos tecnológico", muito se discute a respeito dos impactos jurídicos e nas vidas humanas que perfis na *internet* podem trazer para a sociedade. O universo de ações e recursos que as redes sociais [2]oferecem, em parceria

[2] A utilização das redes sociais virtuais modificou profundamente a forma de obtenção, tratamento e divulgação de dados pessoais, o que impactou diretamente a própria expectativa de privacidade da pessoa humana. Nos dias atuais, dificilmente o indivíduo poderá alcançar um alto grau de controle sobre as suas informações e

com propagandas e em massa disponibilizadas na *internet*, criam a separação entre mundo real e mundo virtual na vida dos indivíduos que, por muitas vezes, dimensionam suas vidas pelo mundo virtual.

A leitura do art. 3º do Marco Civil da Internet (MCI) estabelece que a *internet* no Brasil esteja alicerçada com base em princípios tais como: princípios da neutralidade da rede, privacidade e da liberdade de expressão, que estão interligados entre si. No princípio da neutralidade pode ser visto um reforço quanto a liberdade de expressão, e a privacidade traz a representação de seu limite.[3]

Na contextualização acerca de privacidade, um de seus aspectos que mais se destacam na atualidade seria o controle da circulação de informações pessoais.

> A ideia de privacidade, porém, é profundamente equivocada, pois ignora a existência de relações privadas limitadas aos membros de um grupo, e não reconhece que o indivíduo pode querer ocultar determinadas informações apenas de pessoas específicas, compartilhando-as normalmente com outras. [...] quando informações intimas a respeito de um indivíduo circulam em um pequeno grupo de pessoas que o conhecem bem, seu significado pode ser ponderado ante outros aspectos do caráter e da personalidade desse indivíduo. Em contrapartida, quando essas mesmas informações são removidas do contexto original e reveladas a estranhos, o indivíduo se torna vulnerável, correndo o risco de ser julgado com base em seus gostos e experiências mais embaraçosos (LEONARDI, 2012, p. 65).

Nesse sentindo, têm-se que as configurações atuais de privacidade teriam rompido as barreiras entre "pessoa/informação/segredo" para que com isso pudesse se estruturar de maneira a ter a seguinte conformação "pessoa-informação/circulação/controle". De acordo com Teffé e Moraes (2017, p. 6): "A liberdade de expressão, considerada como liberdade de externar ideias, juízos de valor e as mais variadas manifestações do pensamento, além de já ser amplamente protegida pelo constituinte, apresenta no MCI tutela destacada, sendo

---

características pessoais depois que as inserir na rede. Dessa forma, pode-se afirmar que a velocidade da circulação da informação é inversamente proporcional à capacidade de seu controle, retificação e eliminação. Cabe lembrar que a rede social virtual configura um modelo de negócio bastante rentável, embasado em conceitos como visibilidade, vigilância, identidade e indexação. Sua estrutura apresenta duas fases principais. Em primeiro lugar, visa-se alcançar uma massa crítica de usuários e, posteriormente, parte-se para a exploração e a monetização da rede social, por meio da venda de espaços para a publicidade, da comercialização de produtos (como publicações patrocinadas) e da "venda" de perfis, cadastros e dados pessoais de seus usuários (TEFFÉ; MORAES, 2017, p. 15).

[3] O princípio da neutralidade da rede, em particular, determina que a rede deve tratar da mesma forma tudo aquilo que transportar, sem fazer discriminações quanto à natureza do conteúdo ou à identidade do usuário, buscando-se, assim, "garantir uma experiência integral da rede a seus usuários" .A regra deve ser, portanto, o tratamento isonômico dos pacotes de dados, sem distinção por conteúdo, origem, destino, serviço, terminal ou aplicação, havendo expressa vedação ao bloqueio, monitoramento, filtragem ou análise do conteúdo dos pacotes (art. 9º do MCI). O princípio impõe que a filtragem ou os privilégios de tráfego devam respeitar apenas e tão somente critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos ou culturais que criem qualquer forma de discriminação ou favorecimento (WU, 2012, p. 244).

considerada um fundamento e um princípio para a disciplina do uso da *internet* no Brasil e condição para o pleno exercício do direito de acesso. Ao longo do Marco Civil, percebe-se a preocupação do legislador com a compatibilização desses princípios, tendo por fim assegurar que, também na *internet*, a pessoa humana possa livremente desenvolver sua personalidade".

A criação de aparelhos modernos e móveis, como os *smartphones*, abriu um novo leque de interação entre pessoas de diversas partes do mundo, sem a necessidade de contato físico ou proximidade, mudando significativamente a forma de relacionar-se. Essa modificação também contribuiu para que houvesse o afastamento físico do homem moderno, ele acabou por permitir um contato mais frequente usando esses recursos tecnológicos, tornando o relacionamento social mais direto e interativo e novo quanto a convivência.

Cria-se a cultura da auto exposição na web. Para se sentirem "digitalmente incluídas" na sociedade da informação, algumas pessoas colocam-se em evidência de forma temerária, alimentando o firme propósito de serem "localizadas" na rede mundial de computadores [...] Enfim, a *internet*, além de facilitar a violação da privacidade por terceiros, induz o usuário inconsciente à auto exposição exagerada" (VIEIRA, 2007, p. 193).

Percebe-se nessa nova forma de se relacionar a inversão dos papéis no que se refere ao fato de que primeiro era o contato físico para que posteriormente fossem possíveis à comunhão de ideias. Em tempo rela a sociedade, as pessoas e o mundo em si atuam ativamente para a promoção de discussões e seleção de conceitos e informações que serão inseridos em meio a rede e a comunicação virtual (TEFFÉ; MORAES, 2017).

Ao se fazer uma análise acerca das principais ferramentas que facilitam a exposição do indivíduo na *internet*, entende-se que em regra, esses possuem características tanto da Web 2.0 (participativa) quanto da Web 3.0 (semântica ou a inteligente) e que esses tipos de web possuem fácil acessibilidade através de aplicativos que foram desenvolvidos para funcionarem em celulares e *tablets*. A internet móvel proporciona ferramentas de grande importância nas ações humanas diárias, pois facilita a interação entre usuários e facilita o acesso à informação e conteúdo de forma objetiva (KREIN, 2018).

"Quanto maior a sua rede de contatos, maior é o número de pessoas que possui acesso ao que você divulga, e menores são as garantias de que suas informações não serão repassadas. Além disso, não há como controlar o que os outros divulgam sobre você" (CERT.br, 2012, p. 88).

Segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE) no ano de 2015 o acesso à *internet* através de celulares cresceu de forma significativa se comparado àquela utilizada com o uso do computador em todos os grandes centros urbanos do país. Com

efeito, o uso de celular como veículo para acesso à *internet* passou de 80,4%, em 2014, para 92,1%, em 2015 (IBGE, 2015).

Para Sibilia (2013) As redes sociais são usadas para as mais diversas finalidades, desde criação de perfis digitais a criação de nichos engajados em uma determinada ideia ou gostos em comum, bem como divulgação de *marketing* de produtos e serviços. Ainda, as redes sociais são uma forte ferramenta para promover opiniões políticas, religiosas e ideológicas, sendo importante para a organização de manifestações sociais nos países. O uso das redes constituem a principal forma de interação entre usuários atualmente.

"A dinâmica das redes sociais na *internet* é pautada por elementos e processos que terão influência direta na estrutura da mesma, como a cooperação, conflito, agregação, ruptura, os quais acontecem de forma emergente, e dão a percepção do caráter altamente mutante, dinâmico e surpreendente. Justamente por estar em uma constante mutação é que as redes sociais na *internet* demonstram uma evolução em seu caráter de interatividade e mobilidade, se consolidando como Redes Sociais na *Internet* 3.0" (LIMA, 2016, p. 33).

O que se entende por privacidade e exposição, parece estar sendo mudado ou adaptado graças ao uso contínuo das redes sociais por usuários, tendo em vista que cada perfil digital contém grande acervo de informações pessoais. Houve um tempo onde a cultura oitocentista, onde prezava-se pelo íntimo, pela essência pessoal, solitude de pensamentos, transformou-se drasticamente na metade do século XX, onde a cultura de exposição da imagem própria ou alheia dominou as relações humanas. (SARMENTO, 2006; SIBILIA; DIOGO, 2011).

Atualmente, o que domina na sociedade é o anseio para exibição sem precedentes da vida particular dos indivíduos, feitas por eles mesmos, transformando a cultura de uso da *internet.* Esse comportamento é visto com mais intensidade principalmente no público jovem. Esses expõem todos os detalhes possíveis tanto os mais relevantes quanto o mais irrelevante, momentos nos quais são compartilhados em redes sociais e aplicativos interativos (SILVA, 2010). Para Ayres e Ribeiro (2015) as redes sociais disponibilizam funções, os quais permite o manuseio de informações pessoais e interação com um grande número de pessoas, os autores trazem uma abordagem acerca da utilização dos recursos da ferramenta conhecida atualmente como *Whats App Inc.*

A auto exposição de usuários em perfis sociais é assustadora. Existe um certo tipo de prazer em expor opiniões, imagem, vida pessoal, rotinas e tudo o que abrange a privacidade do indivíduo. Esta cultura não se restringe apenas com o uso de *smartphones,* mas é estendida através de programas de tv, *reality show*s etc. Observa-se dessa forma o surgimento de uma geração no qual há o desejo crescente de ser notado, visto para além daquele mundo que o

circunda (MARICHAL, 2013).

As empresas ao fazerem uso da tecnologia na sociedade de informação, armazenam e coletam dados pessoais para a criação de um perfil de consumo, expondo pessoas a um tipo de risco delicado, seja pela vigilância exercida pelo Estado ou pelo setor privado, que é realizada por algoritmos de última geração e pelo *machine learning.* Conforme Yuval Noah Harari afirmou que "no século XXI, nossos dados pessoais são provavelmente o recurso mais valioso que ainda temos a oferecer, e os entregamos aos gigantes tecnológicos em troca de serviços de e-mail e de vídeos engraçadinhos".[4]

O capitalismo de vigilância trata o ser humano como matéria prima grátis, direcionando-o, através do seu comportamento, a contratação ou compra de algum produto. Em posse desses dados, as empresas ou o próprio Estado os analisam com intuito de melhoramento de produtos ou serviços, utilizando inteligência artificial para distinguir perfis comportamentais que preveem os gostos pessoais dos usuários. Essa análise e previsão comportamental é denominada pela autora Shoshana Zuboff de "mercados de comoprtamentos futuros."[5]

Existe o conceito de "corpo eletrônico", descrito por Stefano Rodotà, que seria uma entidade não apenas de massa corpórea, mas também de um corpo digital que possui personalidade e integra sua identidade.[6] Outra definição é feita por Roger Clarke[7], utilizando a expressão "*persona digital"*, que caracteriza a constituição do indivíduo como um conjunto de dados privados mantidos, transformando a pessoa em um avatar digital. À luz desses conceitos, qualquer tratamento de dado pessoal pode causar dano ao titular, porém alguns dados ao serem tratados podem causar danos irreparáveis. Portanto, há a necessidade dessa distinção na norma jurídica.

O cerne da questão que envolve dados pessoas está na preocupação ao seu armazenamento, tratamento e circulação da *persona digital*, podendo facilmente estigmatizar os titulares, causando danos à sua imagem. Há riscos de que esses dados ocasionem exclusão ou segregação social, portanto o controle deve ser rigoroso e eficaz através de textos legais. Assim, alguns dados específicos devem ser declarados como dados sensíveis, merecendo total atenção e leis atuantes.

---

[4] *Homo Deus* – Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016, p,. 343.

[5] ZUBOFF, Shoshana. The age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Nova Iorque: Public Affairs, 2018, pos. 188 (e-book). Obra já traduzida por George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

[6] RODOTÀ, Stefano. *Intervista su privacy e liberta.* Roma – Bari. Laterza, 2005, p. 120-121.

[7] CLARKE, Roger. Profiling: A Hidden Chalenge to the Regulation of Data Surveillance. *Jornal of Law Information and Science*, v.4, n. 2, p. 403, Hobart, dez 1993.

A ênfase no tratamento de dados sensíveis está na observância dos direitos à privacidade e dignidade, sopesado com o direito a liberdade de expressão, tendo como foco na classificação dos conteúdos (íntimos, sexuais e médicos) e foco nos prejuízos causados pela má administração, quando expostos indevidamente. Além disso, o uso em massa de algoritmos que preveem os anseios e gostos dos indivíduos, hipervulnerabiliza o mesmo que é consumidor, tirando-lhe ou dirimindo o poder do livre arbítrio nas escolhas de produtos ou serviços.

O comportamento humano nas últimas décadas tem se mostrado cada vez mais irracional e propenso ao erro, devido à inúmeras quantidades de informações que manipulam o cérebro. A exemplo, atualmente crianças conseguem aprender de maneira muito mais rápido do que crianças que viveram antes da revolução digital.[8]

A pessoa humana deve ser garantida a tutela singular, tendo em vista os seus princípios, decorrente do valor unitário do indivíduo. Um dos valores essenciais do ordenamento é a personalidade, contendo inúmeras outras demandas que se fundamentam nele e sendo exigido constantemente a sua tutela. Em contraponto às inclinações do mercado, o ordenamento jurídico deve enfatizar a unidade da pessoa. Costuma-se encontrar na sociedade da informação "pessoas eletrônicas", criadas pelo capitalismo ou outros interesses no recolhimento de informações. Já falava Rodetà que "estamos nos tornando 'abstrações no cyberspace', e, de novo, estamos diante de um indivíduo 'multiplicado'. Desta vez, porém, não por sua escolha, não por sua vontade de assumir identidades múltiplas, mas para reduzi-lo à medida das relações do mercado".[9]

Tal fato, contribui para a mitigação do externo, onde cada indivíduo encontra aquilo que mais se parece com seu ser, anulando qualquer pensamento contrário às suas ideias, interesses ou estilos de vida. O privilégio para o indivíduo está no seu mundo digital, na sua "bolha de algoritmos", fazendo-o esquecer da consciência e crítica social/pública e transformando-o em um prisioneiro do seu universo exclusivo e sua zona de conforto.

Como se não bastasse, a tecnologia não interrompe o seu *modus operandi*, trazendo cada vez mais facilidades e perigos com o famoso jogo de dados. Aparatos tecnológicos estão mais baratos à cada ano, como câmeras de vigilância, sensores de vídeo, *smartphones* que rastreiam qualquer movimentação do seu usuário e até programas que catalogam a digitação.

---

[8] BRIAN, Christian; GRIFFITHS, Tom. *Algoritmos para viver: a ciência exata das decisões humanas.* São Paulo: Companhia das Letras, 2017, p. 13-14 e 16.

[9] RODOTÀ. Stefano. *A vida na sociedade da vigilância: a privacidade hoje.* Organização, seleção e apresentação Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 125.

Tudo isso para fazer personalidades digitais que são estudadas pelo mercado e analisadas para o direcionamento certeiro para determinado fim.

Com todas essas questões a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) justifica que a tutela de dados pessoais está efetivada nos direitos humanos e fundamentais, conforme artigo 2º, inciso VII. Ainda, em seu artigo 6º, inciso IX estabelece a ilicitude de usar dados pessoas com fins discriminatórios ou abusivos. O princípio contido nesses incisos são manifestados sempre quando houver, no tratamento de dados sensíveis ou não, algum tipo ou característica de desprestígio. Portanto, a não discriminação é o fundamento para proteção de dados sensíveis, principalmente quando se trata de direitos sociais constitucionalmente ensinados, como trabalho, saúde, educação e moradia, contidos no artigo 6º da Constituição Federal.

É certo que quando se busca a proteção da privacidade, há a interrupção de atividades específicas. Quando acontece a invasão de privacidade, ações pontuais são mitigadas ou interrompidas. Logo, a informação por si só já tem um valor importante na sociedade bem como a forma ela pode ser utilizada, abrindo o leque para uma série condutas, visando a propaganda ou a utilização do perfil do indivíduo sem o seu consentimento, para obter o infalível lucro, através da posse de dados. Outro caso é o *Big Data,* onde um conjunto de informações de todas as espécies podem ser correlacionadas para criar uma matéria de pertinência nacional ou de pertinência à dignidade da pessoa humana, como prevenção de doenças, assuntos de segurança pública (terrorismo) e outros temas como racismo e pornografia infantil.

Semelhantemente, os dados sensíveis são constituídos não apenas por sua natureza personalíssima e única de casa indivíduo, como também pela maneira que esses dados são tratados, podendo facilmente gerar danos irreparáveis a dignidade da pessoa. Um caso que aconteceu nos Estados Unidos merece destaque, quando um grupo de engenheiros da Google conseguiu prever a epidemia do vírus H1N1. Eles publicaram a matéria na revista científica *Nature*, explicando que chegaram a essa conclusão devido ao monitoramento de buscas feitas por usuários na internet.

Entretanto, tal fato se caracterizou um efeito negativo por causa desse tipo de informação que fora divulgada. Questionou-se a possibilidade das informações terem sido analisadas pelos grandes laboratórios a fim de aumentar os preços dos medicamentos para gripe, ou essas informações terem sido usadas por seguradoras para fins de cálculos de risco.

Essa prática é denominada *profiling*[10], utilizado bastante no ramo do Direito Digital, a fim de analisar diversas faces na utilização de algoritmos no tratamento de bancos de dados (*Big Data*) que proporcionam um filtro para cada tipo de perfil comportamental, para futuras projeções e objetivos definidos.

Na Lei Geral de Proteção de Dados Pessoais, em seu artigo 12, parágrafo II, fala exatamente sobre o tema, classificando essa prática: "Poderão ser igualmente considerados como dados pessoais, para fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada". A chamada "metainformação"[11] é concretizada através da técnica *profiling,* onde usa-se métodos estatísticos, inteligência artificial e outras estratégias para criar-se um compilado de preferências pessoais e registro de atividades, desenhando um quadro de tendências comportamentais e escolhas para cada tipo de perfil pessoal.

Esse perfil é o que está registrado no banco de dados de uma pessoa específica e compreende toda a sua personalidade. É um compilado de vários dados pessoais, propondo conseguir uma "imagem detalhada e confiável, visando, geralmente, à previsibilidade de padrões de comportamento, de gostos, hábitos de consumo e preferências do consumidor".[12] Essa técnica apresenta riscos à personalidade, e sua aplicação depende de leis rígidas para proteger o consumidor vulnerável, notificando o consentimento, à luz do artigo 11, inciso I, da Lei 13.709/2018.

Alguns incidentes com o tratamento de dados pessoas sensíveis ocorreram nos últimos anos. Em 2016, o serviço de coleta de sangue australiano (Red Cross Blood Service) foi responsável pelo vazamento de dados de 550.000 doadores. As informações de todas essas pessoas vieram a público, notadamente as que tinham comportamentos sexuais considerados "arriscados". Outro caso de vazamento de dados aconteceu no Canadá, no ano de 2017, onde uma fabricante de brinquedos sexuais, a Standard Innovation, disponibilizou para venda um vibrador que possuía conexão por *bluetooth e wi-fi* com o celular. Posteriormente foi descoberto que a empresa tinha acesso aos dados de uso do brinquedo que eram enviados para

[10] A palavra para o português é perfilamento, sendo esta acolhida pelas Ciências Criminais, como bem esclarece Tálita Heusi: "O perfilamento criminal, também tem sido denominado de: perfilagem criminal, perfilamento comportamental, perfilamento de cena de crime, perfilamento da personalidade criminosa, perfilamento do ofensor, perfilamento psicológico, análise investigativa criminal e psicologia investigativa. Por conta da variedade de métodos e do nível de educação dos profissionais que trabalham nessa área, existe uma grande falta de uniformidade em relação às aplicações e definições desses termos. Consequentemente, os termos são usados inconsistentemente e indistintamente". HEUSI, Tálita Rodrigues. Perfil criminal como prova pericial no Brasil. *Brazillian Journal of Forensic Sciences, Medical Law and Bioethics*, v. 5, n. 3, p. 237, Itajaí, 2016.

[11] DONEDA, Danilo - Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 173.

[12] MENDES, Laura Schertel - Privacidade, proteção de dados e defesa do consumidor. São Paulo: Saraiva, 2014, p. 53-54.

o seu servidor, inclusive no exato momento de uso. Por último, em 2014, um sistema de pontuação foi criado na China para classificar os cidadãos para ingresso em cargos políticos e serviços públicos.[13]

Além disso, a inteligência artificial substituiu em toda ou em parte as decisões humanas em diversos setores sociais. Baseadas em sistemas automáticos, algoritmos de *marketing* e *softwares* que analisam riscos preditivos, essas atribuições tecnológicas são capazes de "investigar" potenciais riscos de indivíduos cometerem crimes, baseando-se em analises em computadores e cálculos estatísticos.

O artigo 5º, I, da Lei 13.706/2018, observa que o dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável". Já o dado sensível é o dado "pessoal sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural", conforme artigo 5º, inciso II.

No artigo, a igualdade matéria é aplicada sem prejuízo à privacidade, acima da liberdade, o que dá autonomia para o pleito dos direitos, sem possíveis restrições ou obstáculos. Portanto, os dados sensíveis contidos no artigo 5º, inciso II da LGPD, são "opções realizadas pelo legislador motivadas pelo efeito potencialmente lesivo do seu tratamento".[14]

O principal atributo do dado pessoal é a identidade da pessoa natural pertencente a ele, impedindo-se o anonimato, portanto, ao "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento". (Lei Geral de Proteção de Dados Pessoais, artigo 5º, III).

