CONFLUÊNCIAS | Entrevista

ISSN: 1678-7145 | E-ISSN: 2318-4558

Seção Entrevistas

Volume 26, Número 2, agosto de 2024
Submetido em: 21/08/2024
Aprovado em: 03/10/2024

ENTREVISTA COM A PROFESSORA MÓNICA ARENAS RAMIRO, professora da Universidade de Alcalá

Mónica ARENAS RAMIRO[1]
Universidade de Alcalá (UAH)

Eder Fernandes MONICA (Eder van PELT)[2]
Universidade Federal Fluminense (UFF)

Hilbert REIS[3]
Universidade Federal Fluminense (UFF)

Prof.ª Mónica Arenas Ramiro

Entrevista realizada por e-mail em maio de 2024.

[1] Professora de Direito Constitucional da Universidade de Alcalá (UAH) – Espanha. Doutora em Direito pela Universidade de Alcalá (UAH). Delegada de Proteção de Dados da Universidade de Alcalá (UAH). – E-mail: monica.arenas@uah.es – Orcid: https://orcid.org/0000-0002-9329-2246.

[2] Professor adjunto da Faculdade de Direito e Professor permanente do Programa de Pós-Graduação em Sociologia e Direito da Universidade Federal Fluminense. (UFF). Doutor em Ciências Jurídicas e Sociais pela Universidade Federal Fluminense (UFF). – E-mail: ederfm@id.uff.br – Orcid: https://orcid.org/0009-0000-5666-6491.

[3] Professor de Direito da Escola Técnica Estadual "José Martimiano da Silva" (ETEC – Ribeirão Preto). Doutorando em Sociologia e Direito pela Universidade Federal Fluminense (UFF) – E-mail: hilberts@id.uff.br – Orcid: https://orcid.org/0000-0002-9539-4844.

Estimada Professora Mónica Arenas Ramiro. Inicialmente, gostaríamos de agradecer a sua participação nesta entrevista. Muito brevemente, nesta introdução, destacaremos seus trabalhos mais importantes e recentes, especialmente aqueles sobre consentimento nas redes sociais (2010), brechas digitais de gênero (2011), transparência e partidos políticos (2017 e 2021), aplicativos de rastreio de contatos e o passaporte COVID (2021), e partidos políticos e Internet (2022). Assim, gostaríamos de ampliar um pouco esta apresentação, perguntando sobre sua trajetória acadêmica e projetos de pesquisa.

Eder Monica; Hilbert Reis: O que a motivou a conciliar as aulas de Direito Constitucional com as pesquisas sobre sociedade digital e proteção de dados? Poderia nos contar sobre o início dessa experiência e os motivos que a levaram a abordar essas questões tão delicadas em nossa contemporaneidade?

Mónica Ramiro: Sempre me preocupei muito com a proteção da dignidade das pessoas e com os perigos dos avanços tecnológicos e científicos. No fundo, questionava-me como o uso indevido das nossas informações pessoais, que poderia aumentar exponencialmente com as técnicas informáticas, poderia condicionar a nossa forma de viver em sociedade, de nos relacionarmos, comunicarmos e participarmos. Mas também me interessava, por outro lado, o fato desses mesmos receios e temores dos avanços tecnológicos representarem um freio ao avanço digital de nossas sociedades e à pesquisa ou inovação. Desde Hipátia de Alexandria, quantos e quantas pesquisadores e cientistas não foram martirizados pelas suas ideias e quantas invenções não foram perdidas por fruto do temor ao desconhecido.

Quando o meu Diretor de Tese — há muitos, demasiados anos — disse-me para pensar em um tema de pesquisa, sabia que queria escrever sobre algo impactante na vida dos cidadãos, que tivesse a capacidade disruptiva de transformar as pessoas e o Estado. E por isso optei por analisar a regulamentação do tratamento de dados pessoais.

Não é certo que a informação seja o petróleo do século XXI. Informação sempre foi poder. Não é algo novo. Mas os avanços tecnológicos permitiram formas melhores e mais poderosas formas de coletar, armazenar e distribuir dados, entre outras coisas.

Não podemos esquecer que o controle desta informação deveria ser um poder de todos os cidadãos, de cada um de nós, porque se trata da nossa informação pessoal, o que nos identifica e nos define. É nosso direito fundamental. E por isso a importância de lhe dar uma abordagem constitucional, a partir do prisma dos direitos fundamentais. Os dados são objeto de proteção de um direito fundamental: o direito fundamental à proteção de dados. Isto pode ser encontrado no texto constitucional espanhol (no seu artigo 18.4 — embora não expressamente —) e em muitos outros textos constitucionais, esse habeas data, inclusive internacionalmente com a proteção da vida privada pelo Conselho da Europa por meio da Convenção Europeia dos Direitos Humanos de 1950, ou ao nível europeu conforme expresso pela Carta dos Direitos Fundamentais da União Europeia. Ocorre que perdemos isso de vista e passamos a monetizar um direito fundamental, deixando-o nas mãos de gigantes tecnológicos cuja principal função não é servir à cidadania.

Devemos encontrar um equilíbrio. Um equilíbrio entre a tecnologia e o Direito, um equilíbrio e uma colaboração necessária entre o setor público e o setor privado. Estou convencida de que só conseguiremos isso se o fizermos sob o prisma do Direito Constitucional, a partir de uma reinterpretação da Teoria dos direitos fundamentais e do Estado, por ser certo que estamos perante uma mudança de paradigma.

Eder Monica; Hilbert Reis: Em "*Brecha digital de género: la mujer y las nuevas tecnologías*", de 2011, com uma dose de esperança sobre as novas tecnologias digitais desde perspectiva de gênero, a senhora conclui que: "se queremos uma sociedade democrática, devemos defender o reconhecimento das mulheres como sujeitos de direitos, como criadoras e não como meras destinatárias, e que isto não seja visto como mera manifestação teórica" (RAMIRO, 2011, p. 120). Treze anos depois, com o avanço contínuo das Tecnologias de Informação e Comunicação (TIC) e com o aumento de questões que envolvem a cultura tecnológica na perspectiva de gênero, qual o seu diagnóstico sobre os avanços e retrocessos nesta questão?

Mónica Ramiro: Dizem que as crianças pequenas têm pequenos problemas e as crianças grandes têm grandes problemas. Não estou dizendo que a digitalização seja um problema, mas é um grande desafio, um enorme desafio. E para grandes desafios, grandes respostas. E a

resposta não deve ter apenas um enfoque internacional, para além das fronteiras, porque a digitalização quebra barreiras, devendo ter também um enfoque de gênero.

Devemos também aplicar a perspectiva de gênero aos avanços tecnológicos. Estou convencida de que a tecnologia é neutra, mas as pessoas que a desenha e a aplica não o são. Portanto, se tivermos sociedades que discriminam, a nossa tecnologia, a nossa sociedade digital também será discriminatória. As ferramentas de IA (inteligência artificial) são alimentadas por dados e informações pessoais. Se alimentarmos "a besta" com dados ruins, com algoritmos discriminatórios, nossa IA será sexista ou xenófoba. Se tivermos sociedades que discriminam, teremos tecnologia e ferramentas tecnológicas que discriminam. Não podemos ficar surpresos que uma IA que aprende com o Twitter se torne sexista ou racista, pois não poderia ser de outra forma.

Em questão de gênero, no caso das mulheres, o problema ocorre porque o acesso, utilização, concepção e controle das novas ferramentas tecnológicas e da Internet é marcado por fortes estereótipos sociais. É ilusório e irrealista afirmar que atualmente não existem diferenças injustificadas de tratamento e que estas não são perpetuadas mediante estereótipos de ódio reproduzidos na Internet e pelos algoritmos e inteligências artificiais que estão programados para tomar decisões que afetam os cidadãos.

Por esta razão, estou convencida de que estamos em um ponto, em um momento da história no qual podemos reverter a ordem estabelecida e aproveitar esta mudança de paradigma para quebrar os odiosos estereótipos que permanecem ancorados nas nossas sociedades. A tecnologia permite isso: sermos mais participativos independentemente do gênero, mas, ao mesmo tempo, permite-nos utilizar informações pessoais para ter em conta as necessidades específicas de um determinado gênero.