Quanto ser o dado sensível ou não, percebe-se a inclinação do legislador brasileiro ao Regulamento Europeu (GDPR), por classificar exemplificativamente esse tipo de dado. Observa-se também que o tratamento a dados sensíveis desloca à Lei do Cadastro Positivo (Lei 12.414/2011), que não permite anotações em banco de dados utilizados para examinar créditos de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas", conforme artigo 3º, inciso II, da referida lei.

No Brasil reconhece-se, portanto, que são aplicadas as mesmas regras no tratamento

[13] TEFFÉ, Chiara Spadaccini de - A categoria especial dos dados sensíveis: fundamentos e contornos. In: SCHEREIBER, Anderson; MONTEIRO FILHO, Carlos Edson do Rêgo; OLIVA, Milena Donato. *Problemas de Direito Civil*; homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Jnaiero: Forense, 2021, p. 106.
[14] MULHOLLAND, Caitlin - A tutela dos dados pessoais sensíveis, op. cit., p. 123.

de dados sensíveis aos dados pessoais, ainda que não sejam sensíveis, pois mesmo conceitualmente não sendo, podem vir a ser, conforme preleciona o artigo 11, parágrafo I da LGPD. Um exemplo disso, é quando se obtém domínio sobre localização geográfica, histórico de compras, de pesquisas, conteúdos de leitura etc, e o tratamento desse conjunto de informações pessoais podem identificar praticamente qualquer perfil humano, desde orientação sexual até opinião política.

O dano previsto no artigo 11 da LGPD é exigido no texto, entretanto deve-se tomar cuidado ao interpretar para que tal interpretação não obstrua ou mitigue a aplicação da lei, sendo certo que caso haja tratamento de dados sensíveis não taxados no artigo 11, inciso I e II da LGPD, deve-se entender que o dano é presumido por violação aos princípios fundamentais da dignidade de pessoa humana, à vida privada, à imagem, sem a perda da independência da proteção de dados.

Ao comparar o artigo 7º da LGPD, que trata de dados pessoais em geral e o artigo 11 da mesma lei, percebe-se a convergência de várias orientações, tendo em sua base legal o consentimento para o tratamento adequado dos dados, pontuando outras atividades, como é o caso de observância à obrigações legais por quem está controlando ou tratando os dados. Portanto, dados podem ser usados pela administração pública, para análise executiva de políticas públicas contidas em lei, contratos ou regulamentos legais. Do mesmo modo, dados podem ser usados por órgãos de pesquisas, que realizará estudos sociais, observando sempre que possível, a anonimização. Podem ser usados também para a proteção da vida, da saúde etc.

A diferença existente entre esses artigos, reside no fato de o artigo 11, inciso I, estabelece restrição ao consentimento, devendo ser de forma “específica e destacada, para finalidades específicas”. Os pressupostos do inciso V, IX e X do artigo 7º da LGPD não foram mencionados no artigo 11. Neste artigo, há a hipótese de tratamento de dados sensíveis sem o consentimento do proprietário dos dados, quando estes forem indispensáveis à execução de políticas públicas legais. Interesses relevantes previstos em lei, não se faz necessário o consentimento do titular dos dados, pois após a ponderação, verifica que o interesse público se sobrepõe ao interesse particular, mesmo este sendo direito fundamental. Entretanto, a professora Caitlin Mulholland critica essa orientação, dizendo que “especialmente se considerarmos que a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de direitos fundamentais, tais como os da igualdade,

liberdade e privacidade".[15]

A lei também faz uma ressalva, em seu artigo 11, inciso II, alínea "g", ao tratamento de dados sensíveis sem o consentimento, quando existe a possibilidade de prevenir fraude e insegurança do titular nos métodos de cadastramento e identificação em sistemas eletrônicos, sendo assegurados os direitos transcritos no artigo 9º da LGPD. No que diz respeito à saúde do titular, o artigo 11, parágrafo IV, proíbe a comunicação dos dados sensíveis relacionados à saúde com finalidade de obter vantagem econômica. Entretanto, as exceções constam prestações de serviço de saúde, assistências seja farmacêutica, seja de saúde, considerado o artigo 11, parágrafo 5º, abrangendo também terapias, serviços auxiliares de acordo com a necessidade dos titulares dos dados, permitindo também a: I - a portabilidade de dados quando solicitada pelo titular; II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

Ainda sobre a saúde, o artigo 13 da LGPD autoriza o tratamento de dados para pesquisas e estudos em temas relacionados à saúde pública, com ressalvas, visando melhoramento da mesma. Tais dados devem ser cuidadosamente analisados, mantendo-se em ambiente controlado e seguro, obedecendo as condutas de segurança e regras previstas no regulamento, bem como o anonimato e pseudonimização, além da observância do modelo íntegro que envolvem estudos e pesquisas, como aqueles contidos no Código de Ética e princípios de Bioética, normas internacionais e regulamentações sanitárias. Não é permitida a disponibilidade dos dados pessoais à terceiros ou entidades não autorizadas, sendo imputada total responsabilidade sobre o tratador dos dados que estão sob estudo ou análise.

Conclui-se, portanto, que a proteção normativa aos dados pessoais e aos dados pessoais sensíveis se encontra em caminhos extremamente árduos.

### 3.2 - Direito eletrônico e direitos fundamentais

A Constituição Federal de 1988, expressa os direitos fundamentais em seu Título II, subdividindo-o em cinco capítulos: Dos Direitos Individuais e Coletivos (art. 5º); Dos Direitos Sociais (6º ao 11º); Na Nacionalidade (12º e 13º); Dos Direitos Políticos (14º a 16º); Dos Partidos Políticos (17º) (BRASIL, 1988).

Classificando em quatro gerações distintas, na qual a primeira geração é decorrente da Declaração Universal dos Direitos Humanos, alçando os direitos à vida, integridade física,

[15] MULHOLLAND, Caitlin. - A tutela dos dados pessoais sensíveis, op. cit., p. 128.

liberdade, igualdade e propriedade; a segunda geração característica do século XX, reconhece os direitos sociais do trabalho, habitação e saúde; os de terceira geração (*fraternité*), que consiste nos direitos difusos, coletivos e individuais homogêneos, e por fim os de quarta geração, que contempla os direitos de gerações futuras, tem-se que os direitos fundamentais coexistem de forma harmônica, mostrando-se como orientador para a solução das controvérsias decorrentes do Direito Eletrônico, configurando-se como em instrumento de integração normativa, através da hermenêutica jurídica.

Frente ao exposto, tem-se que o delineamento acerca da proteção necessária à intimidade, honra, imagem, nome, manifestação do pensamento, marca, propriedade, no ambiente do cibernético consiste na abrangência da efetividade do Direito Eletrônico.

Acerca do direito eletrônico Paci (2017, s/p) dispõe que: "A informática jurídica ou direito eletrônico é a ciência que estuda a utilização dos elementos físicos eletrônicos, como o computador, no Direito; isto é, a ajuda que este uso presta ao desenvolvimento e aplicação do direito. Em outras palavras, é o instrumental necessário a utilização da informática no Direito. O Direito Eletrônico, digital ou da Informática não se dedica apenas ao estudo do uso dos aparatos da informática como meio auxiliar ao direito, delimitado pela informática jurídica, mas, ao contrário, constitui o conjunto de normas, aplicações, processos, relações jurídicas que surgem como consequência da aplicação e desenvolvimento da informática, isto é, a informática é geral deste ponto de vista e da forma como é regulado pelo direito".

Assim, o direito eletrônico objetiva a regulação das relações realizadas entre indivíduos no ambiente virtual, de forma a viabilizar o controle bem como a fiscalização das relações dos mais diversos meios de comunicação, inclusive os da própria informática. Á vista disso, tem-se que as normas constitucionais aplicam-se aos eventos cibernéticos.

Ademais, o resguardo dos direitos eletrônicos visa a consolidação dos direitos fundamentais, visto que conforme dispõe a Constituição Federal de 1988, ninguém sofrerá interferências na sua vida privada (seja na família, lar, correspondência), tampouco ataques à honra e reputação (Declaração Universal dos Direitos Humanos, art. XII e Constituição Federal, art. 5º, X, XI e XII) (BRASIL, 1988).

Frente ao exposto, o fato de impedir que outra pessoa utilize a imagem de terceiro sem autorização tem como finalidade resguardar a proteção de seu status naturalístico perante a sociedade, bem como garantir os direitos à vida privada e imagem, contidos no artigo 5º, inciso X da Constituição Federal, bem como no artigo 26º, nº 1 da Constituição Portuguesa.

### 3.3 - A figura do Stalking

A liberdade de ir e vir, e bem-estar perante a uma sociedade, são requisitos básicos para se ter inteiramente respeitada a dignidade humana. Não é uma realidade distante, que diariamente pessoas no mundo inteiro têm seus direitos prejudicados, principalmente o de ir e vir, por inúmeros motivos que muitas vezes essa restrição não vem por parte do Estado, mas sim daqueles que fazem parte da sociedade.

No entanto, se a notícia falsa, "apesar de relevante para a sociedade, sacrifica-se o direito de informação, ou se a notícia é verdadeira, mas sem relevância pública, sacrificar-se-á igualmente o direito de informação" (NICOLODI, 2007, p. 26).

Essa afirmação deve ser aceita com ressalvas, eis que em relação à veracidade informativa, outros fatores devem ser sopesados, como a ciência da "inverdade da notícia, o fato de o jornalista não tê-la checado devidamente, ter agido de má fé, além de ter que se levar em conta o fato de não se exigir do jornalista a verdade absoluta dos fatos" (NICOLODI, 2007, p. 27).

É bastante comum o *stalking* ocorrer quando há o rompimento de um relacionamento entre duas pessoas. Uma das partes a partir de então, por ter sido frustrado um sentimento "amoroso", é movida pelo ódio da perda, promovendo assim ações de perseguição e controle exacerbado para com a outra parte.

"A psicologia forense classifica os *stalkers* nas seguintes categorias: rejeitado, perseguidor, retardado, vingativo, erotomaníaco e sádico. As ações dos *stalkers* são vistas como perigosas em diferentes níveis, conforme o sentimento da vítima" (BRANDT, 2014, p. 1).

O perseguidor, de início pode se utilizar de táticas simples, banais e até mesmo, aparentemente, sem indicativos de algo preocupante como ligações e mensagens românticas. Posteriormente com a insistência e a rejeição da vítima, passa a se tornar inconveniente, perturbador, e as ações do *Stalker*, ainda mais intensas e gravosas como publicação de boatos em sites da *internet* para chamar atenção da vítima, mesmo que de forma negativa.

É comum também quando o *stalker* tem traços mais doentios, o envio de presentes indesejados, encomendas que podem ter conteúdo ameaçador, frequentar lugares que a vítima frequenta para coletar detalhes do cotidiano ou até mesmo ter o contato forçado. Muitas vezes resultando dano à integridade psicológica e emocional, restrição à sua liberdade de locomoção ou lesão à sua reputação.

No cenário mundial, as soluções para os problemas colocados devem ser tratadas pelo

direito internacional, ou tratados e convenções, exigindo a adoção de instrumentos jurídicos internacionais adequados. A Convenção sobre o Cibercrime (2001), e o seu objetivo no Protocolo Adicional deve responder a este desafio, com o devido respeito aos direitos humanos na nova sociedade da informação. Ambos os textos contêm disposições relativas às seguintes infrações: acesso ilegal, a interceptação ilegal, interferência de dados, interferências, má utilização dos dispositivos, falsificação, fraude, pornografia infantil (artigo 9 º da Convenção sobre a Cibercriminalidade) e contra o racismo e a xenofobia na internet.

Nos artigos da referida Convenção, tutelam a integralidade corporal e psicológica da pessoa, punindo aquele que, por sua conduta ou comportamento, cause danos às funções biológicas, anatômicas, fisiológicas ou psíquicas de terceiros. O legislador estabelece uma conduta determinada para que o crime se configure, onde o nexo causal entre uma ação do autor acabe causando danos e a efetiva ofensa à integridade psicológica ou física ou quando ocorre a invasão da privacidade da vítima, onde o elemento subjetivo é a vontade do agente de perseguir, conturbar, perturbar, invadir a esfera íntima do sujeito. O crime é consumado quando a pessoa tenta perturbar a vida ou a prejudica de alguma forma, causando ao polo passivo profundo abalo.

Muitas pessoas deixam-se vulneráveis ao assédio on-line, não observando se o Provedor de Serviços de Internet (ISP) tem uma política aceitável que proíbe *cyberstalking*, o desvelo do estado da sua conta do cartão de crédito, sobre as compras que faz. No caso de alguma irregularidade, deve-se notificar o banco.

Cabral (2011, s/p) exemplifica: “Atualmente, o termo *paparazzi* está intimamente associado a um fotógrafo de comportamento mais agressivo, que assedia, persegue (*stalking*) ou se intromete indevidamente na vida das celebridades, com o intuito de obter lucros à custa da intimidade alheia. Dessa forma, a celebridade acaba por ter sua privacidade invadida, tanto em relação a assuntos de interesse público relacionados à sua atividade profissional, quanto a assuntos de interesse particular”.

Outra modalidade de *stalking* muito comum que se mostra presente há longos anos na história de nossa sociedade, e tido como algo aceitável e tolerável, é a praticada pelos até então chamados *paparazzi*, em regra, um vocábulo de procedência italiana, empregado para definir os repórteres fotográficos que trabalham registrando fotos e momentos íntimos, familiares, pessoais de indivíduos famosos sem permissão, tornando esse fato público, após noticiar na imprensa as fotografias indesejadas, invadindo assim a vida e privacidade de pessoas tidas como celebridades.

Entretanto, não se pretende dizer que o trabalho jornalístico do *paparazzi* deve ser

censurado ou mitigado, mas apenas que seja observado os limites legais para que não seja classificado como atividade ilícita quando for exercido na vida particular das pessoas. Sabe-se, portanto, que o Brasil é um Estado Democrático de Direito, no qual garante a liberdade de expressão. Sabe-se também que a informação e comunicação exercidos por meios midiáticos são importantes para contribuir com as liberdades sociais e individuais, além de contribuir com a ordem social.

Durante séculos, comportamentos que caracterizaram *stalking*, eram tidos como atos românticos, amorosos e apaixonados, abrindo alas permissivas para a persistência despótica de expressões afetuosas não pactuadas pela outra parte. Transparece a capacidade de demonstrar a qualquer custo afectos dominantes à outra pessoa, e, de maneira sutil, a construção social colaborou para a estrutura do *stalking*. Portanto, a fronteira que determina o que é aceito socialmente como "romantismo" e o que configura *stalking*, é milimétrica. A maior prova disso é o fato de que as vítimas desse comportamento abusivo e as vezes assediador, são por vezes taxadas pelo termo "vitimistas", isto é, favorecimento pessoal relacionado a sensação de quem está sob opressão, maus-tratos, discriminação etc.

Ainda assim, a tipificação do *Stalker* ainda é um desafio para a maioria dos legisladores e investigadores, visto a dificuldade de traçar os limites do que de fato é aceito como "romântico" e o que é de fato "invasivo", dada a natureza labiríntica que compõe diversas ações individuais que se perpetuam no tempo.

Casos reais que repercutiram no mundo todo, fizeram legisladores, juristas e autoridades ponderarem a tipificação do *stalking*, como forma de intimidar e qualificar esse crime. Na década de 90, cinco mulheres foram assassinadas vítimas de *stalking* em um intervalo de 1 ano, com maior repercussão dada a morte da atriz Rebecca Schaeffer, morta com um tiro a queima roupa no peito, após mais de 3 anos de intensa perseguição por Robert John Bardo. Tal tragédia culminou na legislação sobre o tema no Estado da Califórnia que aprovou a lei *anti-stalking*, passando a vigorar no dia 1 de janeiro de 1991 (WIKIPÉDIA, 2021ª).

Nos Estados Unidos, o '*stalking*' é registrado como o vilão causador por danos sociais e físicos a milhares de mulheres e homens todos os anos. Brandt (2013), comenta que na Inglaterra, e em outros países europeus os registros das autoridades policiais referem, anualmente, cerca de 600 mil homens e 250 mil mulheres, vítimas de crimes como a invasão de privacidade, ofensa à reputação e danos à integridade psicológica e emocional.

Pode-se citar também como exemplo o caso do assediador da rainha pop Madonna, que em 2012 estava com medo por sua vida pela segunda vez, como o homem que foi

condenado por persegui-la nos anos 90 escapara da instituição mental onde ele fora encerrado. Robert Dewey Hoskins foi considerado uma ameaça e sentenciado primeiro a 10 anos de prisão por perseguir Madonna em 1996. Ele tinha sido obcecado com a *'Material Girl'* por anos, quando ele pulou a cerca da casa da cantora em Hollywood Hills. Oskins era um homem violento e tinha dito que ele iria se casar com Madonna ou "cortar a garganta de orelha a orelha". Hoskins serviu o seu tempo e mais tarde foi transferido para um hospital psiquiátrico após a outra prisão, mas escapou da instalação no início de 2012. Ele foi detido pela polícia em fevereiro e levado de volta para o Hospital Estadual Metropolitano em Norwalk, Califórnia (STALKER..., 2012). Em terras portuguesas, a palavra "*stalking"* passou a ser conhecida após o vocalista da banda UHF, Antônio Manuel Ribeiro, relatou que foi perseguido por uma fã durante 6 anos, fato que cessou apenas com um processo judicial (RODRIGUES, 2014).

A gravidade desses casos são alguns dos milhares de exemplos que acontecem todos os dias, em pequenas ou grandes proporções, em quase todos os países do globo. Com o advento da tecnologia, o *cyberstalking*, forma digital de *stalking*, ganhou força e se configura atualmente na maioria das vezes em redes sociais. Isso porque hoje, a maioria dos jovens vivem duas vidas, a saber, uma digital e outra real. Quanto mais preenche-se com fotos, informação, conteúdo nas redes, mais se estar favorecendo comportamentos abusivos de pessoas determinadas a uma espécie de "perseguição virtual".

Ainda que as redes sociais e todos os outros tipos de sistemas tecnológicos garantam privacidade e proteção de dados, nunca configura o mesmo nível de privacidade que se tem na vida real.

Quando os tribunais são chamados pelas vítimas a intervir, as decisões judiciais passam, na maioria das vezes, por proibir a aproximação física entre o alvo e o agressor.

Em estudos mais específicos através da Resolução 1962 da Assembleia Parlamentar do Conselho da Europa, pode se verificar que cerca de 10% da população europeia já tenha sido vítima desse crime, o que levou atualmente a Europa a possuir algumas leis *anti-stalking* em nove países: Alemanha, Áustria, Bélgica, Dinamarca, Holanda, Irlanda, Itália, Malta e Reino Unido (EURONEWS, 2013).

Seguindo em acordo com a Associação Portuguesa de Apoio à Vítima, é sabido que antes de 2014, algumas das condutas relacionadas ao conceito de assédio persistente já se encontram tipificadas no Código Penal português, porém de maneira esparsa.

Com o advento das evoluções tecnológicas de maneira assustadoramente rápida,

pressão midiática e a influência da Convenção de Istambul[16], entendeu-se que era imprescindível a criação de um tipo independente para suprir as lacunas deixadas pelo legislador, haja vista que em Portugal, não havia uma legislação específica. Porém em setembro de 2014, os deputados do Grupo Parlamentar do Bloco de Esquerda apresentaram o seguinte projeto de lei, após o apelo da Assembleia Parlamentar do Conselho da Europa, leis[17] mais especificas relacionados ao crime de *stalking*[18], tipificado como perseguição.

Destaca-se a palavra "reiteração" que consiste na prática contínua de atos que caracterizam o crime ou contribuem para a sua formação e evolução. Além disso, o conjunto de fatos deve ser analisados em sua totalidade, enfatizando o caráter intimidatório da vítima.

Em resumo, o acórdão da decisão do Tribunal de Guimarães negou o recurso penal 332/16.6PBVCT.G1 com justificativa de que:

> Comete o ilícito do artº 154º-A, nº 1 do CP, com dolo directo o arguido que, de forma reiterada, contactava telefonicamente a ofendida, a horas diversas, perturbando quer o seu desempenho profissional, quer o seu descanso; deslocava-se ao seu local de trabalho, procurando encontrar-se com ela; entregava quase diariamente no local de trabalho de ofendida cartas e sacas de papel com embrulhos dentro para serem entregues àquela; deslocava-se, com frequência, à residência da ofendida, ora para colocar bilhetes no pára-brisas do seu automóvel, ora aguardando a sua chegada, quer à porta da entrada do prédio, quer à porta da garagem, ora, então, rondando-a, para controlar a sua rotina diária; agindo com o propósito de provocar à ofendida medo e prejudicar e limitar os seus movimentos, bem sabendo que desse modo a lesava na sua liberdade pessoal, como pretendeu e conseguiu. Portanto ficou provado que o "o arguido agiu de forma livre, deliberada e conscientemente, ciente que a sua conduta era proibida e punida por lei". (Processo 332/16.6PBVCT.G1. Relator: ALDA CASIMIRO. Acórdão: Tribunal de Guimarães, data de julgamento 05/06/2017) (TRIBUNAL DA RELAÇÃO DE GUIMARÃES, 2017, s/p).

No Brasil, o Código Penal tipifica na seção I dos crimes contra a liberdade individual,

[16] É um acordo entre países do bloco europeu que faz parte do Conselho da Europa e visa combater a violência contra a mulher e a violência doméstica. Estreou na cidade de Instambul, Turquia, em 11 de maio de 2011 (WIKIPÉDIA, 2020ª).