As possibilidades que se abrem para criar sociedades mais justas e igualitárias são inquestionáveis, da mesma forma que é inegável que o ambiente digital não fará outra coisa senão reproduzir os odiosos estereótipos discriminatórios, não apenas de gênero, que existem na nossa atual sociedade, se não o evitarmos.

Devemos partir do fato de que a tecnologia é mais um instrumento nas mãos das pessoas, uma ferramenta neutra que favorece a integração das pessoas na sociedade e que terá os efeitos

positivos ou negativos que nós próprios lhes proporcionamos, embora carregados, pois não pode ser diferente com a nossa bagagem social. O problema, portanto, não serão os instrumentos ou a tecnologia utilizada, mas o tipo de sociedade que construímos, onde se gere a referida informação e ao serviço da qual se colocam esses instrumentos.

Daí a importância, como acabamos de sinalizar, de que a concepção e utilização de algoritmos ou ferramentas como a Inteligência Artificial respeite os direitos fundamentais desde uma perspectiva de gênero, tendo em conta os papéis que tradicionalmente são atribuídos às mulheres e que condicionam o seu acesso e uso da tecnologia, a fim de erradicar as diferenças existentes, adaptando-as a um ambiente digital. Tudo isto, ao mesmo tempo que os poderes públicos e o setor tecnológico tomem as medidas necessárias para reconhecer as mulheres como sujeitos de direitos com oportunidades iguais aos homens. Por esse mesmo motivo, devemos eliminar não só as barreiras de acesso, mas também as barreiras que nos excluem da tomada de decisões e da concepção no domínio das TIC.

Eder Monica; Hilbert Reis: Nos últimos anos, muitos países, entidades e pessoas foram vítimas de espionagem por meio de programas de computador. Em 2021, com o apoio da Anistia Internacional e da ONG francesa *Forbidden Stories*, estimou-se que mais de 50 mil jornalistas, empresários, defensores dos direitos humanos, líderes religiosos e chefes de estado de diversos países podem ter sido vítimas de espionagem através do programa de computador de espionagem chamado 'Pegasus', desenvolvido pela empresa israelense *NSO Group*. No ano seguinte, um comunicado do Governo de Espanha, de 2 de maio de 2022 (MENÉNDEZ, 2022), informava sobre a utilização do Pegasus para espionar o Presidente do Governo e o Ministro da Defesa. Em 2024, a Polícia Federal brasileira iniciou a Operação “Vigilância Aproximada” para investigar o uso indevido do programa *FirstMile*, da empresa israelense *Cognyte* (anteriormente chamada de *Verint*) (CNN, 2024).

Neste caso, estão sendo investigadas situações de espionagem ilegal de algumas autoridades importantes do Brasil. Diante desses casos de espionagem por intermédio de programas informáticos, que envolvem Estados democráticos, quais os reais riscos da utilização destes programas para as democracias, especialmente em relação aos Estados democráticos?

Mónica Ramiro: É evidente que se os cidadãos souberem que são vigiados ou, mesmo que não estejam a ser vigiados, suspeitarem dessa vigilância, não agirão com a mesma liberdade como se controlassem o que se sabe ou o que se conhece sobre eles.

O filósofo inglês Jeremy Bentham já nos alertava para isso no final do século XVIII com a ideia do panóptico (modelo de estrutura prisional que consiste na existência de uma torre de vigilância central rodeada de celas, da qual os presos não sabiam se havia ou não alguém vigiando na torre). Assim, se os cidadãos não controlarem o que se sabe sobre eles, não participarão livremente na sociedade da qual fazem parte, afetando diretamente o princípio democrático.

Mas a questão não é só esta; o verdadeiro problema é o uso ilícito que está a ser feito deste tipo de ferramentas, ou seja, a finalidade para a qual estes programas são utilizados: essencialmente, controlar os cidadãos e, mais especificamente, os cidadãos que têm representação ou poder de decisão estatalmente e, assim, desestabilizar os Estados; ou monitorar potenciais elementos subversivos contra o poder estabelecido, embora sem as garantias de um Estado de direito.

Neste sentido, tenta-se justificar a utilização ilícita destes programas sob o pretexto da segurança nacional. O eterno e falso debate: proteger direitos ou garantir a segurança nacional. Contudo, em um Estado de direito, o fim não justifica os meios.

A ideia de democracia não implica exclusivamente a ideia de participação, que só pode ocorrer em condições de liberdade, mas também de responsabilização, e isso só pode ocorrer à luz do sol, ou seja, à luz da transparência e responsabilidade dos poderes públicos. A democracia só pode ser exercida em condições de transparência, implicando a responsabilização dos poderes públicos. Assim, a utilização deste tipo de sistema deve ser transparente quanto à sua existência, condições de uso e garantias.

Estamos configurando os parâmetros da privacidade em um mundo digitalizado e aberto a novas ameaças que abalam a estabilidade dos nossos Estados, mas devemos evitar transformar os nossos Estados democráticos em Estados policiais. Caso contrário, como o TEDH já decidiu no caso Klass, corremos o risco de "destruir a democracia para defendê-la" (§ 49).

Eder Monica; Hilbert Reis: Diante do problema jurídico consistente em saber se os Estados podem ou não monitorizar os seus cidadãos de uma forma tão sensível, sob o pretexto da segurança nacional, poderia partilhar a sua impressão sobre as atuais soluções jurídicas disponíveis em Espanha e na Europa para casos desta natureza?

Mónica Ramiro: O lado negativo, ou mais negativo, da tecnologia nos revela casos de espionagem massiva de cidadãos estrangeiros ou nacionais por meio de serviços de inteligência não sujeitos ao princípio do Estado de Direito, o controle total da população através do reconhecimento facial, à alteração da vontade democrática por meio de técnicas de manipulação neuro-emocional nas redes, da falsificação da realidade mediante de estratégias de desinformação e notícias falsas, ou do efeito discriminatório através da utilização de algoritmos baseados na caracterização dos sujeitos através do conhecimento dos seus dados pessoais. Estes são bons exemplos de riscos, embora não sejam os únicos.

Estas ameaças afetam, de uma forma ou de outra, em maior ou menor grau, todos os direitos e liberdades que conhecemos, desde a liberdade de informação, expressão e informação, até aos direitos de participação, privacidade e igualdade, entre outros, e, em última análise, à dignidade e ao livre desenvolvimento pessoal.

Assim, é necessário adaptar as garantias existentes para isto não acontecer. A tecnologia deve estar a serviço da humanidade. E daí a sua configuração conforme a lei e, fundamentalmente, de acordo com princípios e valores éticos.

Embora a segurança nacional seja um objetivo legítimo que permite a utilização de programas de espionagem e limitação dos nossos direitos fundamentais, em um Estado democrático e de Direito toda limitação de direitos deve estar contida numa regra clara e previsível e deve, também, ser necessária numa sociedade democrática, o que implica passar num rigoroso teste de proporcionalidade, para que, quando confrontados com mecanismos menos prejudiciais para atingir um objetivo legítimo, sejam estes aqueles que deverão ser utilizados. Esta é a indicação não só dos Tribunais, mas também das autoridades de proteção de dados, como o Comitê Europeu para a Proteção de Dados (CEPD).

Já em 1978, o Tribunal Europeu dos Direitos Humanos (TEDH) decidiu sobre a questão no caso Klass e, quarenta anos depois, em 2021, no caso *Big Brother Watch*, o TEDH concluiu

que embora estes sistemas em si não contrariem o Convenção Europeia dos Direitos Humanos (CEDH), é necessário que "sejam limitados aos casos estritamente necessários para salvaguardar as instituições democráticas" e que tenham "garantias adequadas e eficazes contra abusos". Igualmente, o Tribunal de Justiça da União Europeia (TJUE), em 2020, no caso *Quadruture Du Net*, observou que as restrições à proteção dos dados pessoais devem ser estabelecidas sem ultrapassar os limites do estritamente necessário, de modo que será essencial a realização da ponderação correspondente.