[17] Art. 154º - A 1 - Quem, de modo reiterado, perseguir ou assediar outra pessoa, por qualquer meio, direta ou indiretamente, de forma adequada a provocar-lhe medo ou inquietação ou a prejudicar a sua liberdade de determinação, é punido com pena de prisão até 3 anos ou pena de multa, se pena mais grave não lhe couber por força de outra disposição legal. 2 - A tentativa é punível. 3 - Nos casos previstos no n.º 1, podem ser aplicadas ao arguido as penas acessórias de proibição de contacto com a vítima pelo período de 6 meses a 3 anos e de obrigação de frequência de programas específicos de prevenção de condutas típicas da perseguição. 4 - A pena acessória de proibição de contacto com a vítima deve incluir o afastamento da residência ou do local de trabalho desta e o seu cumprimento deve ser fiscalizado por meios técnicos de controlo à distância.
5 - O procedimento criminal depende de queixa. (DECRETO-LEI n.º 48, 1995, s/p).

[18] Luz (2012, p. 6) assevera que "as condutas deveriam ser repetidas, praticadas de maneira reiterada, livre e consciente. A continuação e recorrência durante um período de tempo definido é, pois, um elemento constituinte do tipo objetivo do crime. Podemos considerar, portanto, que é um crime de trato sucessivo, pois que se caracteriza pela repetição de condutas essencialmente homogéneas unificadas por uma mesma resolução criminosa."

um rol que por si só, não bastaria para a configuração do *stalking*, visto a são crimes muito genéricos para a sua caracterização. A Lei Maria da Penha (nº 11.340/06) pode se adequar aos casos de *stalking* se for configurado no ambiente familiar, conforme disposto no art. 5º: "Art. 5º. Para os efeitos desta Lei, configura violência doméstica e familiar contra a mulher qualquer ação ou omissão baseada no gênero que lhe cause morte, lesão, sofrimento físico, sexual ou psicológico e dano moral ou patrimonial: I - no âmbito da unidade doméstica, [...] II - no âmbito da família, [...] III - em qualquer relação íntima de afeto, [...]" (BRASIL, 2006, s/p, grifo nosso).

Se o fato causar dano a mulher no seio familiar, afetivo ou doméstico, cabe a tipificação nessa lei. Entretanto, casos em que exista perseguição obsessiva, não configura o tipo legal previsto nos artigos expostos.

No ano de 2013, o primeiro caso de aplicação dessa lei aconteceu no estado de São Paulo, onde uma adolescente de 13 anos era perseguida por um rapaz de 18. Após a família da moça perceber as atitudes do autor eram obsessivas, ajuizou uma ação exigindo o pagamento de 2.000 (dois mil reais) de multa pela ameaça. O rapaz não desistiu, pois percebeu que a justiça ficara inerte e nada cobrou, incentivando-o indiretamente a continuar ameaçando a jovem.

O caso só foi solucionado em 2018, quando a advogada da família baseou a tese de que o jovem acreditava que havia relação entre o ele e a moça, fato que configurou a aplicação da Lei Maria da Penha (BRANDALISE, 2020).

Recentemente no Brasil, o *stalking* era uma contravenção penal, ou seja, infração penal de menor potencial ofensivo e é enquadrado no art. 65 do Decreto-Lei nº 3.688 de 1941, que afirma: "molestar alguém ou lhe perturbar a tranquilidade, por acinte ou por motivo reprovável: Pena – prisão simples, de quinze dias a dois meses, ou multa, de duzentos mil réis a dois contos de réis" (BRASIL, 1941, s/p).

Ao analisar o artigo em questão, percebe-se a quão branda é a pena de quem comete tal crime que facilmente pode evoluir para algo mais grave como ameaça e até mesmo a morte. Fora isso, ainda se torna mais adequado um tipo específico para a infração penal.

Um fato curioso aconteceu na 3ª Turma Criminal do Distrito Federal no ano de 2020 no caso julgado contra um autor de *stalking*[19] em que lhe recaiu a pena de contravenção penal

[19] APELAÇÃO CRIMINAL. CONTRAVENÇÃO PENAL DE PERTURBAÇÃO DA TRANQUILIDADE. VIOLÊNCIA DOMÉSTICA E FAMILIAR. AUTORIA E MATERIALIDADE COMPROVADAS. STALKING POR MEIO DE REDES SOCIAIS. DOSIMETRIA. REGIME SEMIABERTO. RÉU REINCIDENTE E COM MAUS ANTECEDENTES. REPARAÇÃO DO DANO À VÍTIMA. DANO MORAL IN RE IPSA. NECESSIDADE E ADEQUAÇÃO DA INDENIZAÇÃO COMPROVADAS. 1. Comprovadas a materialidade e

do art. 65.

Observa-se que no texto da ementa, há a palavra *"stalking por meio de redes sociais"*, causando a falsa impressão de que essa modalidade de *stalking* está tipificada em alguma lei. O caso em tela se tratava do ex-companheiro da vítima, que o denunciou depois que descobriu que ele criava contas falsas em redes sociais para perseguir a vítima. O Brasil até então não tinha sequer um enquadramento específico para o crime de *stalking*. A Lei nº 14.737/12 visou tipificar a perseguição obsessiva, sendo sancionada pelo Presidente em 2012 e acrescentou o art. 147-A[20] ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais).

O novo crime trata-se de uma ação penal pública condicionada, onde o sujeito ativo é o *"stalker*" e o sujeito passivo a vítima perseguida, tendo em vista que a ação deve ser representada pela vítima. Vale salientar, a previsão do caráter de reparação, haja vista ser de interesse do destinatário da violência a ponderação sobre os custos pessoais a serem enfrentados pelo processamento da demanda judicial, uma vez que, não raras exceções, o agente perseguidor é pessoa de convívio próximo da vítima.

Já dizia o professor Damásio de Jesus (2009, p. 68): "[...] quanto a eventual criação de figura específica, possivelmente na qualidade de crime subsidiário para a conduta do *"Stalking"*. Essa infração penal, de subsidiariedade expressa, poderia afastar as contravenções penais em caso de *"Stalking"* e até mesmo alguns crimes de pequena gravidade, cuja pena venha a ser menor do que aquela a ser atribuída ao *"Stalking"* ou "Assédio por Intrusão". A pena a ser prevista poderia ter um patamar superior a 2 anos em seu máximo abstratamente

---

a autoria delitivas da contravenção penal de perturbação da tranquilidade, por acervo probatório harmônico, a condenação é medida que se impõe. 2. A perturbação da tranquilidade e da incolumidade psíquica da vítima, efetuadas sistematicamente pelo ex-companheiro por meio de mensagens em redes sociais, utilizando-se de perfis falsos, caracteriza a contravenção do art. 65 do Decreto-Lei 3688/41, por *stalking*. 3. Nos crimes praticados no âmbito da violência contra a mulher, por motivação de gênero, a palavra da vítima merece especial relevo, conforme remansosa jurisprudência deste Tribunal de Justiça. 4. Os critérios legais para fixação de regime dispostos no art, 33, § 2º, alínea "b"; e § 3º, determinam o regime inicial semiaberto para o réu reincidente e com circunstâncias judiciais desfavoráveis, por ser portador de maus antecedentes. 5. Recurso conhecido e não provido. (Acórdão 1249363, 00041942920188070006, Relator: WALDIR LEÔNCIO LOPES JÚNIOR, 3ª Turma Criminal, data de julgamento: 14/5/2020, publicado no PJe: 22/5/2020. Pág.: Sem Página Cadastrada) (DISTRITO FEDERAL, 2020, s/p).

[20] Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. § 1º A pena é aumentada de metade se o crime é cometido: I – contra criança, adolescente ou idoso; II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código; III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma. § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência. § 3º Somente se procede mediante representação (BRASIL, 1940, s/p).

cominado, ensejando o afastamento de contravenções penais e crimes de menor potencial ofensivo em casos de conflito aparente de normas (Princípio da Subsidiariedade)".

Sem dúvidas foi um grande progresso para suprir a lacuna que deveria ter sido sanada há anos, principalmente pelo fato de que o Brasil, segundo dados da *Global Web Index*, ter a quinta maior taxa de feminicídios por 100 mil mulheres em todo o mundo, além de ser o segundo país que mais usa redes sociais (DUARTE, 2019).

### 3.4 - O hacker e a invasão de dispositivos

Em primeiro momento, faz-se importante diferenciar os *Hackers* e os *Crackers* para que haja maior entendimento acerca dos assuntos abordados adiante. "Os *hackers* têm amplo conhecimento em computadores e *internet* e atuam junto com a justiça e com a polícia, a fim de detectarem, identificarem e, então, combaterem a ação dos criminosos virtuais. Já os crackers são os responsáveis pelos crimes virtuais, ou crimes da rede, os quais utilizam os seus conhecimentos sobre os computadores e a *internet* para prejudicar, em algum aspecto, outros indivíduos" (ROSSINI, 2004, p. 110).

Segundo Augusto Rossini (2004, p. 110) descreve: "[...] o significado de "delito informático" poderia ser apontado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, fazendo o uso da *internet*, utilizando o ambiente de rede ou distante dele, e que ofenda de forma direta ou indiretamente, a segurança da informática, que tem por elementos a integridade, a disponibilidade a confidencialidade".

Com relação aos delitos informáticos, são contravenções penais, não somente no âmbito da informática e sim em qualquer conduta que possa ter relação com os sistemas informáticos. Portanto, se resume crime informático sempre que o computador for um instrumento para a prática de um crime. Ademais, o autor descreve "o delito informático é gênero, do qual delito telemático é espécie, dada a peculiaridade de ocorrer no sistema e a partir do inter-relacionamento entre os computadores em rede telemática usados na prática delitiva". (ROSSINI, 2004, p. 110).

Para Feliciano (2000, p. 42): "Conheço por criminalidade informática o recente fenômeno histórico-sociocultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.)".

Portanto, segundo a Organização para a Cooperação Econômica Desenvolvimento da

ONU “O crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento de dados e/ou transmissão de dados” (ROSSINI, 2004, p. 109).

Como já explanado, a invasão de privacidade é outra forma de uso ofensivo das tecnologias. O *hacker* pode ser qualquer pessoa se tiver conhecimento básico, desejo, motivação e (às vezes) algum dinheiro, adentra a vida dos usuários que estão conectados de alguma forma nas redes. Além dessas características, o *hacker* de sucesso deve ter uma grande dose de paciência e capacidade de planejamento. No entanto, nem todos os *hackers* são todos iguais, nem todos os *hackers* têm os mesmos objetivos. Eles são geralmente classificados em três grupos principais: *hackers black hat*, *hackers white hat* e *hackers gray hat*. Um *hacker white hat* é uma pessoa que tenta encontrar vulnerabilidades de segurança de computador e explorá-las para ganho financeiro pessoal ou outros motivos maliciosos (SILVEIRA *et al*., 2017).

Um *hacker white hat* é um especialista em segurança de computador que invade sistemas e redes protegidos para testar e avaliar sua segurança. Eles usam suas habilidades para melhorar a segurança, expondo vulnerabilidades antes que *hackers* maliciosos (conhecidos como *hackers black hat*) possam detectá-los e explorá-los. Há o terceiro grande grupo, *hackers gray hat* é alguém que pode violar os padrões ou princípios éticos, mas sem a intenção maliciosa atribuída aos *hackers black hat.*

Os *hackers* de “chapéu cinza” geralmente operam para o bem comum. Na prática, nas comunicações, o termo: “Hacker ético” também pode ser ouvido, mas a discussão sobre ética pode ser um terreno amplo e escorregadio. É ético espionar os próprios filhos “para o seu bem”? Portanto, permaneceremos no grupo nomeado. É interessante que todos usam as mesmas ferramentas e métodos, e a principal diferença está em seus objetivos e resultados (SILVEIRA *et al*., 2017).

Por outro lado, os *hackers* podem ser divididos em vários grupos de acordo com seus conhecimentos e habilidades. O nível mais alto consiste em hackers que sabem exatamente o que fazem, que estão muito familiarizados com o sistema e são capazes de criar o software apropriado, incluindo vírus e outro *malware*. O nível médio é formado pelos chamados “técnicos” que estão aptos a utilizar ferramentas que podem ser adquiridas no mercado de software e hardware. O terceiro, o nível mais baixo de *hackers*, consiste nos chamados *“script kiddies”*. Um *script kiddie* é um termo depreciativo para os mais imaturos, mas, infelizmente, muitas vezes tão perigoso explorador de falhas de segurança na Internet. Eles exploram as fraquezas dos computadores da *internet,* muitas vezes de forma aleatória e com pouca consideração ou talvez até mesmo compreensão das consequências potencialmente

prejudiciais. (MENEZES; PRETTO, 2019).

Em relação aos métodos de hackear os dados podem ser roubados de várias maneiras, desde o roubo brutal de todo o computador, passando pela cópia de conteúdo de discos rígidos, até métodos sofisticados de acesso remoto. A maneira mais fácil é roubar dados de dentro. Pode fazer funcionários permanentes insatisfeitos com as condições de trabalho, funcionários temporários ou em regime de meio período, ou mesmo um funcionário responsável pela segurança e manutenção do sistema.

O acesso pode ser fornecido através da chamada porta dos fundos. Se ele fornece uma conexão externa constante e no cabo colar uma etiqueta "Segurança - Não desconectar" é provável que ninguém interfira nesta conexão até a nova reconfiguração do sistema. Em todas essas ações, é necessário um contato físico direto com o dispositivo. Os ataques realizados na rede são mais sofisticados e geralmente incluem busca por uma porta de acesso aberta, endereços de e-mail e senhas, *DDoS*, acesso a servidores de arquivos, brechas no *firewall* etc. Uma possibilidade é o uso de *backdoors*[21] deixados abertos por muitos fabricantes para efeito de controle dos produtos.

O desenvolvimento de software e hardware pode ser um trabalho bastante enfadonho. Essas atividades requerem testes frequentes, reconfiguração, conexão de diferentes contatos e/ou partes de programas, solução de problemas e assim por diante. Se alguma alteração exigir autenticação, isso reduzirá significativamente a eficiência do trabalho. Portanto, os desenvolvedores inicialmente deixam em aberto a possibilidade de aplicar vários golpes, apenas por eles conhecidos, comandos que pulam certas fases do trabalho. Eles são chamados de "*easter eggs*[22]". Como regra, esses controles devem ser excluídos do código do programa à medida que o trabalho é concluído.

No entanto, muitas vezes, os *easter eggs* permanecem no software. Ao testar diferentes combinações de teclas, ou por erro do usuário, ou acidentalmente, os usuários podem encontrá-las e usá-las. Como exemplo, podem ser usados atalhos de teclado para Microsoft Word no Windows.

Para realização do hackeamento, é inevitável o uso da engenharia social. Existe uma variedade de soluções diversas e imaginativas, mas uma das mais estúpidas e mais frequentemente aplicadas é que, por e-mail, o atacante solicita o fornecimento de informações pessoais de sua vítima, incluindo a senha para o endereço de e-mail especificado.

---

[21] Sistema usado para proteger computadores, atuando como uma "porta dos fundos" para possíveis ataques em rede. (WIKIPÉDIA, 2020[b]).

[22] São chamados de pegadinhas virtuais, pois escondem alguns segredos dentro de sistemas operacionais, websites, programas etc. (WIKIPÉDIA, 2020[c]).

É desnecessário dizer sobre as possibilidades que o invasor ganha usando esses dados. Este *hack* é baseado no envio de e-mails em massa. Um dos mais usados é a variante em que uma pessoa pretende ser a vítima. Por exemplo: um atacante, usando um telefone celular descartável, liga para a vítima se passando por um representante do provedor de serviços de Internet ou banco no qual a vítima tem uma conta. O atacante explica à vítima que há algum problema com a conta que a operadora não pode resolver sem a ajuda do titular, precisando assim da seus dados e senha.

A vítima surpreendida geralmente informa sua senha. O fraudador pode continuar oferecendo ajuda para o pagamento de contas pendentes se a vítima fornecer as informações do cartão de crédito etc.

Frente a isso, tem-se que os avanços na tecnologia são acompanhados por metodologias de ataque em constante evolução, usadas por hackers, que estão se tornando cada vez mais sofisticadas. A definição de um *hacker* é alguém que utiliza seu conhecimento técnico para invadir de forma criativa um dispositivo de computador ou rede, independentemente da intenção. Hackear em si não é ilegal, a menos que o *hacker* esteja comprometendo um sistema sem a permissão dos proprietários, resultando em *hackers* bons, ruins e questionáveis. Os *hackers* são motivados por vários fatores, incluindo curiosidade e desafio, lucro, recreação ou protesto (BISSO *et al*., 2020).

O tipo de *hacker* com o qual a maioria das pessoas está familiarizada são os 'chapéus pretos'. Esses são criminosos mal-intencionados calculados que geralmente exploram um sistema de computador ou rede para seu próprio ganho pessoal ou financeiro. Eles podem não apenas tentar roubar dados pessoais, como detalhes de cartão de crédito, credenciais de usuário e informações pessoais para chantagem, mas também podem modificar ou destruir dados. Para evitar os ataques inevitáveis desses *hackers*, metodologias de proteção mais novas e avançadas precisam ser implementadas para proteger nossos dados, exigindo pesquisa e o relatório de falhas.

As empresas não devem apenas ter medidas de segurança abrangentes, mas também podem contar com a ajuda de um 'chapéu branco', ou *hacker* ético, ou pelo menos ter um canal de divulgação para *hackers* amadores que encontrarem falhas em seus sistemas. Infelizmente, muitas empresas ainda não possuem um canal para divulgar uma vulnerabilidade e, neste caso, é mais seguro ficar omisso. Os *hackers* éticos usam seu poder para o bem, realizando testes de penetração, testando sistemas de segurança locais e realizando avaliações de vulnerabilidade. Eles estão aqui para proteger nossos dados, identificando vulnerabilidades, expondo o problema e reparando as falhas antes que o *hacker*

de chapéu negro as encontre e explore. Algumas das vulnerabilidades mais críticas da história da Internet foram descobertas e resolvidas graças aos esforços de *hackers* éticos alimentados pela curiosidade e altruísmo.

*Hackers* éticos podem trabalhar de forma independente, ser contratados diretamente por uma empresa ou agência governamental para testar seus sistemas ou para hackear produtos em desenvolvimento, ou são contratados por empresas de segurança que desenvolvem suas próprias ferramentas ou são subcontratadas por empresas. Comunidades de hackers éticos também existem, como a *Hacker One*, e essas pessoas podem participar de programas de recompensa de bugs para obter lucro. Um número crescente de empresas está oferecendo esses programas, permitindo que *hackers* ataquem um dispositivo ou rede específica em troca de uma recompensa substancial por qualquer falha que encontrem e revelem. *A Apple Inc.*, por exemplo, está oferecendo recompensas de até US $ 200.000 para *hackers* que encontrarem e relatarem vulnerabilidades em seus sistemas. O pentágono Norte Americano também foi aberto para *hackers* e corrigiu mais de 3.000 bugs, pagando mais de US $ 300.000 (BISSO *et al*., 2020).

Muitas habilidades necessárias para hackear se sobrepõem às habilidades exigidas por um cientista de dados. Embora eles possam não ter experiência em matemática e estatística, eles tendem a ter um amplo conjunto de habilidades, incluindo excelentes habilidades de programação, e usam criatividade e engenhosidade para construir coisas e encontrar soluções inteligentes. Além de *hackers* éticos, os cientistas de dados também estão fazendo sua parte para combater o *hacker* de chapéu preto. A ciência de dados está sendo usada de forma positiva nas áreas de intrusão e detecção de vírus e *malware*, criando uma abordagem mais preditiva para detectar violações. Uma abordagem automatizada desenvolvida por cientistas de dados também foi desenvolvida para analisar a atividade em fóruns clandestinos de crimes cibernéticos (BISSO *et al*., 2020).

No entanto, com a ciência de dados e automação, surgem novas áreas de ataque para o *hacker*. Inteligência artificial e aprendizado de máquina são ferramentas perfeitas para o *hacker*, onde são usadas para tomar decisões sobre o que atacar, quem atacar e quando atacar. Os *hackers* também podem "brincar com o sistema" aprendendo o código usado para criar automação, manipulando o modelo e mudando o resultado a seu favor. Um exemplo de onde isso pode ser usado é na previsão de riscos ou na operacionalidade de empréstimos bancários.

Muitas violações ao longo dos anos foram encobertas ou minimizadas, com muitas empresas só divulgando h*ackers* aos clientes meses após a ocorrência da violação. Às vezes, uma falha não é divulgada até que uma correção esteja disponível, mas em muitos casos uma

empresa deseja proteger sua reputação e manter a confiança de seus clientes. Não é uma questão de saber se uma empresa terá violação de segurança, mas quando e as empresas devem estar preparadas para quando isso ocorrer. No entanto, antes que uma empresa possa pensar em se defender, ela precisa estar ciente dos dados que possui, identificar os dados mais importantes e confidenciais em seus sistemas e saber onde eles estão armazenados (VARANDA, 2019).

No que se refere as ameaças à segurança as mesmas podem ser categorizadas em quatro partes e essas categorias são as formas ou formas pelas quais as ameaças podem ser realizadas em uma rede. Existem classificações (TECH FAQ, 2010) para as ameaças *hacker*.

a) Ameaças Não Estruturadas: ameaça à segurança não estruturada é o tipo de ameaça criada por uma pessoa inexperiente que tenta obter acesso a uma rede. Eles normalmente usam ferramentas comuns de *hacking*, como scripts de *shell* e crackers de senha. Uma boa solução de segurança deve impedir facilmente esse tipo de ataque. Em outras palavras, esses tipos de *hackers* não podem ser subestimados porque podem causar sérios danos à rede;
b) Ameaças Estruturadas: ao contrário das ameaças não estruturadas, os *hackers* de ameaças estruturadas são bem experientes e altamente sofisticados. Eles usam ferramentas sofisticadas de *hacking* para penetrar nas redes e podem invadir computadores governamentais ou empresariais para extrair informações. Em certas ocasiões, ameaças estruturadas são realizadas por gangues do crime organizado ou concorrentes do setor;
c) Ameaças Externas: algumas pessoas não autorizadas fora da empresa, que não têm acesso ao sistema de computador ou rede da empresa, podem causar ameaças externas. Eles geralmente invadem a rede da empresa por meio da *Internet* ou do servidor. *Hackers* experientes e inexperientes podem representar ameaças externas;
d) Ameaças Internas: esse tipo de ameaça pode ser feito por um funcionário insatisfeito que autorizou o acesso à rede da empresa. Assim como as ameaças externas, o dano que pode ser causado por um *hacker* depende da experiência do *hacker*.