Mais contundente foi o CEPD que, nas observações publicadas em fevereiro de 2022, com referência expressa ao Pegasus, reconheceu o seu potencial e a dificuldade do seu controle e — duvidando que a sua utilização possa ser considerada proporcional mesmo com o objetivo legítimo de prevenir a criminalidade ou manter a segurança nacional segurança, devido ao elevado nível de interferência na vida privada — recomendou a sua proibição. Isto é, como já dissemos, o fim não justifica os meios. E o Parlamento Europeu se pronunciou na mesma linha em uma Recomendação, de junho de 2023, sobre a utilização deste tipo de programas de espionagem de vigilância. Sua aquisição e utilização deverão ser excepcionais e legalmente previstas.

Eder Monica; Hilbert Reis: Como professora de Direito Constitucional na Universidade de Alcalá desde 1999, acredita ser possível harmonizar, do ponto de vista jurídico, a garantia dos direitos fundamentais e a utilização de sistemas de vigilância pelos Estados?

Mónica Ramiro: Dado que parece inegável que os sistemas de vigilância são necessários para garantir a estabilidade dos Estados, e que não podemos tapar o sol com um dedo, se finalmente decidirem utilizá-los, só nos restam as garantias.

Entre as garantias a reforçar, citadas nas Observações do CEPD de 2022 e na Recomendação do Parlamento Europeu de junho de 2023, destacamos: reforçar sua supervisão eficaz através de autoridades de proteção de dados e de controles judiciais antes e depois da sua utilização; aplicar rigorosamente os regulamentos de proteção de dados; reduzir o risco de os dados obtidos com estes programas cheguem a bases de dados localizadas na União Europeia; e, finalmente, capacitar a sociedade civil para aprender sobre a utilização destes sistemas.

A ideia de sigilo e confidencialidade que deveria envolver estes sistemas de vigilância é muitas vezes confundida com a necessidade da não aplicação dos princípios da transparência e da responsabilização. Obviamente, os sujeitos investigados não devem ser informados de que estão sendo investigados para poderem se evadir de suas responsabilidades, mas os cidadãos, inclusive os investigados, devem estar cientes da existência dessas ferramentas e das garantias que envolvem o seu uso, bem como as responsabilidades derivadas de sua utilização ilícita.
Estou convencida da possibilidade e, sobretudo, da necessidade de utilizar este tipo de instrumentos de vigilância e de poder respeitar, ao mesmo tempo, os direitos fundamentais dos cidadãos. A criminalidade utiliza cada vez mais formas sofisticadas de cometer crimes e aproveita as vantagens oferecidas pelas ferramentas tecnológicas e pela Internet para evitar a aplicação da lei.

Contudo, é verdade, que para alcançar este equilíbrio é necessário criar uma cultura e uma vontade não só nos cidadãos — mediante a criação de confiança nos poderes públicos — mas também nos poderes públicos, que utilizarão destas ferramentas. Os funcionários públicos devem ser capacitados, formados em uma cultura de privacidade, para compreenderem a necessidade de respeitar e garantir direitos mesmo em situações complexas onde a segurança nacional está em jogo.

Eder Monica; Hilbert Reis: Professora, esqueçamos um pouco a perspectiva da vigilância por parte do Estado e passar para a questão da proteção dos dados pessoais e da privacidade dos cidadãos. Sabemos que muitos aeroportos, shopping centers e até hospitais utilizam tecnologia de rastreamento *Wi-Fi*. Você poderia comentar brevemente sobre os riscos desta tecnologia para nós, usuários comuns da Internet?

Mónica Ramiro: Hoje em dia vivemos conectados à tecnologia, aos nossos dispositivos móveis e estes estão configurados, erroneamente, para nos localizarem.
Como temos comentado, o objetivo deve ser o uso da tecnologia a serviço da humanidade. O objetivo deve ser utilizar ferramentas e tecnologias que nos levem a localizar pessoas em situações de vulnerabilidade ou perigo e que garantam a segurança e integridade dos cidadãos. Esse deveria ser o propósito dessas tecnologias de rastreamento *WI-FI*. E tudo o que exceda esse propósito legítimo e que não tenha garantias adequadas deve ser proibido.

As vantagens que estas tecnologias oferecem são muitas, mas também os perigos ou riscos que acarretam, uma vez que o rastreamento *WI-FI* envolve o tratamento de dados pessoais, oferecendo informações não só de presença em determinado local, mas também de localização ou rastreabilidade da mobilidade de uma pessoa. E quando isso é feito sem o controle do titular dos referidos dados, sem o seu conhecimento, essa perda de controle já é um problema para a nossa privacidade.

Eder Monica; Hilbert Reis: Recentemente, a Agência Espanhola de Proteção de Dados, o Conselho Andaluz de Proteção e Transparência de Dados, a Autoridade Basca de Proteção de Dados e a Autoridade Catalã de Proteção de Dados desenvolveram diretrizes para o uso de tecnologias de rastreamento *Wi-Fi* (AEPD *et al*., 2024). Como a senhora avalia a implementação de diretrizes e orientações de órgãos e autoridades sobre transparência e proteção de dados para uso de rastreamento de *Wi-Fi*? Isso está previsto no RGPD?

Mónica Ramiro: As autoridades de proteção de dados, sejam estatais, regionais e, da mesma forma, ao nível europeu, estão realizando um importante trabalho, apesar de realizarem o seu trabalho de "pregar no deserto", numa sociedade onde os paradigmas mudaram e os cidadãos, apesar de valorizarem a sua privacidade, decidem compartilhar suas informações pessoais nas redes sociais por um minuto de glória ou fama. A isto soma-se um elevado grau de desconfiança dos cidadãos e uma escassez de recursos, tornando o trabalho que realizam ainda mais louvável. Neste universo das tecnologias de rastreamento *WI-FI*, as próprias Autoridades de Controle indicam expressamente nas referidas Diretrizes: "todas as pessoas devem ter o direito de circular livremente sem "se sentirem espionadas". Esta ideia se conecta com a nossa resposta aos programas espiões. É verdade que o propósito inicial é diferente, mas a percepção cidadã de se sentir observado é a mesma. É essa expectativa de privacidade do ser humano que necessita ser respeitada, que deve ser garantida porque é, nesse contexto, que nos desenvolveremos, participaremos e tomaremos decisões livremente.

Veja, uma coisa é o trabalho das Autoridades de Controle e outra, muito diferente, é o cumprimento e implementação das suas Diretrizes e Orientações, pois estas dependem, como também foi dito, da vontade do setor público e privado. De serem convencidos da necessidade de garantir os direitos dos cidadãos, de garantir a sua privacidade enquanto são tomadas

medidas que possam limitar essa privacidade. Devemos recordar que os direitos não são ilimitados. Não existem direitos ilimitados. O que acontece é que estas limitações, num Estado de direito, devem estar sujeitas a restrições e à existência de garantias necessárias previstas em lei.

O RGPD foi qualificado como um mecanismo normativo neutro, tecnologicamente neutro, que não faz referência a uma ferramenta ou tecnologia específica e, portanto, não se refere a ferramentas de rastreamento *WI-FI* nem se refere explicitamente a sistemas biométricos ou reconhecimento facial.

O RGPD refere-se apenas ao fato de que determinados tratamentos de dados pessoais, que podem incluir dados especialmente protegidos ou categorias especiais de dados, devem ser garantidos e adotados sob a proteção de uma previsão legal, quer esteja prevista na legislação da União Europeia ou nas normativas estatais correspondentes.

Eder Monica; Hilbert Reis: Recentemente, numa consulta que fizemos a um site espanhol, foi exigida uma contraprestação [econômica] para exercer o direito ao anonimato (caso quiséssemos o acesso gratuito, deveríamos aceitar *cookies*; caso contrário, deveríamos pagar pelo acesso). O que a senhora pensa desse tipo de cobrança por sites e redes sociais? A luz do RGPD, seria possível esse tipo de contraprestação para garantir o direito anonimato na internet?

Mónica Ramiro: Não, isso não é normal. Devemos estar cientes de que foram feitos muitos progressos, especialmente nos últimos anos, no que diz respeito à implementação de normativas de proteção de dados, mas ainda há caminhos a percorrer.