Para os países da União Europeia, o Regulamento Geral de Proteção de Dados (RGPD) significa que a proteção de dados e privacidade estão cada vez mais rígidos e os *hackers* éticos concordam que é um passo importante para que as empresas se tornem mais seguras. O RGPD é complexo. Isso significa que as empresas devem controlar os dados que mantêm e exige a implementação de medidas para proteger os dados, incluindo como os

dados são coletados, como você prova isso e como você lida com o gerenciamento de acesso. Se uma empresa não fizer tudo o que pode para proteger seus dados e ocorrer uma violação por negligência, ou se tentar ocultar um incidente e não denunciá-lo às autoridades em 72 horas, corre o risco de ser atingida por multas altíssimas e sua imagem de marca também pode ser destruída.

Embora *hackers* éticos concordem que o RGPD é um passo importante para ajudar as empresas a se tornarem mais seguras, as multas associadas à violação do Regulamento significam que os dados se tornarão o maior ativo e o maior risco da empresa. Os hackers agora vão direcionar esses dados com mais força do que nunca, e as empresas vão ficar mais suscetíveis a ameaças de *ransomware*[23] ou extorsão com os *hackers* usando as pesadas multas RGPD como alavanca. Custa mais se recuperar de um *hacker* do que prevenir que uma invasão *hacker* aconteça em sistemas empresariais ou domésticos.

Esperançosamente, o RGPD faz com que mais empresas percebam o valor da comunidade *hacker* ética, permitindo-lhes encontrar e relatar vulnerabilidades, juntando-se a empresas como *Google Inc*, *Facebook Inc e PayPal Inc.* Apenas priorizar a segurança dará a uma empresa a melhor chance.

No contexto brasileiro da invasão de privacidade, tem-se o caso de maior repercussão envolvendo atriz, modelo e apresentadora Carolina Dieckmann teve suas fotos íntimas divulgadas em um site na *internet* sediado em Londres e depois de um tempo, várias publicações envolvendo essas mesmas fotos já tinham sido amplamente divulgadas. A Polícia Federal ao investigar o caso levantou a hipótese de que, ao deixar o seu computador pessoal na assistência técnica, o infrator conseguiu acesso a conta pessoal da atriz e consequentemente acesso às fotos pelo *e-mail.* Portanto o advogado solicitou aos principais motores de buscas a retirada dos links, o quais foram excluídos pelo *Yahoo! Inc*, mas não pela *Google Inc*. Mais tarde, em depoimento à polícia, Carolina afirmou estar sendo chantageada pelo *hacker* para que as suas fotos não fossem publicadas (WIKIPÉDIA, 2021[b]).

A então presidente Dilma Rousseff sancionou a Lei nº 12.737/2012 como resposta à comoção social e pressão midiática. Embora tenha contribuído ao complexo de normas penais brasileiras, a Lei Carolina Dieckmann não trouxe necessária eficiência no que diz respeito ao combate de crimes do gênero. Em primeiro lugar, destaca-se a pressão exercida pela mídia ao Estado brasileiro para reprimir ou tipificar a conduta criminosa do *hacker*, que culminou na

[23] "*Ransomware* é um tipo de software nocivo (conhecido também como malware) que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas". (O QUE É um ransomware?, 2019).

aprovação da lei em menos de 60 dias e, após sua publicação, demonstrou profundo desconhecimento legislativo, não apenas em matéria penal, mas também em matéria de prática investigativa para crimes dessa natureza.

O principal objetivo da lei foi preencher de forma satisfatória a lacuna que existia no ordenamento jurídico brasileiro, onde não havia tipificação penal para determinados crimes cibernéticos, muito menos se condenava algumas condutas reprováveis, em obediência ao princípio da legalidade. Portanto, ainda que amparado tardiamente pelo direito penal, não foi suficiente para suprir a grande lacuna existente no complexo normativo, quando se analisa o tipo e a punição inexpressiva de detenção de 3 meses a 1 ano, configurado então crime de menor potencial ofensivo.

A simples invasão, segunda a lei e a doutrina penal, não configura o crime pois exige a finalidade de obter, adulterar ou destruir dados e informações. Outra questão é que o artigo 154-A do Código Penal[24] não estabelece o que seria o "mecanismo de segurança", questão basilar para a tipificação da conduta criminosa, visto que, caso o dispositivo invadido não dispor de qualquer meio de proteção (senha, antivírus, *firewall* etc.), não configurará crime, ou seja, caracterizaria conduta atípica.

Não importa se o dispositivo está ou não conectado à *internet*, bastando o dolo da invasão de privacidade. Um exemplo clássico ocorre quando A, amigo de B, pede seu notebook emprestado para terminar alguma tarefa e B cordialmente concede. A, sabia que B mantinha relações sexuais com a namorada e frequentemente gravava vídeos íntimos, colocando-os no armazenamento interno do notebook. Então A, acessa a galeria de fotos e vídeos íntimos de B, salva no seu *pendrive* sem que B desconfie de algo. Posteriormente, expõe os vídeos e fotos em um site ou em aplicativos de mensagens.

Pergunta-se, então, se A cometeu o crime descrito no artigo 154-A do Código Penal brasileiro e a resposta é que não cometeu. Isso se dá ao fato de que A não se utilizou de nenhuma técnica de violação para ter o acesso completo ao dispositivo eletrônico, pois B deliberadamente o concedeu.

Em Portugal, tendo em vista a execução do Regulamento 2016/679 (RGPD), em sequência da Recomendação do Comité de Ministros do Conselho da Europa n.º R (89) 9, de 1989, criminalizou o acesso indevido relacionado à proteção de dados pessoais contido na Lei 10/91º e se manteve vigente na revogada Lei nº 67/98. Entretanto, a Lei nº 58/2019 que

[24] Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

assegura a observância do RGPD pela ordem jurídica portuguesa, estabelece em seu artigo 47º a tipificação do crime[25] de acesso indevido.

Ainda, tem-se também a figura do acesso ilegítimo, no artigo 6º, criminalizado pela Lei 109/91 que adapta o direito interno à Convenção de Budapeste sobre Cibercrime do Conselho da Europa.

Dito isso, ao analisar o contexto legislativo, ressalta-se que Brasil e Portugal são signatários do Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), que concede o direito à privacidade nos termos do artigo 17, bem como a Convenção Americana sobre Direitos Humanos (CADH), o que garante o direito à privacidade no artigo 11, nos seguintes termos: "1. **Todo mundo tem o direito de ter sua honra respeitada e sua dignidade reconhecida**. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques" (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1969, grifo nosso).

Em tempos de redes sociais e extrema divulgação da vida íntima a "extimidade", "quem revela suas intimidades (segredos) para o público, naturalmente está abrindo mão, nessa parte, da sua tutela jurídica. Esse é um campo de ausência de tutela penal, por deliberação do próprio interessado" (GOMES, 2013, p. 1).

Todas estas disposições visam permitir a obtenção ou coleta de dados para fins de investigação criminal ou processo. Os redatores discutiram se a Convenção deverá impor a obrigação de os prestadores de serviços de rotina recolher e conservar os dados de tráfego para um determinado período de tempo fixo, mas não incluem qualquer obrigação desse tipo devido à falta de consenso.

Por sua própria natureza, a colisão de direitos fundamentais se dá no âmbito dos princípios, já que "os direitos fundamentais são outorgados por normas jurídicas que possuem essencialmente as características de princípios" (RIBEIRO, 2018, s/p), e esses não se resolvem sobre o critério do conflito de regras; não há o que se falar em princípios válidos ou inválidos. Portanto quando verificada a existência de uma autêntica colisão de direitos

[25] Artigo 47º - Acesso indevido 1 - Quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados pessoais é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. 2 - A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os artigos 9.º e 10.º do RGPD.
3 - A pena é também agravada para o dobro nos seus limites quando o acesso: a) For conseguido através de violação de regras técnicas de segurança; ou b) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

fundamentais cabe ao intérprete ou aplicador realizar a ponderação dos bens envolvidos, visando resolver a colisão através do sacrifício mínimo dos interesses em jogo (FARIAS, 2001).

O Princípio da Proporcionalidade e o Princípio da Razoabilidade são elementares para remediar a colisão de direitos fundamentais e deve ter como base o Princípio da Unidade da Constituição. Dependendo da situação, esses princípios são aplicados para dar o equilíbrio necessário para a investigação dos direitos dispostos, como afirma René Ariel Dotti (1980, p. 181): "[...] as limitações reciprocamente impostas não resultam da hierarquia entre as liberdades em conflito – posto não ser adequado um critério de superposição – mas das circunstâncias em cada situação concreta".

Além disso, os autores incluíram muitas garantias processuais, o que tornará possível para evitar qualquer abuso dos procedimentos que ele define. Em primeiro lugar, o texto especifica que a introdução e a aplicação das competências e procedimentos estabelecidos na Convenção estarão sujeitas às condições e salvaguardas previstas pelo direito interno de cada Parte; tendo em conta a necessidade de uma adequada proteção dos direitos humanos, especialmente tal como definido nos instrumentos internacionais relevantes (nomeadamente a CEDH e o Pacto Internacional sobre Direitos Civis e Políticos).

No entanto, o Tribunal Europeu dos Direitos do Homem considerou que as ações do Estado a restringir o direito à liberdade de expressão foram devidamente justificadas sob as restrições do parágrafo 2º do artigo 11º da Convenção Europeia de Direitos Humanos, nomeadamente quando essas ideias ou expressões fazem violar os direitos dos outros. Portanto: "Art 11°, parágrafo 2. O exercício deste direito só pode ser objecto de restrições que, sendo previstas na lei, constituírem disposições necessárias, numa sociedade democrática, para a segurança nacional, a segurança pública, a defesa da ordem e a prevenção do crime, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros. O presente artigo não proíbe que sejam impostas restrições legítimas ao exercício destes direitos aos membros das forças armadas, da polícia ou da administração do Estado" (CONSELHO DA EUROPA, 2013, p. 12-13).

O Protocolo, com base dos instrumentos nacionais e internacionais, estabelece à medida que a divulgação das expressões racistas e xenófobas e ideias viola os direitos alheios. A definição contida no artigo 2 º refere-se a material escrito (por exemplo, textos, livros, revistas, depoimentos, mensagens etc.), imagens (por exemplo, imagens, fotos, desenhos etc.) ou qualquer outro tipo de representação de ideias ou teorias racistas e de natureza xenófobas, em um formato que possam ser armazenados, processados e enviados por meio de um sistema

de computador.

Será tornar possível a apreensão de dados por autoridade, ou proibir a pessoa que os possui de divulgá-los ou preservar os dados para os fins da investigação, mas a Convenção não exige e não pode justificar a vigilância de comunicações pessoais ou contatos por prestadores de serviço ou aplicação da lei, a menos que haja uma investigação oficial criminal.

A fim de investigar e processar essas pessoas, a cooperação internacional é vital. A Convenção sobre o Cibercrime (STE 185) foi elaborada para permitir a assistência mútua em matéria de crimes relacionados com computadores, no sentido lato, de forma flexível e moderna. A Convenção sobre o Cibercrime, foi aberta à assinatura em Budapeste em 23 de novembro de 2001 e assinado por 34 Estados europeus e não europeus, recebendo forte apoio dos legisladores e profissionais em toda a Europa e além. É o que afirma parte do preâmbulo.

No entanto, a Convenção foi criticada por diversos motivos por uma série de associações, em especial os que operam no domínio da proteção da liberdade de expressão, e também por representantes de certos ramos da indústria.

Recentemente o Brasil aderiu a Convenção de Budapeste (AGÊNCIA DE MARKETING DIGITAL, 2019) após ser convidado pelo Comitê de Ministros do Conselho Europeu a participar em 2019, com esforços de vários órgãos de segurança pública, fiscais, jurídicos etc., que contribuíram tanto para a formalização da entrada junto aos países membros, quanto para a ratificação legislativa do acordo. Ao todo são 44 estados-membros do Conselho da Europa e 20 estados não membros.

## 4. - O DIREITO AO ESQUECIMENTO

Desde o ano de 2012, quando se falava sobre a necessidade de reformulação do Regulamento Geral sobre Proteção de Dados da União Europeia (Diretiva 95/46/EC, outubro de 1995), o termo “esquecimento” alcançou níveis elevados de importância social. Começou a ser comentado e estudado nas mais diversas áreas das ciências sociais e humanas. Naquela época já havia um temor quanto à velocidade da informação e quem eram os reais detentores dos dados pessoais. Nasce então a corrida para regularizar tais questões. Os cidadãos europeus usariam mecanismos de retomada dos próprios dados, sob controle de entes públicos ou privados, que foram a estes disponibilizados. A RGPD, em seu artigo 17, garante o apagamento de dados ou como popularmente conhecido, direito ao esquecimento (*the right to be forgotten*), cabendo ao ente que está sob domínio de dados pessoais a efetiva retirada ou

cessão do seu tratamento quando for solicitado pelo proprietário, conforme condições estabelecidas no artigo, obrigando também a informação à terceiros.

Muitos criticam a terminologia “direito ao esquecimento”, ainda que se reconheça a importância de atos regulatórios promovidos pelo estado para garantir maior transparência no tratamento e garantir a real privacidade dos indivíduos, tal nomenclatura “pode provocar verdadeiras reações emocionais e instintivas, na maioria das vezes negativas, ao invés de uma resposta racional e responsável” (BERNAL, 2011).

A aplicabilidade do direito ao esquecimento pairou sobre os juristas à época, sendo recebido com críticas, elogios e até ceticismo. Isso foi confirmado após a positivação desse direito no RGPD, pois a nomenclatura não combinava com a sua intenção real, que caracterizou a impossibilidade prática e teórica de exercer um controle à terceiros de esquecer alguma coisa. Embora a União Europeia tenha sido pioneira no debate do direito ao esquecimento, a previsão legal deste direito no Regulamento obstou que a essência do seu significado fosse inserido em seu conceito.

O caso mais emblemático deste assunto, foi sem dúvidas, o julgamento do Tribunal de Justiça da União Europeia envolvendo a empresa Google Spain e o espanhol Mario Costeja González em 2014. A decisão baseou-se não apenas nos argumentos clássicos de ressocialização, mas de uma forma geral de esquecimento, ou seja, aquele que deve ser tutelado em todos os aspectos da vida civil e digital da sociedade de informação. Através desse julgado, também foi pautado outras formas de interpretação da diretiva n.º 95/46/CE em vigor à época, que era usada para fundamentar o direito ao esquecimento.

Por ter sido de grande relevância midiática no ano de 2010 e por ter sido julgado pelo Tribunal de Justiça Europeu, o caso Mario Costeja González rapidamente ganhou o mundo.

Em 2010 esse cidadão apresentou uma reclamação contra um jornal de grande circulação em desfavor da Google Spain e Google Inc., através das autoridades legitimadas para o controle de proteção de dados no território espanhol, alegando que estavam sendo vinculadas notícias referentes ao seu nome quando o mesmo era citado em sites de buscas na internet. Além das notícias que o vinculavam terem caráter negativo, estavam publicadas há 12 anos, visto que o fato ocorrera no primeiro semestre de 1998.

As notícias envolviam um edital de hasta pública referente a um imóvel em que o senhor Mario era o dono e o mesmo foi alienado no passado decorrente de uma execução fiscal. Ocorre que tal fato já havia sido resolvido há bastante tempo, portanto, não justificaria a permanência da matéria no banco de dados virtuais.

Assim o reclamante exigiu a retirada de todo o conteúdo relacionado ao assunto, bem

como o bloqueio dos *spiders*[26] contidos nos motores de buscas, alegando que a não mais havia interesse público na divulgação, o que não justificava a indexação pela Google Inc.

Pelo fato de que as publicações das notícias foram feitas com a autorização legal, além de terem sido determinadas por autoridades, houve indeferimento do pedido em se tratando do jornal, pois o mesmo apenas cumpriu o seu dever observado na lei. Em relação ao Google o pedido foi deferido, tendo que o mesmo retirar todo o conteúdo que tratava do assunto.

A partir daqui o caso ganhou ainda mais repercussão, pois a empresa inconformada entrou com recurso judicial sendo posteriormente o processo suspenso pelo tribunal espanhol (Audiência Nacional). Tal acontecimento trouxe a dependência do Tribunal de Justiça da União Europeia para resolução de diversos aspectos danosos quanto a interpretação das questões do direito da personalidade, contidas no RGPD, tendo em vista a evolução assustadora das tecnologias emergentes do século XXI.

As questões prejudiciais que exigiram um posição do Tribunal são: os motores de buscas e suas atividades fazem parte do tratamento pessoal de dados?; os motores de busca são responsáveis pelo que mostram nas páginas?; a obrigatoriedade de excluir conteúdo é legítima, mesmo que legalmente tratadas e contidas nos sites de origem?; é legítimo o indivíduo exigir aos motores de buscar a exclusão do conteúdo justificando a lesão da imagem ou a mera vontade de ser excluídos, ainda que publicados licitamente na página de origem?

O entendimento do Tribunal se configurou no sentido de a indexação de dados na internet, por si só, já é caracterizado o seu tratamento (caso lindvist[27]). De acordo com a interpretação já prevista na RGPD a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, já se considera tratamento de dados.

Portando, de acordo com decisão do Tribunal proferida no ano de 2014, nos casos em que houver o nome ou matéria vinculada à alguém pode-se pleitear diretamente ao administrador a retirada do conteúdo, reconhecendo o direito ao esquecimento. Assim, após dada a decisão, esse direito passa a ser exercido por todos os usuários da União Europeia através do formulário chamado "s*earch removal request under data protection law in*

[26] "Um *web crawler*, *spider* ou *bot* de mecanismo de busca, baixa e indexa conteúdo de todas as partes da internet. O objetivo de um *bot* desse tipo é detectar do que se tratam (quase) todas as páginas da internet para que as informações possam ser recuperadas quando necessário. São chamados de *"web crawlers"* porque *"crawling",* em inglês, é o termo técnico para o acesso automático a um site e a obtenção de dados por meio de um software." (O QUE é um web crawling?, 2020, s/p).

[27] TJUE, julgado em 06/11/2003, processo: C-101/01, parágrafo nº 25. (UNIÃO EUROPEIA, 2003).

*Europe*", que prevê a retirada do conteúdo devidamente justificado pelo titular, sendo então examinado por uma comissão na empresa.

### 4.1 - A origem do direito ao esquecimento

O caso mais antigo desse direito remete à legislação e jurisprudência francesa e italiana chamada *droit à lòubli* (*right to oblivion*), no final dos anos de 1970. Sua tutela é aplicada especialmente em casos criminais de condenados que não desejam mais que sua imagem vincule suas condutas passadas. Esse direito é exercido para visar a prevenção, impedindo que terceiros divulguem notícias pretéritas de um passado ilícito. Essa ideia tem como objetivo passar ao indivíduo a capacidade de mudança, mas não precisando ser "assombrado" pela divulgação de fatos passados tortuosos.

Entretanto, o *droit à lòubli* abrange outras searas do direito, não se limitando apenas à parte criminal, sendo, portanto, invocado nos casos em que envolve temas como direito à privacidade e direito a personalidade, por exemplo, pessoas que ganharam popularidade temporária e não conseguiram se desvencilhar da "fama" passageira após um período de tempo. Nesses casos, a fundamentação para a tutela desse direito está na proteção da dignidade, personalidade, vida privada e identidade e, portanto, é de fácil colisão com outros direitos como a liberdade de expressão e acesso a informação. O objetivo é atingido quando há a limitação de informações privadas, pois não sopesa o interesse público frente as divulgações desse tipo.

"Este conceito do direito ao esquecimento é fundado na necessidade essencial de um indivíduo determinar o desenvolvimento da sua vida de maneira autónoma, sem ser continuamente estigmatizado por uma ação específica ocorrida no passado, principalmente quando esses eventos ocorreram há muitos anos e não tem relação alguma com o contexto contemporâneo. O *droit à lòubli* satisfaz uma necessidade humana específica e assim facilita a sua propagação conceitual e a proteção do direito de ser esquecido em várias situações." (MATELERO, 2013, p.230.)[28]

A seguir, analisaremos os principais casos do direito ao esquecimento no Brasil.

[28] Tradução livre: "This concepto f the right to be forgotten os based on the fundamental need of na individual to determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past, especially when these events occured many years ago and do not have any relationship with the comtemporary contexto. The droit à l'oubli satisfies a specific need of human beings and this has facilitated the diffusion of the concept and the protection of the related right in diferente legal contexts".

## 4.2 - Direito ao esquecimento no Brasil

O Congresso Nacional iniciou articulações legislativas após a entrada em vigor do Regulamento e Diretiva Gerais sobre Proteção de Dados da União Europeia, vigendo em maio de 2018. Tal processo, culminou na aprovação da Lei Geral de Proteção de Dados Pessoais brasileira (Lei nº 13.709/2018). Entretanto, mesmo antes da lei ser aprovada, houve um clamor jurisdicional para que o vácuo legislativo fosse suprido, tendo em vista que tratava-se do tema do direito à privacidade e consequentemente do direito a dignidade da pessoa humana. (SARMENTO, 2014, p. 47)

É importante destacar que nessa época, já vigorava uma lei de proteção de dados em países da América Latina, por exemplo, Argentina e Colômbia. Entretanto, a execução e aplicação dessas leis no que diz respeito ao direito ao esquecimento não eram específicas ao tema, podendo ser usados outros dispositivos legais pelas respectivas Supremas Cortes para a resolução de casos que envolvam esse direito, indicando que os julgamentos dessa matéria podem ser debatidos de maneiras diferentes.

Os casos relacionados ao exercício do direito em diversos países, inclusive no Brasil, em grande maioria trata-se do pedido de supressão dos conteúdos em mídias, por exemplo, televisão, redes sociais e provedores de busca na internet (MONCAU, 2017). Algumas características peculiares ao exercício do direito ao esquecimento apresentam obstáculos que vão desde o ato da desindexação a delimitação e conceituação do tema, posto que qualquer pedido pode facilmente se enquadrar nessa tese. Ou seja, qualquer pessoa que não queira que seu passado seja vinculado à alguma página encontrada em sites de buscas, pode justificar seu pedido com base nesse direito. Como consequência desse fenômeno, o judiciário brasileiro acumula diversas demandas sobre o assunto.

Entretanto, os pedidos em questão não partilham das mesmas particularidades e é importante uma análise cuidadosa para que se faça a distinção correta de cada caso, conforme pensamento de Sérgio Branco: “Este é um dos grandes desafios da precisão da abrangência do direito ao esquecimento. Existe uma tendência à superinclusão de pleitos que podem ser perfeitamente enquadrados em outras categorias ou que, ainda pior, necessariamente precisam ser qualificados de modo diverso” (BRANCO, 2017, p.146).

Cabe destacar que o direito em análise é altamente variável, sendo possível abarcar diversos outros direitos positivados no ordenamento jurídico brasileiro. Na esfera cível, é relacionado com os tradicionais direitos fundamentais à imagem, à privacidade, à honra, à intimidade (art. 5º, inciso X, da CFRB e art. 11 e seguintes do Código Civil de 2002), além do

princípio basilar da dignidade da pessoa humana (art. 1º, inciso III, da CFRB). Também é possível observá-lo no na Lei do Cadastro Positivo (Lei nº 12.414/2011), bem como no Código de Defesa do Consumidor (Lei nº 8.078), nos artigos 7º, inciso X e 19, do Marco Civil da Internet (Lei nº12.965/2014). Na esfera criminal, têm-se os artigos 63 e 64, inciso I, do Código Penal e o artigo 748 do Código de Processo Penal, pois trata-se do instituto da reincidência que tem como objetivo minimizar os efeitos da pena.

A doutrina majoritária entre os civilistas brasileiros, afirma que o direito ao esquecimento é tratado como um ramo do direito à privacidade, presente no art. 5º, inciso X, XI e XII da CFRF e art. 21 do Código Civil de 2002, pois aquele direito pretende evitar que fatos passados ao individuo, relacionados à sua imagem, venham a causar constrangimento atual em virtude da descontextualização.

O Enunciado 531[29]que foi aprovado na VI Jornada de Direito Civil, evento promovido pelo Conselho da Justiça Federal, não raro é citado em jurisprudências, sendo considerado um manual ao direito ao esquecimento, informando que o mesmo deveria ser interpretado a luz do artigo 11 do Código Civil de 2002. Por haver a ausência da previsão legal, tal direito não deverá ser suprimido, tendo em vista que o princípio da dignidade da pessoa humana é norteador de vários outros direitos relativos ao direito ao esquecimento.

A coleta de informações pessoas na internet a cada dia tem se acumulado de tal forma que é normal surgirem questionamentos sobre quem são responsáveis pelos tratamentos de dados e para que são usados. Portanto, é de suma importância a construção legislativa e jurisdicional para a transparência sobre o tratamento e o controle pessoal, caso a não seja de matéria de interesse público.

Observa-se no Brasil que está caminhando para uma convergência da definição do direito ao esquecimento como sendo um ramo do direito à privacidade, relacionado ao controle sobre dados pessoais, tendo em vista o caso Aída Curi discutido em audiência pública no Supremo Tribunal Federal. Decorrido o chamado *amici curiae*, foi atestado a existência de 3 correntes relacionadas ao direito ao esquecimento por Anderson Schreiber: (i) pensamento pró-informação, onde não se reconhece a veridicidade desse direito, nem mesmo

[29] ENUNCIADO 531 – A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Artigo: 11 do Código Civil Justificativa: 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-detento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados. (BRASIL, 2013, p. 1).

a sua ligação com os direitos à privacidade e à intimidade; (ii) pensamento pró-esquecimento, onde coloca-se na balança o direito a informação e o direito à reserva, à intimidade e à privacidade. Aqui o esquecimento pesa no conflito e legitima a retirada de fatos considerados prejudiciais e defasados ao indivíduo; (iii) pensamento intermediário, onde não há hierarquia entre o direito à privacidade e seus ramos e o direito à informação, devendo cada caso ser ponderado. (SCHREIBER, 2017).

Conforme explanado, existe uma dificuldade quando se fala do direito ao esquecimento, pois há várias posições doutrinárias sobre o tema, além do real significado desse direito aplicado ao caso concreto, bem como as obrigações que dele emanam. A reflexão sobre o assunto é devido as demandas que chegam nos tribunais, que será comentado mais adiante. Embora haja jurisprudências consolidadas sobre tema no Superior Tribunal de Justiça, deve-se ter uma noção para onde estamos indo e para onde vamos, pois muitas são as controvérsias que existentes.

### 4.2.1 - O caso da Chacina da Candelária

A expressão "direito ao esquecimento" foi utilizada pela primeira vez no Superior Tribunal de Justiça, julgando os recursos especiais dos casos Chacina da Candelária (1.334.097/RJ) e Aída Curi (1335.153/RJ), em 2013, ano anterior ao famoso caso González. Ambos foram amplamente divulgados pela mídia televisiva à época e o Ministro Relator dos recursos, Luís Felipe Salomão, julgou-os com critérios diferentes. Atualmente, ambos estão esperando apreciação do Supremo Tribunal Federal, sendo a repercussão geral reconhecida no caso Aída Curi.[30]

O caso da Chacina da Candelária versou sobre uma ação ajuizada por Jurandir Gomes de França, contra a TV Globo, que o convidou para uma entrevista no programa "Linha Direta-Justiça" em 2006, para a reconstrução do crime bárbaro que aconteceu em frente a Igreja da Candelária na cidade do Rio de Janeiro, em 1993. O autor da ação participaria como coautor/partícipe do episódio, embora ele tenha recusado o convide da emissora. Após julgamento em Júri Popular, foi absorvido pelo Conselho de Segurança, afirmando que Jurandir não fora autor do crime. Sem sua autorização o programa foi transmitido, citando seu nome e indicando sua absolvição.

Embora essa sentença fosse benéfica a Jurandir, a sua imagem foi exposta e o seu

[30] STF, Recurso Extraordinário, nº 1.010.606, sob diretoria do Min. Dias Toffoli.

nome citado sem o seu consentimento, ocasionando transtorno na sua vida social, tendo em vista diversas ameaças sofridas por traficantes e dificuldades em conseguir emprego ou fixar em um. Tais transtornos mudaram o estilo de vida de Jurandir, fato que o fez recorrer a justiça contra a rede de televisão, pleiteando danos morais.

O magistrado do caso na primeira instância indicou duas controvérsias na ação: (i) por ter sido tal crime bárbaro e de grande comoção social, questionou-se se a mídia requer o consentimento dos envolvidos para exibição de imagens e afins; (ii) puxar da peculiaridade da proteção à privacidade o direito ao anonimato.

Com o andamento da ação, provou-se que a TV Globo não agiu de má-fé e não houve ilicitude em transmitir as imagens, pois, além de comunicar previamente o ocorrido, o programa tratava-se de reconhecido interesse social, bem como mostrar a desastrosa investigação que envolveu todo o caso. Por fim, foi reconhecido o direito ao anonimato como um dos ramos do direito à privacidade e intimidade e que o direito ao esquecimento e ao anonimato podem ser mitigados quando contextualizados com questões de grande comoção social, tendo em vista ser inviável narrar os fatos sem os dados elementares. Portanto, a sentença foi proferida no sentido de que o direito de informar foi lícito, eivado de regularidade, sendo a demanda de Jurandir julgada improcedente.

Inconformado, os advogados interpuseram recurso de apelação, reformando a sentença. Pela primeira vez o termo “direito ao esquecimento” foi usado pelo relator, quando o mesmo citou o caso da ex-prostituta americana Melvin e do caso alemão Lebach I, para fundamentar a tese de algumas histórias podem ser reproduzidas ou narradas sem necessariamente mencionar todos os integrantes daquele contexto. Assim, a sentença foi revertida ao pagamento de R$ 50.000 (cinquenta mil reais) contra a TV Globo, fundamentada na tese de que a emissora poderia ter se utilizado de um pseudônimo qualquer para preservar a dignidade do autor, tendo em vista que fora absorvido de um crime bárbaro e tem o direito de ser esquecido.

Ainda, foram interpostos mais recursos, um especial e um extraordinário. Ambos foram negados. Chegaram, portanto, à apreciação do Superior Tribunal de Justiça e Supremo Tribunal Federal devido à apresentação de um agravo. O STJ registou que a questão da “ausência de contemporaneidade da notícia de fatos passados, a qual, segundo o entendimento do autor, reabriu antigas feridas, já superadas, e reascendeu a desconfiança da sociedade quanto a sua índole (..)” (STJ, 2013a, p. 22). Ficou evidente que o assunto deveria ser utilizada a ponderação dos direitos da personalidade e os direitos à liberdade de expressão e os direitos à informação, tendo como base a conjuntura social, cultural e tecnológica atuais.

Ao final do voto, foi questionado se o direito ao esquecimento deveria fazer parte do ordenamento jurídico brasileiro, fato que foi unanimemente concordado entre os relatores baseando esse posicionamento no âmbito cível e penal (STJ, 2013a, p.34). Portanto, estabeleceu-se o conceito de "um direito de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores, de natureza criminal, nos quais se envolveu, mas que, posteriormente, fora inocentado" (STJ,2013a, p. 23). Estabeleceu-se também que referências ou investigações criminais não poderiam ser perpetuadas no tempo, possuindo "prazo de validade", ou seja, caso fosse "ressuscitada" informações criminais pretéritas, ensejaria fato ilícito. Portanto, mesmo que a notícia eivada de vícios seja um empecilho à liberdade de expressão, a notícia honesta e verdadeira não poderá ser inquestionável e nem blindada pela liberdade de informação e liberdade de imprensa. O chamado "direito à esperança" e "direito da regenerabilidade humana" (STJ, 2013a, p.45), seria fundamentado no ordenamento jurídico brasileiro, baseado nos direitos fundamentais e princípio da dignidade da pessoa humana, assim como no ordenamento infraconstitucional. Portanto:

A assertiva de que uma notícia lícita não se transforma em ilícita com o simples passar do tempo não tem nenhuma base jurídica. O ordenamento é repleto de previsões em que a significação conferida pelo Direito à passagem do tempo é exatamente o esquecimento e a estabilização do passado, mostrando-se ilícito sim reagitar o que a lei pretende sepultar (STJ,2013a, p.40)

Terminada essa análise, percebe-se que mesmo que o crime da Chacina da Candelária fosse de grande relevância e trauma social, tais acontecimentos poderiam ser narrados de forma a proteger a imagem de Jurandir, sem que os fatos prejudicassem a razoabilidade da história. Ainda, como fora dito, houve uma segunda exposição dos acontecimentos pela emissora, mais uma vez um ato ofensivo à dignidade humana, justificado no acórdão como uma preferência constitucional na defesa de Jurandir, aos temas relacionados à vida privada, honra, intimidade, imagem, família, previstos no art. 220, parágrafo 1º e no parágrafo 3º do art. 222 da CFRB. Isso resultou na rejeição do recurso da emissora de televisão Globo e manteve-se a decisão condenatória pelo tribunal.

Por fim, observa-se que esse caso em si, não notou de imediato o direito ao esquecimento, sendo este se desenvolvendo ao longo do processo. Os temas centrais do pleito eram fundamentados no direito à imagem e à privacidade do autor e o direito ao esquecimento só ganhou notoriedade quando o relator do recurso de apelação, no Tribunal de Justiça do Rio de Janeiro, o mencionou.

Adiante, no STJ, o julgamento desse caso se assemelha bastante com o caso *droit à l'oubli,* conforme já mencionado nos capítulos anteriores. Destaca-se a importância de sopesar os direitos fundamentais da liberdade de expressão e o direito ao acesso à informação e os direitos relativos à personalidade. Com a necessidade de proteção da vida privada, o relator também cita os casos de Lebach I e da ex-prostituta de Melvin como fundamento de sua tese relativa ao direito ao esquecimento.

Desta forma, este direito foi aplicado e reconhecido pelo STJ no caso concreto, expondo que fatos criminais desabonadores não poderão ser lembrados contra a vontade do indivíduo, tendo em vista a "data de validade" do fato ou da notícia, tornando-o ilícito conforme o passar do tempo. Semelhante ao caso alemão, a referência do nome de Jurandir foi crucial para o conteúdo decisório da condenação contra a emissora.

### 4.2.2 - O caso Aída Curi

Semelhante ao caso descrito acima, o motivo que fizeram os irmãos Nelson Curi, Waldir Curi e Maurício Curi ajuizarem a ação de danos morais e materiais contra a TV Globo, foi que a notificação contra a exibição do caso no programa da emissora foi ignorada, ocasionando a reabertura dos traumas sofridos com a morte da irmã, Aída Curi. No pedido, estava a indenização sobre justificativa de que a emissora teria se beneficiado economicamente por ter utilizado do nome, histórias pessoais e imagem da família Curi, angariando grande audiência e monetização publicitária, configurando-se enriquecimento ilícito.

O juiz de primeiro grau pontuou controvérsias na verificação ou não da inobservância do direito à personalidade dos autores da demanda, justificando assim o deferimento do pedido. Entretanto, ao analisar o caso, afirmou que não ficou comprovado que a Globo havia se beneficiado monetariamente ao reproduzir os fatos do assassinato de Aída. Utilizou-se também da ponderação entre os direitos à liberdade de expressão e de imprensa e os direitos à personalidade, concluindo que não houve qualquer ilicitude por parte da emissora, assim julgando pleito improcedente.

Aos autores recorreram da decisão, e ela foi mantida com base no fundamento de que os acontecimentos narrados já tinham sido amplamente divulgados e já eram de conhecimento público à época do crime. Nesse caso, o direito a comunicação e informação deveria prevalecer em relação ao direito de ser esquecido por fatos nascidos no passado. Destaca-se que o termo "esquecimento" foi usado no acórdão com o argumento de que não basta apenas

“esquecer” para se configurar a redenção, pois muitas vezes é indispensável que acontecimentos pretéritos venham à tona para que sirva de lição moral para as futuras gerações. Forma interpostos recursos especial e extraordinário (STF, RExt nº 1.010.606), ambos não foram admitidos. Mesmo que não admitidos, os recursos subiram ao STJ e STF por meio da interposição de agravo.

O episódio Aída finalmente se tornou um caso de direito ao esquecimento, com a justificativa que o programa “Linha Direta” violou tal direito ao reconstruir e transmitir o crime em rede nacional. Ainda que o caso em análise seja eivado de semelhanças com o caso da Chacina da Candelária, pois ambos narram crimes cometidos no passado, as decisões dos juízes foram diferentes. O desfecho de Aída não foi o mesmo, não sendo reconhecido do direito ao esquecimento pelos motivos de: (i) o crime foi de grande importância para a história brasileira, pois serviu de estudo acadêmico em várias áreas de conhecimento; (ii) a impossibilidade de narrar os fatos sem o nome e personalidade real da Aída Curi; (iii) não ficou comprovado, na cobertura do crime no passado, o excesso na narração dos fatos; (iv) o intervalo de tempo entre o fato criminoso e a transmissão pela emissora Globo. Por essa causa, o STJ concluiu que o caso configurou uma das “exceções decorrentes a ampla publicidade a que podem se sujeitar alguns delitos” (STJ, 2013a, p. 38).

No recuso extraordinário, que subiu posteriormente ao STF por meio de agravo, teve como seu relator o Ministro Dias Toffoli (RExt nº 1.010.606). Foram feitas considerações relevantes quanto em tema do direito ao esquecimento em audiência pública ocorrida para junho de 2017. O Procurador Geral da República, Rodrigo Janot, posicionou-se por não validar o direito ao esquecimento frente ao direito à liberdade de expressão e de informação, ao se exigir pela parte autorização prévia para informar, transmitir e comunicar fatos passados, tampouco legitimar a existência de dano de caráter indenizatório. Semelhante ao caso da Chacina, percebe-se que a tutela do direito ao esquecimento não foi pleiteada no início da petição em primeira instância. O tema foi evoluindo conforme o direito à personalidade fosse discutido, embora mais tardio, pois nem nos acórdãos em segunda instância foi suscitado. O caso dos julgamentos do *droit à l’oubli* também se assemelha à Aída, fato é que o Ministro Relator destacou que a garantia do direito ao esquecimento nem sempre garantia o direito de indenizar (STJ, 2013b, p.41).

Como foi dito, as decisões tomaram resultados distintos. Observa-se que a liberdade de expressão foi assegurada em ambos os casos, mesmo que em níveis variados. Assim, o STJ solidificou entendimento que o direito ao esquecimento pode “conviver” com a liberdade de expressão sem que esta seja menosprezada. Isso se dá devido à decisão do STJ no caso da

Chacina, onde decidiu que os fatos pretéritos podem ser transmitidos ou divulgados sem que haja necessidade da menção dos nomes dos autores do pleito, somente tendo relevância a menção dos nomes aos fatos contemporâneos. Portanto, segundo o Tribunal, o caso Aída Curi tornou-se dificultoso ou mesmo impossível proteger a liberdade de expressão sem citar o nome da vítima.

Daniel Sarmento criticou essa perspectiva da 4ª Turma, afirmando que não houve observância da Constituição Federal, pois as liberdades à informação e transmissão seguraram a emissora Globo:"não só o direito à escolha dos fatos a serem narrados em sua programação, mas também do ângulo de análise destes fatos, bem como do conteúdo da sua narrativa, o que, naturalmente, envolve a eleição dos personagens cujas participações são retratadas." (SARMENTO, 2015, p.50)

É defendido por este professor que em ambos os casos não é aplicado o direito ao esquecimento, pois não haveria base constitucional ou legal para a sua tutela, tendo em vista o caráter genérico e inconsistente em que se constrói esse direito, causando prejuízo à garantia da liberdade de expressão, notadamente nos casos em que há relevante interesse público. Diante das controvérsias, o direito ao esquecimento é questionado quanto a sua demanda social e seus efeitos na vida dos indivíduos, visto que os primeiros casos que os tribunais superiores tiveram acesso não se tratava desse direito propriamente dito, e sim de outros direitos relativos ao tema, como direito à personalidade, à imagem, à privacidade, ao nome e a imagem. Ainda, o tribunal se utilizou da ponderação desses direitos com os direitos relacionados à liberdade de expressão e imprensa para melhor dirimir a controvérsia jurídica. Análogo ao caso *droit à l'oubli,* o direito ao esquecimento nasce mais como uma narrativa para que o nome de alguém seja desvinculado de alguma notícia ou fato pretérito, ou destas não ser mais associado, do que um direito propriamente autônomo. Segundo o professor Sarmento, "nem todo desejo configura direito fundamental" (SARMENTO, 2015, p.49)

Tendo em vista que os autores do processo pleitearam indenização, poderiam fundamentar a tese nos direitos clássicos que giram em torno da personalidade, ou propriamente no direito ao esquecimento, pois constituem os mesmos objetivos da demanda, ou seja, punir os responsáveis pelo abalo moral e psicológico em razão da matéria jornalística, sofrido pelos autores.

É importante observar, que no caso do *affaire* Landru, o professor Gérard Lyon-Caen expôs o direito ao esquecimento através da interpretação do pedido do pleito pela *prescription du silence* (prescrição do silêncio), devido a expressão em si ser obscura, dificultando um conceito mais objetivo do esquecimento e impedindo a sua invocação própria.

O conflito nos casos que envolvem o tema do direito ao esquecimento, sem dúvidas devem ser solucionados pela ponderação de direitos fundamentais que já estão no ordenamento jurídico. Portanto, uma demanda em relação ao tema, pode ser fundamentada tanto nos moldes do direito ao esquecimento, quanto nos direitos clássicos da personalidade e o pedido de indenização pode ser deferido normalmente em ambos os casos.

Questiona-se se o direito ao esquecimento poderia ser invocado nesses casos como um direito autônomo, tendo em vista que qualquer outro direito clássico equiparado fundamentaria as demandas de *droit à l'oubli*. Entretanto, a partir deste momento, será analisado julgamentos que foram pedidos o direito ao esquecimento, centralizado ao provedor de buscas da internet, e outros casos de apreciação do STJ sobre o tema, no cenário do *droit à l'oubli,* entre outras demandas no contexto virtual.

### 4.2.3 - Xuxa vs. Google Brasil Ltda.

Em terras brasileiras, a apresentadora Xuxa Meneguel, denominada "Rainha dos Baixinhos", participou de um filme contendo cenas de sexo no ano de 1982. Passados os anos, tornou-se apresentadora de um conhecido programa infantil na televisão, no qual lhe rendeu seu apelido e prestígio entre as crianças. A tecnologia foi então avançando e com o surgimento da *internet,* ficava fácil acessar o filme pornográfico em plataformas de buscas, o que em certo grau, provocaram críticas e assassinato à reputação da apresentadora. Xuxa então ajuizou ação para a retirada de qualquer vínculo a sua imagem relacionada ao termo "Xuxa pedófila" ou ao filme em si.