No que diz respeito à utilização de *cookies*, as instruções ou diretrizes das Autoridades de Controle têm sido um pouco díspares (de fato, a nossa Agência Espanhola de Proteção de Dados teve que adaptar, em julho de 2023, o seu Guia sobre a utilização de cookies). Mas o Comitê Europeu dos Direitos Humanos o deixou claro em fevereiro de 2023, nas suas Diretrizes 03/2022 sobre padrões enganosos nas redes sociais: os internautas deverão aceitar ou rejeitar expressamente a utilização de *cookies*, os quais devem ser apresentados em local e formato de destaque. O objetivo do RGPD e das próprias Autoridades de Controle, encarregadas de o fazer cumprir e fiscalizar o seu cumprimento, não é outro senão capacitar os cidadãos. Daí a exigência

de aceitar ou rejeitar expressamente os cookies, sem que a não aceitação implique a falta de prestação do serviço solicitado.

Além disso, este critério já era evidente para o TJUE (Tribunal de Justiça da União Europeia). E o TJUE deixou isso ainda mais explícito ao condenar o tipo de ações como as descritas na pergunta. Assim, a utilização de cookies nos obriga a abrir telas que nos perguntam que tipo de cookies queremos que sejam instalados em nosso dispositivo. Mas em nenhum caso e em nenhuma circunstância será permitido, e isso consta na condenação do TJUE, ter que aceitar cookies para que um determinado serviço nos seja prestado. Isto tem-se repetido desde o conhecido caso Planet49 (caso C-673/17), de outubro de 2019.

Eder Monica; Hilbert Reis: Professora, sobre IA: para finalizar, quais medidas devem ser adotadas pelo Estado para proteger os direitos fundamentais e a privacidade das pessoas, especialmente no que diz respeito à IA?

Mónica Ramiro: Tanto o setor público como o privado — especialmente desde a declaração global de pandemia de coronavírus em 2020 — aceleraram o seu processo de transformação digital e desencadearam o surgimento, desenvolvimento e evolução de todo um conjunto de tecnologias disruptivas que trouxeram vantagens, mas também causaram novas ameaças aos direitos e liberdades das pessoas. Estamos perante um conjunto de desafios aos quais devemos responder a partir do mundo do Direito.

Da mesma forma, não podemos perder de vista que o que está em jogo são direitos, e isso é essencial para focar nosso objetivo e legislar num sentido correto, pois o que protegemos são pessoas e não outros interesses geopolíticos, sociais ou econômicos. Isto implica adotar uma visão "antropocêntrica" e "antropogênica", onde "a dignidade pessoal é a força motriz das obrigações legais", e onde todos os atores envolvidos na transformação estejam sujeitos às mesmas regras de forma proativa, transparente e auditável e com uma série de valores éticos.

Além de normas claras e precisas — e éticas — e do estrito cumprimento do teste de proporcionalidade, antes da implementação de qualquer nova invenção, é necessária uma avaliação do impacto na vida dos sujeitos, considerando valores éticos e não discriminatórios. Os esforços europeus são direcionados nesta linha e não apenas o Regulamento sobre

Inteligência Artificial recentemente aprovado, mas também com as conhecidas "Diretrizes éticas para uma IA confiável", do Grupo de Peritos de Alto Nível da UE para IA, publicadas já em abril 2019, e que se centram em três componentes: a Inteligência Artificial deve ser lícita, ética e robusta do ponto de vista técnico e social. Estas orientações orbitam em torno da transparência com as exigências de facilitar a rastreabilidade e auditabilidade dos sistemas de Inteligência Artificial, ou a promoção, formação e educação, a fim de aprender sobre como estabelecer uma Inteligência Artificial confiável. Estou convencida de que tudo isto pode ser transferido para qualquer novo desenvolvimento ou avanço tecnológico.