O Superior Tribunal de Justiça analisou a responsabilidade dos provedores de busca no caso da apresentadora ea empresa Google. O REsp 1316.921/RJ, logo ganhou notoriedade tendo em vista a ausência de regulação sobre a responsabilidade civil dos provedores de buscas. O termo "direito ao esquecimento" em nenhum momento foi utilizado pelas partes ou pelo Tribunal, e o caso foi inspirado nos julgamentos do TJUE.

Na primeira instância, o pedido foi deferido, ordenando apenas a retiradas dos conteúdos indicados pela autora, sem que houvesse a retirada dos links apresentados pelos sites de buscas que eventualmente viessem a aparecer. Houve contestação da decisão pela empresa Google, exigindo que o Superior Tribunal de Justiça, explicasse qual seria o limite da responsabilidade dos provedores de buscas, frente aos usuários da internet. A relatora a ministra Fátima Nancy Andrighi, entendeu que os provedores de busca não têm responsabilidade sobre os conteúdos ali exibidos, logo não controlam os resultados das

informações (BRASIL, 2012). Eles, os provedores de pesquisas, foram conceituados como um tipo de provedor de conteúdo, pois "não incluem, hospedam, organizam ou de qualquer forma gerenciam as páginas virtuais indicadas nos resultados disponibilizados" (STJ, 2012, p. 10). Portanto, a responsabilização dos provedores de buscas foi considerada ilegítima quando oferecesse resultados de outras páginas de conteúdo vigente na internet, tendo em vista a descaracterização da teoria da responsabilidade objetiva e a teoria do risco da atividade, contidas no art. 927, parágrafo único, do Código Civil.

Ainda, entendeu-se que o controle prévio na identificação de conteúdos ofensivos ou ilícitos ao indivíduo, não seria de responsabilidade do provedor, pois tal tipo de análise é de cunho subjetivo o que impossibilitaria o seu crivo automático. A opção resultante para essa problemática seria o usuário que se sentiu lesado contatar a página responsável pela sua reprodução e solicitar a retirada, para que o conteúdo não vincule novamente à algum provedor de busca. Constatou a possibilidade de cumprir comandos objetivos como retirada de conteúdo, impedindo que buscadores encontrem termos como "xuxa pedófila".

Entretanto, tal medida carece de eficácia, pois qualquer conteúdo poderia ser acessado caso haja modificação dos critérios de pesquisas, por exemplo, caso a pesquisa fosse feita em um provedor localizado em outro país. A Ministra Relatora fundamentou a tese de que tal atitude configuraria uma forma de censura. A supressão a qualquer tipo de *link* ou imagem encontrada em uma pesquisa por motores de buscas, viola o direito ao acesso à informação previsto no artigo 220, da CFRB. Assim, os provedores não são obrigados a exclusão do conteúdo pesquisado quando for usado termo ou expressão.

Em segunda instância, a decisão relacionada a supressão de conteúdo apontado pelo autor, o STJ entendeu que: (i) somente se houver ordem judicial mandando restringir; (ii) o requerente deverá indicar o endereço (URL) das páginas consideradas ilícitas ou mesmo o IP (i*nternet protocol*) dos servidores. O STJ, portanto, arguiu em favor dos provedores de buscas, afirmando que caso a vítima identificasse essas informações, haveria carência no interesse de agir da demanda contra os provedores, tendo em vista ser mais lógico e eficiente direcionar a reclamação aos sites ofensivos para que o desejo de retirada do conteúdo fosse realizado.

Conclui-se através desse julgamento que os provedores de pesquisas não são responsáveis por revelar os *links* de matérias consideradas ilícitas feitas por terceiros. Também não serão coagidos para estabelecer métodos de filtragem nas buscas, ou seja, um controle prévio do conteúdo, quando buscado por um usuário qualquer na *internet*. E por último, os provedores não serão obrigados a suprimir qualquer resultado de pesquisas feitos

especificamente através de expressões ou textos, ainda quando apontado o endereço onde o conteúdo está localizado.

A apresentadora, não satisfeita, ingressou com uma reclamação perante o Supremo Tribunal Federal, que levou em plenário da 2ª Turma por consequência de um agravo regimental, justificando a violação da súmula vinculante nº 10, sendo posteriormente desprovido. O entendimento que prevalece na maioria das vezes pelo STJ segue nesse sentido de não responsabilização dos provedores de pesquisas, sendo recorrentemente observado pela Corte

Afere-se que com a decisão, os tribunais brasileiros possuem entendimento contrário aos tribunais europeus, que afirmam ser de responsabilidade dos provedores os resultados obtidos nas pesquisas.

Existem outros casos em que decisões[31] do Superior Tribunal de Justiça seguiram a mesma linha de raciocínio, ou seja, a de não responsabilizar os provedores pelas informações indexadas, devendo o titular processar o responsável que elaborou a matéria, notícia ou conteúdo e não o provedor de buscas.

Porém, no ano 2009, o STJ proferiu um acórdão em um Recurso Especial nº 1.660.168/RJ[32] em que ganhou o voto do ministro Marco Aurélio Bellize, contrário ao entendimento que vinha sido aplicado em decisões anteriores relativa ao direito de ser esquecido na *internet.*

O caso era de uma promotora que foi vinculado seu nome à notícias de envolvimento em fraude de concurso público para ocupação do cargo de juiz na cidade do Rio de Janeiro. Dessa maneira, ajuizou ação contra o Google, Microsoft e Yahoo, exigindo a desvinculação do seu nome às reportagens. O Conselho Nacional de Justiça emitiu parecer alegando que não houve indícios suficientes para concretizar a fraude.

Em primeira instancia o pedido foi considerado improcedente, entretanto, após recurso, o Tribunal de Justiça do Rio de Janeiro condenou as empresas e exigiu a instauração de filtros de pesquisa para que o nome da promotora não seja vinculado aquelas notícias,

[31] STJ, REsp 1.407.271/SP, 3ª T., Relª Min. Nancy Andrighi, J. 21.11.2013, DJe 29.11.2013; STJ, Reclamação nº 5.072/AC, Relª p/o Ac. Min. Nancy Andrighi, J. 11.12.2013, DJe 04.06.2014; STJ, REsp 1.316.921/RJ, 3ª T., Relª Min. Nancy Andrighi, J. 26.06.2012, DJe 29.06.2012; STJ, AI-REsp 1.593.873/SP, 3ª T., Relª Min. Nancy Andrighi, J. 10.11.2016, DJe 17.11.2016.

[32] No acordão, a referida decisão continua esclarecida o seguinte texto: "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 fato noticiado, mas não àqueles que buscam exclusivamente pelos dados pessoais do indivíduo protegido." (REsp 1660168/RJ, Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018) (BRASIL, 2018[b], p. 2).

conforme o voto prevalecido do ministro Marco Aurélio Bellize.[33]

O acórdão também presumia que o acionamento do Poder Judiciário para que o direito de ser esquecido na *internet* seja exercido, se faz de fundamental importância, sendo utilizado a ponderação em cada caso concreto. Percebe-se que são inúmeras controvérsias que envolvem essa questão e a tendência é de que os tribunais sejam ainda mais acionados com a ascensão tecnológica.

### 4.2.4 - Ricardo Zarattini Filho vs. Diário de Pernambuco S.A

No mês de outubro do ano de 2016, mais um caso em terras brasileiras mereceu destaque quanto a tema direito ao esquecimento. O STJ julgou o caso de um pedido de indenização contra o jornal Diário de Pernambuco, alegando Zarattini, de que ele tinha sido acusado como autor do atentado ao Aeroporto dos Guararapes em 1966 pelo advogado Wandekolk Warderley em uma entrevista em concedida ao jornal em 1995. Ainda, sustentou que todas as investigações e ação penal promovidas contra ele, o absorveram. O juiz de primeira instância, ao analisar a controvérsia, condenou o jornal à indenização por danos morais. Porém, após recurso, a sentença foi modificada em segunda instância, protocolando então a parte autora recurso especial perante o STJ.

Semelhante nos casos anteriormente comentados, Aída e Chacina, o direito que fora pleiteado inicialmente foi o direito à imagem e à honra. No primeiro momento, não se falou em direito ao esquecimento, sendo este invocado apenas no STJ, graças ao voto contrário do Ministro Ricardo Villas Bôas Cueva, entendendo ser matéria de responsabilidade civil. À princípio o relator do recurso, Ministro Paulo de Tarso Sanseverino, negou o apelo de Zarattini, sendo posteriormente derrubado e revertido graças ao voto do Ministro Cueva que foi acompanhado pelos outros colegas ministros. Com o recurso provido, o então Ministro defendeu que deveria ser garantido à Zarattini o direito ao esquecimento, visto que a ele fora concedido anistia.

Nesse julgamento, houve a tese de afastamento do direito ao esquecimento pelo Ministro João Otávio de Noronha, que sustentou que o caso se trata de "episódio de inegável relevância e compreensão do momento histórico que se passava o país, constituindo-se, portanto, matéria de inequívoco interesse público" (STJ,2016, p.48).

[33] Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018) (BRASIL, 2018[b], p. 2).

Percebe-se que o critério produzido por esse caso, é que todos aqueles que tiverem se beneficiados com a anistia, são lhe concedidos o direito ao esquecimento. Ainda, o interesse público é fator de ponderação para o acolhimento ou não de pleitos fundamentados no esquecimento. Nota-se que esse julgamento gera desconforto e amedrontamento para casos semelhantes no futuro. Também, a evocação do esquecimento nesse caso, mostra-se completamente diferente dos demais já descritos, tendo em vista que o autor buscou indenização pela inverdade contada pelo advogado, pedido que já tinha sido deferido em primeira e segunda instância, através do próprio voto do Ministro Ricardo Villas Bôas. Portanto, não há base jurídica para a aplicação desse direito, caracterizando assim como um equívoco do STJ em utilizar a tese do esquecimento.

## 5. - ASPECTOS GERAIS AO ESQUECIMENTO

É de fundamental importância a proteção da imagem, privacidade, intimidade e a honra dos indivíduos, tendo em vista que são direitos relativos à personalidade e princípio da dignidade da pessoa humana, todos eles assegurados pela Constituição Brasileira e por normas Europeias. Tais direitos, constituem a base de qualquer relação humana e social, de natureza personalíssima.

> Concluindo, a personalidade é composta de atributos, tais como a vida, a honra, o nome, a capacidade, o estado, o corpo físico, a psique, a dignidade, etc. Atributos são elementos componentes, em outras palavras, o material de que é composto um objeto. A pessoa humana é composta de todo esse material, ou seja, de todos esses atributos. O que se chama de direitos da personalidade são, na verdade, direitos decorrentes desses atributos, visando à proteção e à promoção da pessoa humana e de sua dignidade. Essa visão moderna de que a honra, o nome, a vida etc. integram a pessoa é fundamental para a positivação da proteção e da promoção do ser humano e para a compreensão e a garantia da igualdade, pelo menos em termos formais. (FIUZA, 2009, p. 172).

No ordenamento jurídico brasileiro, o Código Civil de 2002 e a Constituição Federal Brasileira de 1988, andam juntas sobre o viés de garantir a integridade e a dignidade da pessoa humana. O Código Civil, em específico, traz um capítulo totalmente dedicado aos direitos da personalidade, visando sua proteção em inúmeros aspectos. Os direitos da personalidade estão disciplinados no capítulo II, nos artigos 11 a 21: “o Art. 11 do referido código, dita que com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária” (BRASIL, 2002, p. 214).

Seguindo a mesma linha de raciocínio a Constituição Federal brasileira, no artigo 5º, X, estabelece que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988, p. 35).

É inegável que a sociedade vivencia uma explosão tecnológica, capaz de que sem se perceber, permite o acesso a vida privada dos usuários, principalmente aqueles mais dependentes da internet, seja por fatores ligados ao trabalho, lazer etc. Em um único dispositivo celular, tem-se uma infinidade de funções ligadas à internet, bem como algoritmos que armazenam as informações pessoais mais importantes para direcionar o usuário à compra de um produto ou tendências de seu interesse.

A questão crucial é como ser esquecido na sociedade de informação e como ter o direito do anonimato, visto que são inúmeros os recursos tecnológicos disponíveis que alimentam nichos e desejos pessoais em cada dispositivo com acesso à internet. Ainda que haja dúvidas sobre o esquecimento ser possível, a Lei Geral de Proteção de Dados (lei n.º 13.709/2018) abarcou todas essas evoluções tecnológicas, trazendo mecanismos mais rápidos e eficazes de busca em provedores, facilitando a apreciação de documentos e fatos que eventualmente possam trazer ofensas à imagem alheia.

Segundo os Tribunais, é correto afirmar que esses provedores não são responsabilizados a priori por disponibilizar, após buscas na internet, conteúdo dos links fixados nos sites. Caso suceda uma decisão judicial onde exista ilegalidade, ofensa, material impróprio etc. em algum site de busca, pode-se então exigir a retirada do material do provedor. É o que diz o art. 19 da Lei 12.945/2014: "Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário" (BRASIL, 2014, s/p).

A forma mais eficaz de concretizar o direito ao esquecimento é o direito a desindexação que é a retirada das informações denominadas "lista de resultados" contida em sites de buscas quando se pesquisa uma palavra-chave. Porém, a informação continua a existir na rede, mas não estará disponível de forma mais fácil a quem utilizar da pesquisa, ou seja, para encontrá-la deve-se utilizar filtros específicos.

O entendimento do Superior Tribunal de Justiça frente à lei do Marco Civil, era de

que: houvesse a necessária retirada dos materiais solicitados pela pessoa que desejasse ser "esquecida", ela deveria listar todos os links e fontes para que fossem retirados[34]. O direito era garantido à quem o pleiteasse, porém a tarefa era árdua em listá-los caso houvessem centenas de links espalhadas na rede.

Atualmente, o entendimento da Corte foi modificado no sentido de que o próprio provedor tem a obrigação de retirar as informações que fazem referência ao autor. Dessa forma, caso decorra esta imposição, qualquer pesquisa que for feita da mais simples a mais complexa, não deverá apresentar resultados que refiram às lesões à personalidade de quem pleiteou a ação.

Pode-se ver que a lei garante o direito ao titular dos dados de obter do controlador, em qualquer tempo, mediante requisição, a retirada das informações que julgar lesivas à sua personalidade, ou que contenham excessos em desacordo com a lei. Por ordem judicial, é completamente plausível que os sites de buscas disponibilizem os links lesivos ao requerente.

Portanto, o passo mais adequado ao exercício do direito ao anonimato se traduz na responsabilidade do provedor em fornecer, bloquear, retirar ou excluir todos os links relacionados à pessoa lesada, caso seja comprovada a lesão e imposto por ordem judicial.

O Marco Civil da Internet, lei que foi aprovada em 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da *internet* no país que aborda diversas referências a proteção de dados pessoais, sendo regulamentado posteriormente pelo Decreto n.º 8.771 de 11 de maio de 2016. A promulgação da Lei Geral de Proteção de Dados foi posterior ao Marco Civil, fato é que esta é tratada como lei geral frente a especificidade da LGPD.

E por falar em lei geral, a Constituição Federal de 1988 traz apenas algumas referências à proteção de dados, quando fala sobre *habeas data* em seu artigo 5º, inciso LXXII: "LXXII - conceder-se-á *"habeas-data":* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;" (BRASIL, 1988, p. 22).

Além desse remédio constitucional garantido pela Carta Maior, tem-se também referência à proteção da vida privada no artigo 5º, inciso X: "são invioláveis a intimidade, a

[34] "Nesse contexto, a desindexação de links na rede foi a principal forma escolhida pela Comunidade Europeia para possibilitar aos indivíduos o exercício de seu direito à autodeterminação informativa sobre matérias, textos ou notícias publicadas sobre si na rede: ela age sobre os resultados de pesquisa apresentados pelos provedores de busca como o Google Search. Desse modo, "apaga-se" o elo entre informação e o terceiro que faz a pesquisa, mas mantém-se intacta na internet a matéria jornalística que publicou o fato. É uma forma de conciliar as liberdades comunicativas com o direito ao esquecimento [...]." (ACIOLI; EHRHARDT JÚNIOR, p. 406).

vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;" (BRASIL, 1988, p. 18).

Destaca-se que a Lei do Marco Civil desvincula a responsabilidade dos provedores no caso em que forem utilizados de maneira ilícitas por terceiros na rede, salvo quando for notificado por ordem judicial o caráter ilícito da informação e o provedor não retirar ou indisponibilizar o conteúdo. Nos casos em que os haja nudez, cenas de sexo de caráter privado, é legítimo o próprio titular ou representante legal a notificação ao provedor exigindo a retirada do material impróprio, seja em redes sociais ou *sites* de buscas. Também será responsabilizado caso o provedor não tome providências.

Em Portugal, as principais leis que cercam o assunto relacionados à proteção de dados pessoais, são a lei n.º 67/98, que alterou para o ordenamento jurídico português a diretiva n.º 95/46/CE, e posteriormente, a nova RGPD e o decreto-lei nº 7/2004, que alterou para o ordenamento português a diretiva n.º 2000/31/CE, bem como a Constituição Portuguesa nos artigos 26º, nº 1, 2 e 3, 35º, 37º e 38º.

Há tempo, questões jurídicas conflituosas entre a liberdade de expressão e os direitos de personalidade tornaram-se cada vez mais frequentes com o advento da sociedade da informação. Desde 1997, o governo português se preocupou em tomar algumas medidas para reflexão do advento dessa sociedade, lançando então o chamado Livro Verde que foi publicado no mesmo ano e aprovado pelo Conselho de Ministros.

O objetivo do livro era trazer uma visão estratégica para basear medidas relativas as consequências da sociedade da informação em Portugal, sendo descritas orientações e pautas propostas pelos governantes à época para o enfrentamento de eventuais dificuldades. Percebe-se aqui, que mesmo em 1997, as mudanças sociais influenciadas pelo avanço tecnológico já eram sentidas no Estado português.

O conteúdo que merece destaque no livro diz respeito à possível caducidade dos modelos clássicos de regulamentação, fazendo assim necessário a moderada intervenção do Estado para inserir meios mais atualizados de proteção, frente ao desenfreado avanço social moderno, principalmente em face a questões jurídicas como liberdade de expressão e o não policiamento político-ideológico.

O RGPD seguiu todas as diretrizes da diretiva nº 95/46/CE, contendo os princípios e objetivos por ela positivados, ou seja, o conteúdo geral dos conceitos que englobam os dados pessoais e suas implicações. Existem algumas definições relevante, destaca-se os "dados sensíveis" expostos no nº 51 do Regulamento: "Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e

liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas" (UNIÃO EUROPEIA, 2016, p. 10).

Percebe-se que tal conteúdo é ainda mais delicado, visto que abrange aspectos como a vida sexual, visão política/filosófica, fé religiosa, origem da raça, étnica etc. Não é à toa que a Regulamento destaca o maior aparo à essas matérias mais íntimas e essenciais à descrição da personalidade de cada indivíduo. Porém, esse direito pode ser acessado em casos de relevante interesse público para execução de obrigações que a lei determinar, como em casos que envolvam a segurança pública, segurança do Estado, defesa, prevenção, investigação, repreensão de crimes, execução de ações cíveis e penais dentre outros (artigo 23º, RGPD).

A diretiva europeia n.º 95/46/CE, além da proteção das pessoas singulares no que diz respeito ao tratamento de dados e à livre circulação dos mesmos, também difundia a proteção para as atividades de segurança estatais, portanto, sendo esta já transposta pela RGPD, em tese caracteriza maior proteção para os titulares, além de novos institutos de proteção. Há ainda o decreto-lei n.º 7/2004 que transpôs a diretiva n.º 2000/31/CE, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno, destaca-se a prestação de serviços feitas por intermediários, situados no artigo 12º e seguintes.

A regulamentação dos serviços abrange os prestadores de serviços na internet e os prestadores intermediários, que fazem um trabalho técnico e específico para que a informação seja transportada, obtida ou arquivada. Segundo a própria lei, são serviços que compreendem: transporte (art. 14º), armazenagem intermediária (art. 15º), armazenagem permanente (art. 16º) e associação de conteúdos em rede (art. 17º).

Aos prestadores de serviços intermediários, segundo a lei, suas responsabilidades são diferenciadas a depender dos tipos de serviços exercidos, não possuindo também o dever geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito (art. 12º). Quanto ao serviço de simples transporte, a referida lei os isenta de culpa por eventuais ilegalidades das matérias de transmissão.

Da mesma forma, a lei abrange os que prestam serviços de armazenagem intermediária, entretanto, somente serão responsabilizados caso não procederem conforme as regras do setor, como a atualização de informações ou o uso da tecnologia para obter informações privilegiadas de dados, bem como se ficar caracterizado a não remoção dos

conteúdos arquivados quando obtidos na sua origem (art. 15º).

Os prestadores intermediários do serviço de armazenamento de dados em servidores e associações de conteúdos, respondem apenas, no exercício da sua atividade, por aquilo que de fato tenham conhecimento como manifestamente ilícito.

Conclui-se que os fornecedores de conteúdo, ou seja, aqueles responsáveis por originar as informações na rede, são responsabilizados conforme o regime comum do decreto-lei 7/2004, e que os prestadores intermediários de serviços possuem responsabilidade específica. Trazendo a luz, afirma o artigo 11º que "a responsabilidade dos prestadores de serviços em rede está sujeita ao regime comum, nomeadamente em caso de associação de conteúdos, com as especificações constantes dos artigos seguintes." (DECRETO-LEI N.º 7, 2004, s/p).

No contexto mais recente e no âmbito do direito europeu, destaca-se o Regulamento Geral sobre a Proteção de Dados que foi aprovado em 2018 vinculando todos os países da União Europeia, não sendo necessário prévia aprovação da legislação supletiva pelos estados-membros, visto que não se trata de uma diretiva e sim um regulamento.

A diretiva nº 95/46/CE foi citada na exposição de motivos do Regulamento Geral, confirmando a utilidade dos princípios e diretivas por ela positivados, entretanto, pelo fato da diretiva exigir normas internas de transposição e permitir a supressão de seus institutos por outros ordenamentos internos dos estados-membros, detectou-se a partir desse contexto, um esfacelamento das normas de proteção de dados na União Europeia.

Sabe-se que é livre a circulação de dados pessoais pela internet na União, o que sem dúvida fica prejudicada a aplicação de uma norma interna por um determinado estado-membro. Essa questão abriu o debate para medidas que pudessem instituir apenas uma norma geral para toda a Comunidade Europeia.

Ainda na exposição de motivos que compõem o regulamento, os esforços presentes no RGPD trazem o combate à insegurança e incertezas frente ao caráter comercial do uso da internet, visto que, através de anos de pesquisas, a vigência da diretiva 95/46/CE não trazia um certo conforto nas operações comerciais (principalmente compra e venda) na internet, ocasionando a perda de interesse dos usuários, seja para concretização de atos negociais quanto de consumo.

O Regulamento optou por manter os artigos 12º e 15º da diretiva 2000/31/CE que diz respeito aos prestadores intermediários de serviços, já abordado mais acima. As categorias especiais, que na diretiva 95/46/CE eram tratados como dados pessoais sensíveis, o RGPD acrescentou no seu artigo 9º informações adicionais referentes à orientação sexual, dados

genéticos e condenações criminais ou medidas de segurança, se for o caso. Manteve, entretanto, os demais tipos informações de dados estabelecidos pela diretiva e abrindo exceções no tratamento desses dados à depender de situação onde a lei permite. Em qualquer circunstância, o titular deve ser comunicado.

O direito dos titulares dos dados no regulamento são bastantes claros, a saber, alguns dos mais relevantes: direitos de informação (art. 14º), de acesso (art. 15º), de retificação (art. 16º), de ser esquecido (art. 17º), de limitação do tratamento (art. 18º), de notificação da retificação ou apagamento dos dados pessoais (art. 19º), de portabilidade dos dados (art. 20º), de segurança do tratamento (art. 32º), a comunicação de uma violação de dados pessoais (art. 34º), à tutela jurídica (art. 77º e seguintes). Todos estes citados corroboram em favor da proteção da personalidade, sem prejuízo das outras garantias previstas no regulamento.

O dispositivo mais importante para esse tema, o artigo 17º do regulamento se encontra a positivação do direito ao esquecimento na internet na Comunidade Europeia. Como está assinalado, o titular tem o direito de obter perante o responsável pelo tratamento a extinção de dados pessoais desde que cumpridos os requisitos contidos nas alíneas seguintes. Para requerer o apagamento, basta preencher apenas um requisito, não sendo necessário a cumulação deles.

Entende-se por tratamento "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (art. 4º nº.2, RGPD, 2016) (UNIÃO EUROPEIA, 2016, p. 33).

Se os dados se tornarem obsoletos, ultrapassados, também pode o titular exercer seu direito, visto que a finalidade da sua publicação ou permissão ao acesso se esvaiu. Se o titular retirar o consentimento que baseou o tratamento dos dados, não houver fundamento jurídico para o tratamento, também tem o direito de ser excluídos. Se o titular se opor ao tratamento dos dados nos moldes do artigo 21º, n.º 1 e n.º 2 e nos casos onde não existem interesses legais para o tratamento, deverá proceder a exclusão. Caso os dados pessoais sejam tratados de forma ilícita, tem direito ao apagamento. Por ordem jurídica eivada do direito da União ou de algum Estado-Membro que o responsável pelo tratamento de alguma forma se relacione, serão excluídos. Por fim, situações em que os dados sejam recolhidos de menores de 16 anos sem consentimento dos responsáveis parentais, pode-se exigir o apagamento.

O artigo 17º n. 2º também estabelece que o responsável pelo tratamento, após apagar ou indisponibilizar os dados pessoais do titular, deve tomar outras medidas para que o direito ao esquecimento se concretize em sua plenitude, como a comunicação a terceiros que trataram os dados e estiverem sob sua responsabilidade. Caso contrário, poderá responder solidariamente.

Ainda no artigo, observa-se no n.º 3 o contraponto da liberdade de expressão manifesto e outras exceções, quando o apagamento não será efetivado nos casos em que ficar comprovada a liberdade de expressão, o cumprimento de obrigação legal relativa ao direito da União ou de um Estado Membro, o direito público da saúde, a pesquisa de materiais históricos ou científicos, e em que seja para exercício de defesa de um direito no processo judicial.

A teoria escalonada do ordenamento jurídico é um método em que as normas possuem níveis de hierarquia entre si. Entretanto, para análise de uma norma, deve-se ter uma outra como objeto de comparação, pois não existe hierarquia própria em uma norma individual, carecendo, portanto, do conflito necessário para se estabelecer níveis entre elas. Logo, a Constituição Federal está no topo da pirâmide de normas, servindo como norteadora em qualquer conflito. (GOMIERO, 2005).

"A ponderação de interesses é composta por fases, as quais o intérprete deve incumbir-se de cumprir para alcançar um resultado prático para o caso concreto" (GOMIERO, 2005, p. 42). Só deve-se usar o método da ponderação se existir dois ou mais princípios colidentes.

Segundo Ávila (2004 apud GOMIERO, 2005, p. 95) na primeira fase, que é a "preparação da ponderação", o aplicador do direito deve procurar identificar o conflito normativo, aferindo todos os elementos, indicando o objeto de ponderação. Se for apurada a ocorrência do conflito constitucional, passa-se para a segunda fase, a "realização da ponderação", que é a ponderação propriamente dita. Nesta etapa, o aplicador do direito deve averiguar a relação entre os princípios colidentes, impondo compressões, buscando achar um ótimo ponto, tendo menor restrição possível. Passando por essa fase, a última etapa é a "reconstrução da ponderação" onde a ponderação é concretizada mediante a regras.

É notório saber que a temática do direito ao esquecimento vigora desde a metade do século XX, trazendo sempre novas adequações à sociedade. Com o avanço das novas tecnologias preenchendo as lacunas comportamentais, a proteção ao direito da personalidade sofreu interferências bruscas que dificultaram a sua tutela efetiva, fazendo-se exigir maiores métodos normativos. No passado não tão recente, o direito ao esquecimento era apenas discutido nos registros de antecedentes criminais. Hoje em dia, basicamente se discute em

todos os aspectos da vida civil das pessoas.

Os exemplos clássicos do direito ao esquecimento não mais figuram a atuação principal da tutela do estado, visto que embora importantes, os casos modernos almejam maior preocupação ao direito da personalidade na sociedade da informação ou o direito ao esquecimento digital (ÁLVAREZ CARO, 2015).

Em 2018, como já abordado no capítulo anterior, a vigência da RGPD trouxe ainda mais segurança para os dados dos cidadãos europeus, fortalecendo os mesmos princípios e garantias das diretrizes passadas. O resultado dessas medidas foram algumas condenações da Google com base no novo regulamento, entre elas uma multa de 100 milhões de euros pela Comissão Nacional de Informações e Liberdade (CNIL), autoridade francesa de proteção de dados, por desobedecer a alguns requisitos contidos no novo regulamento. Segundo a Comissão, a empresa americana desobedeceu aos princípios relativos à proteção de informações, transparência e consentimento dos usuários (FRANCE PRESSE, 2020).

## 6. - CONSIDERAÇÕES FINAIS

O presente estudo se propôs em analisar a influência da tecnologia e direito à privacidade face a auto exposição da vida pessoal e íntima dos usuários de forma a responder o questionamento levantado. Conclui-se, portanto, que o avanço tecnológico mudou significativamente a vida das pessoas, observando os casos de Brasil e Portugal. Por tantas mudanças, necessitou-se do amparo do Direito Eletrônico para resguardar diversas questões apresentadas relativas à proteção da privacidade, imagem, entre outros direitos fundamentais

É notável a expressiva massa de pessoas que estão conectadas de alguma forma a algum *wi-fi* ou mesmo serviços telemóveis/*smartphones* que oferecem cobertura completa em tempo real do que está acontecendo no mundo, previsões do tempo, estatísticas da bolsa de valores etc. Quando não estão conectadas, são vigiadas por câmeras, sendo capturados áudio e imagens em determinados locais públicos. Diante de grandes avanços tecnológicos, resta o homem adequar o seu estilo de vida a essa nova maneira de “enxergar” o mundo e aprender a conviver da maneira mais “virtual” e “vigiada” possível.

É importante a investigação do tema para saber se os princípios relativos à vida privada existentes nos ordenamentos jurídicos, em especial, o brasileiro, o português e União Europeia, ainda serão valorados frente as mudanças que a tecnologia proporcionou ao longo dos tempos.

Pretendeu-se investigar também os principais pontos relevantes a esse tema, com o objetivo de acalorar debates aos operadores do direito, visando outra análise argumentativa, capaz de entender as transformações ocorridas no meio social e a relação com o direito à privacidade.

Nos primeiros capítulos, abordou-se a dinâmica geral entre o sistema de videovigilância e a privacidade, traçando as leis que regem o tema em Portugal e opiniões de juristas. No decorrer dos capítulos seguintes abordou-se a influência da *internet*, outra forma de tecnologia, mostrando a legislação brasileira e portuguesa relacionada à eventuais crimes que fazem com que o direito a personalidade seja suprimido pelo uso ilícito da rede, em especial o direito a imagem, a privacidade e o direito ao esquecimento.

Os casos reais que foram narrados e que serviram de base evolutiva para questões mais abrangentes tem sido até hoje estudados e marcam o princípio da aplicação do direito da personalidade no mundo, em específico no Brasil, Portugal e União Europeia. Sem eles, pode-se dizer que jamais haveríamos tal evolução da maneira que foi conduzida, pois é sabido que a ciência jurídica está sempre em desenvolvimento de modo a acompanhar as mudanças sociais.

Este trabalho também trouxe ao cerne, o direito ao esquecimento, sua evolução e base normativa europeia e brasileira. Com muitas nuances que envolvem o tema, percebe-se muita divergência entre juristas quanto a aplicação e o conceito do que vem a ser o esquecimento. A comparação entre as leis que regem o ordenamento jurídico brasileiro e português, serviu para verificar as dimensões dos debates em cada país, além de analisar quais são as suas carências normativas. Pontuou-se os detalhes mais importantes de como as novas tecnologias influenciaram e influenciam até os dias atuais o comportamento humano e o comportamento legislativo. Observa-se que as alterações sociais são extremamente rápidas e a ciência jurídica não consegue de forma eficaz acompanhar tais mudanças extremamente bruscas.

Resta aos operadores do direito sopesar de maneira bastante cautelosa a maior parte dos casos que haja a supressão da privacidade, bem como todos os outros direitos no âmago da personalidade humana, que foram afetados direta e indiretamente pelas novas tecnologias.

É evidente que o uso da videovigilância e o uso da *internet* suprimem o direito à privacidade e imagem, portanto, o legislador estabeleceu normas e limites para o tratamento de dados, garantias para exercer os direitos previstos nas leis já abordadas, bem como a garantia de segurança com as devidas punições nos casos de crimes.

Tal tarefa não é fácil tendo em vista a sua complexidade, exigindo a tutela do Estado para assegurar aos cidadãos, seja do Brasil, Portugal ou União Europeia, a plenitude dos seus direitos protegidos. Por se tratar de um tema atual, a discussão acerta do assunto ainda

perdurará por longos anos.

Dessa forma, o acerto cronológico normativo deve imprescindível frente ao avanço das novas tecnologias. Ainda que seja um desafio quase que improvável, trata-se de direitos e garantias que abrangem várias searas jurídicas, com características peculiares, o que demanda maior cuidado e responsabilidade. Em países onde políticas públicas e sociais são precárias, como no Brasil, fica evidente que a satisfatória garantia dos direitos relativos à personalidade, dificilmente abastecerá toda a população vulnerável, trazendo assim problemas sérios e irreversíveis para as próximas gerações.

## REFERÊNCIAS


ACIOLI, Bruno de Lima; EHRHARDT JÚNIOR, Marcos Augusto de Albuquerque – Uma agenda para o direito ao esquecimento no Brasil. *Revista Brasileira de Políticas Públicas* [Em linha]. Brasília, Vol. 7, nº 3 (2017), p. 383-410. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4867 [Consult. em 30-10-2020].

AGÊNCIA DE MARKETING DIGITAL – Brasil adere à Convenção de Budapeste e se posiciona contra crimes cibernéticos. *Diário do Turismo* [Em linha]. (2019). Disponível em: https://diariodoturismo.com.br/brasil-adere-a-convencao-de-budapeste-e-se-posiciona -contra-crimes/ [Consult. em 15-12-2020].

AGRA, Walber de Moura – *Curso de direito constitucional*. 8ª. ed. Rio de Janeiro: Fórum, 2014. ISBN: 978-85-450-0470-7.

ALEXY, Robert – *Teoria de los derechos fundamentales*. Tradução de Ernesto Garzón Valdés. 2.ª ed. Madrid: Centro de Estudios Políticos y Constitucionales, 2002. ISBN: 8425913934

ÁLVAREZ CARO, María. *Derecho al Olvido em Internet: el Nuevo Paradigma de la Privacidad em la Era Digital*. Madrid: Editorial Reus, 2015.

ANDRADE, José Carlos Vieira de – *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. Coimbra: Edições Almedina, 2010. ISBN: 9724079228.

ARANGO, Rodolfo – El concepto de derechos sociales fundamentales. Bogotá: Editorial Legis, 2005. ISBN: 9586539679.

ASSEMBLEIA DA REPÚBLICA. *Constituição da República Portuguesa* [Em linha]. 2005. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublica Portuguesa.aspx [Consult. em 6-04-2020].

ÁVILA, Humberto. *Teoria dos Princípios – da Definição à Aplicação dos Princípios Jurídicos*. São Paulo: Malheiros Editora, 2004. ISBN: 6558600072.

AYRES, Marcel; RIBEIRO, João Carlos – A representação de si em interações sociais mediadas por instant messengers: o caso whatsapp [Em linha]. *In* Congresso Brasileiro de Ciências da Comunicação, 38, Rio De Janeiro, 2015. Disponível em: http://portalintercom.org.br/anais/nacional2015/lista_area_DT5-CI.htm [Consult. em 01-04-2020].

BISSO, Rodrigo *et al*. Vazamentos de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados – *Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação* [Em linha]. Três de Maio, Vol. 3, nº. 1 (2020). Disponível em: https://revistas.setrem.com.br/index.php/reabtic/article/view/378 [Consult. em 03-09-2020].

BRANCO, Paulo Gustavo Gonet; MENDES, Gilmar Ferreira – *Curso de Direito Constitucional*. 10.ª ed. São Paulo: Saraiva, 2015. p. 280. ISBN: 6555593946.

BRANCO, Sérgio - Memória e esquecimento na internet. Porto Alegre: Arquipélago Editorial, 2017.

BRANDALISE, Camila – Caso de jovem stalker vira o 1º do país investigado pela Lei Maria da Penha. *Universa* [Em linha]. São Paulo (2020). Disponível em: https://www.uol.com.br/universa/noticias/redacao/2020/01/16/caso-de-stalking-e-o-1-do-pais-investigado-como-violencia-domestica.htm [Consult. em 20-12-2020].

BRANDT, Marcos Henrique – Stalking: perseguição obsessiva. *Jornal Estado de Minas* [Em linha]. Minas Gerais, (2013). Disponível em https://amagis.jusbrasil.com.br/noticias/100536991/stalking-perseguicao-obsessiva [Consult. em 07-11-2019].

BRASIL. Centro de Estudos Judiciários do Conselho da Justiça Federal – *Enunciado n. 531*. A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento [Em linha]. *In* Jornada de Direito Civil, 6, Brasília, 2013. Brasília: Centro de Estudos Judiciários do Conselho da Justiça Federal, 2013. Disponível em: http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/enunciados-vi-jornada/view [Consult. em 08-08-2020].

BRASIL – *Constituição (1988). Constituição da República Federativa do Brasil*. Brasília, DF: Senado, 1988.

BRASIL – *Decreto n.º 8.771 de 11 de maio de 2016.* Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações [Em linha]. Brasília, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm [Consult. em 20-12-2020].

BRASIL – *Decreto-lei no 2.848, de 7 de dezembro de 1940.* Código Penal. [Em linha]. Brasília, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm# art147a [Consult. em 20-12-2020].

BRASIL – *Decreto-Lei nº 3.688, de 3 de outubro de 1941*. Lei das Contravenções Penais [Em linha]. Brasília, 1941. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3688-3-outubro-1941-413573-normaatualizada-pe.html [Consult. em 20-12-2020].

BRASIL – *Lei n. 10.406. 10 de janeiro de 2002*. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 2002.

BRASIL – *Lei nº 11.340, de 7 de agosto de 2006*. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal; e dá outras providências [Em linha]. Brasília, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm [Consult. em 19-08-2020].

BRASIL – *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei Nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências [Em linha]. Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm [Consult. em 19-08-2020].

BRASIL – *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [Em linha]. Brasília, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm [Consult. em 08-08-2020].

BRASIL – *Lei nº 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD) [Em linha]. Brasília, 2018ª. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm [Consult. em 08-08-2020].

BRASIL. Ministério da Mulher, da Família e dos Direitos Humanos – *Exposição de crianças e adolescentes na internet ocupa 5ª posição no ranking do Disque 100* [Em linha]. Brasília: Governo Federal, 2020. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/novembro/exposicao-de-criancas-e-adolescentes-na-internet-ocupa-quinta-posicao-no-ranking-de-denuncias-do-disque-100 [Consult. em 15-05-2020].

BRASIL. Superior Tribunal de Justiça – *Recurso Especial Nº 1.316.921 - RJ (2011/0307909-6)* [Em linha]. Relatora: Ministra Nancy Andrighi, Recorrente: Google Brasil Internet Ltda, julgado em 26/06/2012. Brasília, DF, 2012. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201103079096&dt_publicacao=29/06/2012 [Consult. em 15-05-2020].

BRASIL. Superior Tribunal de Justiça – *Recurso Especial Nº 1.660.168 - RJ (2014/0291777-1* [Em linha]. Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018. Brasília, DF, 2018b. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1628798&tipo=0&nreg=201402917771&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20180605&formato=PDF&salvar=false [Consult. em 15-05-2020].

BRIAN, Christian; GRIFFITHS, Tom - Algoritmos para viver: a ciência exata das decisões humanas. São Paulo: Companhia das Letras, 2017.

CABRAL, Bruno Fontenele – "Paparazzi": considerações sobre o direito à privacidade das celebridades ("right to privacy") nos Estados Unidos. *Revista Jus Navigandi* [Em linha]. Teresina, ano 16, nº. 2759 (jan. 2011). Disponível em: https://jus.com.br/artigos/18312 [Consult. em 20-01-2020].

CAETANO, Marcello – *Princípios fundamentais do direito administrativo.* reimp. ed.

Brasileira de 1977. Coimbra: Almedina, 1996.

CANOTILHO, José Joaquim Gomes – *Direito constitucional e teoria da constituição.* 3ª ed. Coimbra: Almedina, 1983. ISBN: 978-9724021065.

CARVALHO, Gisele Primo; PEDRINI, Taina Fernanda – Direito à privacidade na lei geral de proteção de dados pessoais. *Revista da ESMESC* [Em linha]. Santa Catarina. Vol. 26, nº. 32, (2019), p. 363-382. Disponível em: https://revista.esmesc.org.br/re/article/view/217 [Consult. em 02-04-2020].

CARVALHO, Raquel Melo Urbano de – *Direito Administrativo: parte geral, intervenção do Estado e estrutura da administração*. 2.ª ed. rev. atual. ampl. Bahia: Ed. Juspodvim, 2009.

CAVALCANTE, Márcio André Lopes – *Principais julgados do STF e do STJ comentados*. Manaus: Jus Podivm, 2014. ISBN: 978-65-5680-519-1.

CERT.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - *Cartilha de Segurança para Internet*. 2.ª ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CONSELHO DA EUROPA – *Convenção Europeia de Direitos Humanos* [Em linha]. Estrasburgo, 2013. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf [Consult. em 20-12-2020].

CONSTITUIÇÃO da República Portuguesa. Decreto de aprovação da Constituição [Em linha]. *Diário da República*, n.º 86/1976, Série I de 1976-04-10. Disponível em: https://dre.pt/legislacao-consolidada/-/lc/34520775/view [Consult. em 20-12-2020].

CONVENÇÃO sobre a Cibercriminalidade. *Minuta de Relatório Explicativo* [Em linha]. Disponível em: https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf [Consult. em 20-12-2020].

CONVENÇÃO sobre o cibercrime [Em linha]. Budapeste, 2001. Disponível em: https://rm.coe.int/16802fa428 [Consult. em 20-12-2020].

CORDEIRO, António Menezes – *Tratado de Direito Civil IV-parte geral*. 4.ª ed. Coimbra:

Edições Almedina, 2016. ISBN 978-972-40-68046.

DECLARAÇÃO Universal dos Direitos Humanos. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948 [Em linha]. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos [Consult. em 20-12-2020].

DECRETO-LEI n.º 47344. *Código Civil* [Em linha]. Diário do Governo n.º 274/1966, Série I de 1966-11-25. Disponível em: https://dre.pt/web/guest/legislacao-consolidada/-/lc/123928118/202008292026/73747178/diploma/indice [Consult. em 20-12-2020].

DECRETO-LEI n.º 48/95. *Código Penal* [Em linha]. Diário da República, n.º 63/1995, Série I-A de 1995-03-15. Disponível em: https://dre.pt/legislacao-consolidada/-/lc/107981223/201708230100/indice [Consult. em 20-12-2020].

DECRETO-LEI n.º 7/2004. No uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de Maio, transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno [Em linha]. *Diário da República*, n.º 5/2004, Série I-A de 2004-01-07. Disponível em: https://dre.pt/pesquisa/-/search/240775/details/maximized [Consult. em 20-12-2020].

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios – *Acórdão 1249363, 00041942920188070006* [Em linha]. Relator: Waldir Leôncio Lopes Júnior, 3ª Turma Criminal, data de julgamento: 14/5/2020, publicado no PJe: 22/5/2020. Pág.: Sem Página Cadastrada. Disponível em: https://tj-df.jusbrasil.com.br/jurisprudencia/849749450/41942920188070006-df-0004194-2920188070006 [Consult. em 20-12-2020].

DONEDA, Danilo - Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. [Consult. em 24-11-2022].

DOTTI, René Ariel – *Proteção da vida privada e liberdade de informação: possibilidades e limites*. 1.ª ed. São Paulo: Revista dos Tribunais, 1980. ISBN: 9788520300367.

DUARTE, Fernando – Brasil é vice em tempo gasto em redes em ranking dominado por

"emergentes". *British Brodcasting Corporation News* [Em linha]. Brasil (2019). Disponível em: https://www.bbc.com/portuguese/geral-49602237 [Consult. em 20-12-2020].

EURONEWS – *UE combate fenómeno crescente de "stalking"* [Em linha] Portugal (2013). Disponível em: https://pt.euronews.com/2013/06/10/ue-combate-fenomeno-crescente-de-stalking [Consult. em 8-04-2020].

FARIAS, Edilsom Pereira de – *Liberdade de expressão e comunicação: teoria e proteção constitucional*. Florianópolis: Universidade Federal de Santa Catarina, 2001. 290 f. Tese de Doutoramento.

FELICIANO, Guilherme Guimarães – Informática e criminalidade: parte I: lineamentos e definições. *Boletim do Instituto Manoel Pedro Pimentel* [Em linha]. São Paulo, Vol. 13, nº. 2 (2000), p. 35-45. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2001;000621457 [Consult. em 2-09-2020].

FESTAS, David de Oliveira – O direito às reserva da intimidade da vida privada do trabalhador no código do trabalho. *Ordem dos Advogados Portugueses* [Em linha]. Ano 64, Vol. 1/2 (2004). Disponível em: https://portal.oa.pt/publicacoes/revista/ano-2004/ano-64-vol-i-ii-nov-2004/artigos-doutrinais/david-de-oliveira-festas-o-direito-a-reserva-da-intimidade-da-vida-privada-do-trabalhador-no-codigo-do-trabalho-star/ [Consult. em 2-09-2020].

FIUZA, César – *Direito Civil*. 13ª. ed. Belo Horizonte: Revista dos Tribunais, 2009. ISBN: 8520362591.

FRANCE PRESSE – França multa Google e Amazon por violação de lei de privacidade. *Globo News* [Em linha]. Brasil (2020). Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/10/franca-multa-google-e-amazon-por-por-violacao-de-lei-de-privacidade.ghtml [Consult. em 30-12-2020]..

GOMES, Luiz Flavio – Extimidade: nem o preso escapa disso (?). *Jusbrasil* [Em linha]. Brasil, (2012). Disponível em: https://professorlfg.jusbrasil.com.br/artigos/121928398/extimi dade-nem-o-preso-escapa-disso [Consult. em 08-11-2019].

GOMIERO, Bruno – *A ponderação de interesse na Constituição Federal brasileira* [Em linha]. Rio de Janeiro: Pontifícia Universidade Católica, 2005. Disponível em: https://www.maxwell.vrac.puc-rio.br/10144/10144.PDF [Consult. em 7-11-2020]..

GOUVEIA, Jorge Bacelar – *Manual de Direito Constitucional vol. II*. Coimbra: Edições Almedina, 2016. ISBN:9789724067964.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *PNAD 2015 - acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal* [Em linha]. Rio de Janeiro: IBGE, 2015. p. 28-29. Disponível em: http://loja.ibge.gov.br/pnad-2015-acesso-a-internet-ea-televis-o-e-posse-de-telefone-movel-celular-para-uso-pessoal.html [Consult. em 30-03-2020].

JESUS, Damásio Evangelista de – Stalking. *Revista IOB de Direito Penal e Processual Penal* [Em linha]. Brasil (2009). Disponível em: http://sisnet.aduaneiras.com.br/lex/artigos/ pdf/stalking.pdf [Consult. em 5-07-2020].

KREIN, Julia – Novos trustes na era digital: efeitos anticompetitivos do uso de dados pessoais pelo facebook. *Revista de Defesa da Concorrência* [Em linha]. Brasília, Vol. 6, nº 1, (2018), p. 198-231. Disponível em: http://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/382/189 [Consult. em 29-03-2020].

LEI n.º 1/2005. Regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. [Em linha]. *Diário da República*, n.º 6/2005, Série I-A de 2005-01-10. Disponível em: https://dre.pt/pesquisa/-/search/457049/details/maximized [Consult. em 19-08-2020].

LEI n.º 109/91. Lei da criminalidade informática [Em linha]. *Diário da República*, Diário da República n.º 188/1991, Série I-A de 1991-08-17. Disponível em: https://dre.pt/pesquisa/-/search/674438/details/maximized [Consult. em 19-08-2020].

LEI n.º 33/2007. Regula a instalação e utilização de sistemas de videovigilância em táxis [Em linha]. *Diário da República*, n.º 155/2007, Série I de 2007-08-13. Disponível em: https://dre.pt/web/guest/pesquisa/-/search/636950/details/normal?q=Lei+N%C2%BA%2033%2F2007%2C%202007-08-13 [Consult. em 19-08-2020].

LEI n.º 36/2013. Aprova o regime de garantia de qualidade e segurança dos órgãos de origem humana destinados a transplantação no corpo humano, de forma a assegurar um elevado nível de proteção da saúde humana, transpondo a Diretiva n.º 2010/53/UE, do Parlamento Europeu e do Conselho, de 7 de julho, relativa a normas de qualidade e segurança dos órgãos humanos destinados a transplantação [Em linha]. *Diário da República*, n.º 112/2013, Série I de 2013-06-12. Disponível em: https://dre.pt/home/-/dre/496738/details/maximized [Consult. em 19-08-2020].

LEI n.º 51/2006. Regula a instalação e utilização de sistemas de vigilância electrónica rodoviária e a criação e utilização de sistemas de informação de acidentes e incidentes pela EP - Estradas de Portugal, E. P. E., e pelas concessionárias rodoviárias [Em linha]. *Diário da República*, n.º 166/2006, Série I de 2006-08-29. Disponível em: https://dre.pt/pesquisa/-/search/540822/details/maximized [Consult. em 19-08-2020].

LEI n.º 58/2019. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [Em linha]. *Diário da República*, n.º 151/2019, Série I de 2019-08-08. Disponível em: https://dre.pt/pesquisa/-/search/123815982/details/maximized [Consult. em 19-08-2020].

LEI n.º 67/98. Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados) [Em linha]. *Diário da República*, n.º 247/1998, Série I-A de 1998-10-26. Disponível em: https://dre.pt/pesquisa/-/search/239857/details/maximized [Consult. em 19-08-2020].

LEI n.º 9/2012 de 23 de fevereiro. Procede à terceira alteração à Lei n.º 1/2005, de 10 de janeiro, que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum [Em linha]. *Diário da República*, n.º 39/2012, Série I de 2012-02-23. Disponível em: https://dre.pt/pesquisa/-/search/542867/details/maximized [Consult. em 19-08-2020].

LEIBHOLZ, Gerhard – *Die Gleichheit vor dem Gesetz – Eine Studie auf rechtsvergleichender und rechtsphilosophiseher grundlage*. Berlin: Verlag Von Otto Liebmann, 1925.

LEONARDI, Marcel – *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012. ISBN: 8502145142.

LIMA, Luciano de Almeida – *O direito à privacidade nas redes sociais na internet*. Ijuí: Universidade Regional do Noroeste do Estado do Rio Grande do Sul, 2016. 99 f. Dissertação de Mestrado em Direito Humanos.

LUZ, Nuno Miguel Lima da – *Tipificação do crime de stalking no código penal português: introdução ao problema: análise e proposta de lei criminalizadora* [Em linha]. Lisboa: Faculdade de Direito da Universidade Católica, 2012. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/8952/1/TESE.pdf [Consult. em 4-12-2020].

MANTELERO, Alessandro. The EU Proposal for a General Data Protection Regulation and th roots of the 'right to be forgotten' [S.I.:s.n.], 2013. Disponível em <http://dx.doi.org> [Consult. em 25-11-2022].

MARICHAL, José – De volta à névoa: o futuro do Facebook. *Politics* [Em linha]. Rio de Janeiro, (2013). Disponível em: https://www.politics.org.br/edicoes/devolta-%C3%A0-n%C3%A9voa-o-futuro-do-facebook [Consult. em 04-08-2020].

MENDES, Laura Schertel - Privacidade, proteção de dados e defesa do consumidor. São Paulo: Saraiva, 2014. [Consult. em 22-11-2022].

MENEZES, Karina; PRETTO, Nelson De Luca – Pirâmide da Pedagogia Hacker: de sonhos coletivos a engajamentos reais. *Revista Teias* [Em linha]. Rio de Janeiro, Vol. 20, (2019), p. 148-166. Disponível em: https://www.e-publicacoes.uerj.br/index.php/revistateias/article/view/43382/31267 [Consult. em 08-08-2020].

MONCAU, Luiz Fernando Marrey – Esquecimento não é um direito. Abandonaremos esta tola expressão. Dissenso.org., 05 de maio de 2017. Disponível em <http://dissenso.org> [Consult. em 23-11-2022].

MOREIRA, Poliana Bozégia - Direito ao esquecimento. *Revista de Direito* [Em linha]. Viçosa, Vol. 7, nº 02 (Fev. 2016), p. 293-317. Disponível em: https://periodicos.ufv.br/revistadir/article/view/1572 [Consult. em 20-11-2020].

MULHOLLAND, Caitlin - A tutela dos dados pessoais sensíveis. In: MULHOLLAND, Caitlin (Org.) A LGPD e o marco normativo no Brasil. Porto Alegre

NICOLODI, Ana Marina – Conflitos entre direitos fundamentais – liberdade de imprensa versus direito à vida privada, direito à imagem e direito à honra. *Cadernos de Escola de Direito* [Em linha]. Vol. 1, n.º 8 (2008). Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/cadernosdireito/article/view/2575/2148 [Consult. em 07-05-2020].

NOVELINO, Marcelo – *Manual de direito constitucional*. 9. ed. Rio de Janeiro: Forense; São Paulo: Método, 2014. ISBN: 6556803340.

O QUE é um ransomware? – *Tecnoblog* [Em linha]. (2019). Disponível em: https://tecnoblog.net/275356/o-que-e-um-ransomware/# [Consult. em 03-12-2020].

O QUE é um web crawling?: como funcionam os spiders na internet. *Cloudflare* [Em linha]. Brasil (2020). Disponível em: https://cloudflare.com/pt-br/learning/bots/what-is-a-web-crawler/ [Consult. em 05-12-2020].

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Convenção Americana sobre Direitos Humanos* [Em linha]. San José, Costa Rica, 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm [Consult. em 3-12-2020].

PACI, Maria Fernanda – Considerações gerais sobre direito eletrônico. Âmbito Jurídico [Em linha]. Ed. 162 (jun. 2017) Disponível em: https://ambitojuridico.com.br/edicoes/revista-162/consideracoes-gerais-sobre-direito-eletronico/ [Consult. em 05-11-2019].

PAESANI, Liliana Minardi. *Direito e internet: liberdade de informação, privacidade e responsabilidade civil.* 7. ed. São Paulo: Atlas, 2014. ISBN: 8522478910.

RAMOS FILHO, Evilásio Almeida – *Direito ao esquecimento versus liberdade de informação e de expressão: a tutela de um direito constitucional da personalidade em face da sociedade de informação* [Em linha]. Fortaleza: ESMEC, 2014. Disponível em: http://portais.tjce.jus.br/esmec/wpcontent/uploads/2014/12/Direito-ao-Esquecimento-vs-Liberdade-deInforma%C3%A7%C3%A3o.pdf [Consult. em 06-04-2020].

RESOLUÇÃO do Conselho de Ministros n.º 41/2018. Define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais [Em linha]. *Diário da República*, n.º 62/2018, Série I de 2018-03-28. Disponível em: https://dre.pt/application/conteudo/114937034 [Consul. em 20-12-2020].

RIBEIRO, Bárbara Maria Dantas Mendes – Colisão de direitos fundamentais. *Jus.com* [Em linha]. (2018). Disponível em: https://jus.com.br/artigos/67467/colisao-de-direitos-fundamentais [Consult. em 05-11-2020].

RODOTÀ, Stefano - Il mondo nella rete Quali i diritti, quali i Vincoli. Roma: Editori Laterza. 2014.

RODOTÀ, Stefano - A Vida na Sociedade da Vigilância: a privacidade hoje. Rio de Janeiro: Editora Renovar, 2007.

RODRIGUES, Catarina – Quando gostar se torna sufocante, o stalking contado por uma vítima. *Observador* [Em linha]. Portugal (2014). Disponível em: https://observador.pt/2014/09/04/ quando-gostar-se-torna-sufocante-o-stalking-contado-por-uma-vitima/ [Consult. em 05-11-2020].

ROSSINI, Augusto Eduardo de Souza – *Informática, telemática e direito penal*. 1.ª ed. São Paulo: Memória Jurídica, 2004. ISBN: 8588264242.

SARMENTO, Daniel – A liberdade de expressão e o problema do 'Hate Speech'. *RDE. Revista de Direito do Estado* [Em linha]. Vol. 4, (2006) p. 53-106. Disponível em: http://professor.pucgoias.edu.br/sitedocente/admin/arquivosUpload/4888/material/a-liberdade-de-expressao-e-o-problema-do-hate-speech-daniel-sarmento.pdf [Consult. em 05-07-2020].

SARMENTO, Daniel – Liberdades Comunicativas e "Direito ao Esquecimento" na ordem constitucional brasileira. Migalhas, Rio de Janeiro, 22 de jan. de 2015. Disponível em <http://migalhas.com.br >[Consult. em 22-11-2022]

SIBILIA, Paula – *La intimidad como espectáculo*. Buenos Aires: Fondo de Cultura Económica, 2013. ISBN: 9505577540.

SIBILIA, Paula; DIOGO, Lígia – Vitrines da intimidade na Internet: imagens para guardar ou para mostrar? *Estudos de Sociologia* [Em linha]. Araraquara, Vol. 16, nº. 30 (2011) p. 127-139. Disponível em: https://periodicos.fclar.unesp.br/estudos/article/view/3892 [Consult. em 08-08-2020].

SILVA, Germano Marques da – A polícia e o direito penal. *Polícia Portuguesa*. n.º 82 (jul/ago 1993).

SILVA, José Afonso da – *Curso de direito constitucional positivo*. 33. ed. São Paulo: Malheiros, 2010. ISBN: 978-85-392-0462-5.

SILVEIRA, Ismael dos Santos; BARBOSA, Albert Santos; NUNES, Maria Augusta Silveira Netto – O que é um hacker? *Almanaque para popularização de ciência da computação. Série 1, Informática, ética e sociedade* [Em linha]. Sergipe, Vol. 4, (2016). Disponível em: https://ri.ufs.br/jspui/handle/riufs/8371 [Consult. em 28-09-2020].

SOUSA, António Francisco – Prevenção e repressão como função da polícia e do Ministério Público. *Revista do Ministério Público*, n.º 94 (2003), p. 49.

SCHREIBER, Anderson - As três correntes do direito ao esquecimento. Revista Jota, 18 de jun. de 2017. Disponível em <http://jota.info/artigos> [Consult. em 24-11-2022].

STALKER de Madonna na década de 1990 foge de instituição mental. *G1 News* [Em linha]. Brasil (2012). Disponível em: http://g1.globo.com/mundo/noticia/2012/02/perseguidor-de-madonna-na-decada-de-1990-foge-de-instituicao-mental.html [Consult. em 05-06-2020].

TECH FAQ – *Understanding Network Attacks*. 2010. Disponível em: https://www.tech-faq.com/network-attacks.html [Consult. em 05-06-2020].

TEFFÉ, Chiara Spadaccini; MORAES, Maria Celina Bodin de – Redes sociais virtuais: privacidade e responsabilidade civil: análise a partir do marco civil da internet. *Pensar-Revista de Ciências Jurídicas* [Em linha]. Fortaleza, Vol. 22, nº. 1, (2017) p. 108-146. Disponível em: https://periodicos.unifor.br/rpen/article/view/6272 [Consult. em 07-09-2020].

THE POLICE FUNDATION – *The briefing-CCTV* [Em linha]. 2014. Disponível em:

https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf [Consult. em 07-09-2020].

TRIBUNAL DA RELAÇÃO DE GUIMARÃES – *Acórdão do Tribunal da Relação de Guimarães*. Processo 332/16.6PBVCT.G1. Relator: Alda Casimiro, data de julgamento 05/06/2017 [Em linha]. Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6ed245a0db9eefd58025814500361e75?OpenDocument [Consult. em 07-09-2020].

UNIÃO EUROPEIA – *Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014, Processo C‑131/12* [Em linha]. 2014. Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d585485bc5ed1a4a0698fdcbaf380e2b01.e34KaxiLc3qMb40Rch0SaxuNb3z0?text=&docid=152065&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=262988 [Consult. em 07-09-2020].

UNIÃO EUROPEIA – *Acórdão do Tribunal de Justiça de 6. 11. 2003, Processo c-101/01* [Em linha]. Luxemburgo, 2003. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62001CJ0101&from=en [Consult. em 07-09-2020].

UNIÃO EUROPEIA. Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico») [Em linha]. *Jornal Oficial*, nº L 178 de 17/07/2000 p. 0001 – 0016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32000L0031 [Consult. em 19-08-2020].

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [Em linha]. *Jornal Oficial*, nº L 281 de 23/11/1995 p. 0031 – 0050. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046 [Consult. em 19-08-2020].

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 [Em linha]. *Jornal Oficial da União Europeia*, L 119/1-86. Disponível em: https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-

_protecao_de_ dados.pdf [Consult. em 19-08-2020].

VARANDA, Artur Eduardo Lago Torres – *O Regulamento Geral de Proteção de Dados e a pseudonimização de logs*. Leiria: Instituto Politécnico de Leiria, 2019. 149 f. Dissertação de Mestrado em Cibersegurança e Informática Forense.

VIEIRA, Tatiana Malta **–** *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Brasília: Universidade de Brasília, 2007. 297f. Dissertação de Mestrado em Direito.

ZUBOFF, Shoshana. The age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Nova Iorque: Public Affairs, 2018, pos. 188 (e-book).

WENDT, Emerson; JORGE, Higor Vinicius Nogueira **–** *Crimes cibernéticos: ameaças e procedimentos de investigação*. 2.ª ed. Rio de Janeiro: Brasport, 2013. ISBN: 9788574526362. p. 52-53.

WIKIPÉDIA, a enciclopédia livre – *Carolina Dieckmann* [Em linha]. Flórida: Wikimedia Foundation, 2021[b]. Disponível em https://pt.wikipedia.org/w/index.php?title=Carolina_Dieckmann&oldid=60662842 [Consult. em 16-03-2021].

WIKIPÉDIA, a enciclopédia livre – *Convenção do Conselho da Europa para a Prevenção e o Combate à Violência Contra as Mulheres e a Violência Doméstica* [Em linha]. Flórida: Wikimedia Foundation, 2020[a]. Disponível em: https://pt.wikipedia.org/w/index.php?title=Conven%C3%A7%C3%A3o_do_Conselho_da_Europa_para_a_Preven%C3%A7%C3%A3o_e_o_Combate_%C3%A0_Viol%C3%AAncia_Contra_as_Mulheres_e_a_Viol%C3%AAncia_Dom%C3%A9stica&oldid=57969689 [Consult. em 06-04-2020].

WIKIPÉDIA, a enciclopédia livre – *Rebecca Schaeffer* [Em linha]. Flórida: Wikimedia Foundation, 2021[a]. Disponível em: https://pt.wikipedia.org/w/index.php?title=Rebecca_Schaeffer&oldid=60543844 [Consult. em 28-02-2021].

WIKIPÉDIA, a enciclopédia livre. *Backdoor* [Em linha]. Flórida: Wikimedia Foundation, 2020[b]. Disponível em: https://pt.wikipedia.org/w/index.php?title=Backdoor&oldid=57456394 [Consult. em 17-02-2020].

WIKIPÉDIA, a enciclopédia livre. *Ovo de páscoa (virtual)* [Em linha]. Flórida: Wikimedia Foundation, 2020[c]. Disponível em: https://pt.wikipedia.org/w/index.php?title=Ovo_de_p%C3%A1scoa_(virtual)&oldid=58540961 [Consult. em 18-06- 2020].

WU, Tim – *Impérios da Comunicação. Do telefone à Internet, da AT&Tao Google.* Trad. de C. Carina. Rio de Janeiro: Zahar, 2012. ISBN: 853780889X.