Eder Monica; Hilbert Reis: Por fim, gostaríamos de encerrar a entrevista falando um pouco sobre a importância da troca de conhecimento entre pesquisadores do Brasil e da Espanha. Em 2021, a Revista Confluências, vinculada ao Programa de Pós-Graduação em Sociologia e Direito (PPGSD), organizou um dossiê intitulado "Diálogos entre a União Europeia e a América Latina: desafios e perspectivas para a sociedade internacional no século XXI". Foi o resultado de um intercâmbio científico entre as Universidades Complutense de Madrid (Espanha) e a Universidade Federal Fluminense (Brasil). Seus 16 (dezesseis) artigos envolveram temas sobre trabalho; comunicação e tecnologia digital; movimentos migratórios; meio ambiente; Comércio internacional; e, direitos humanos, numa perspectiva interdisciplinar entre sociologia e direito. Neste dossiê tivemos a agradável oportunidade de ter um artigo da sua autoria: "*Nuevas tecnologías y objetivos para la protección de datos personales en Europa: rastreo de contactos durante la pandemia de COVID-19*".

Além disso, o PPGSD organizou, em conjunto com a Universidade Complutense de Madrid, em 2021, o "IV Congresso Internacional sobre Globalização, Ética e Direito", no qual tivemos a sua participação como uma das coordenadoras de um grupo de trabalho. Em 2023, num acordo entre o PPGSD e a Universidade de Vigo, na Galiza, a Senhora foi a oradora inaugural do Congresso. O que pensa das nossas alianças interinstitucionais e dos diálogos acadêmicos internacionais que temos produzido entre Brasil e Espanha? Que impacto isso tem no debate sobre uma sociedade digital globalizada? Como a universidade pode colaborar neste processo de estabelecimento de uma sociedade efetivamente democrática e plural do século XXI?

Mónica Ramiro: O Brasil é um Estado líder no reconhecimento dos direitos da Internet e dos direitos digitais. Na verdade, foi um dos primeiros Estados do mundo a ter uma "Constituição da Internet". Temos muito que aprender com isso. Mas a Espanha também tem muito a oferecer. Temos grandes especialistas em proteção de dados pessoais e tecnologia e somos também um dos primeiros Estados do mundo a reconhecer, de forma vinculativa, a existência, na Lei Orgânica 3/2018, de direitos digitais (também reconhecidos, embora sem efeito vinculativo, na Carta dos Direitos Digitais aprovada pelo Governo em julho de 2021).

As sinergias entre Brasil e Espanha são muitas e a tecnologia é imparável; por isso, há um longo caminho a percorrer e é melhor fazê-lo em boa companhia.

Não podemos falar de uma sociedade digital globalizada se não fizermos um estudo comparativo, se não olharmos à nossa volta e aprendermos com o que se faz em outros Estados. A Europa deve olhar para os Estados Unidos, para a América Latina e até, embora possa parecer curioso em razão dos sistemas de respeito de direitos fundamentais serem questionáveis, para a China. A regulamentação da tecnologia deve ter um caráter universal e internacional. Daí a importância do Tratado Internacional sobre IA aprovado pelo Conselho da Europa em junho de 2024.

E é neste processo de aprendizagem e disseminação de ideias e conhecimentos onde as Universidades são um elemento central. As universidades sempre foram fonte de geração e transmissão de conhecimento. O nosso futuro dependerá da formação das pessoas que hoje frequentam as nossas Universidades. Os estudantes devem ser formados e capacitados para um mundo digital; entretanto, não devemos apenas torná-los alfabetizados digitalmente, mas também dotá-los dos valores éticos necessários para criar sociedades mais igualitárias e justas. É obrigação de todos nós que fazemos parte de Universidades, públicas ou privadas, contribuir para a formação dos nossos alunos, transmitindo-lhes valores e conhecimentos para saírem preparados para a sociedade da qual farão parte e em que poderão ocupar posições de tomada de decisão, que afetarão a vida de muitas outras pessoas. Se dizíamos que informação é poder, muito mais é a educação.

Os professores têm a sorte de poder fazer parte do processo formativo do nosso futuro, sendo fundamental que nos formemos e tenhamos consciência do que significa o processo de

transformação digital e da necessidade de transmitir não só conhecimentos, mas também valores. Só assim garantiremos um futuro mais justo para todos.

Referências

Agência Espanhola de Proteção de Dados; Autoridade Catalã de Proteção de Dados; Autoridade Basca de Proteção de dados; Conselho de Transparência e Proteção de Dados da Andaluzia. **Tecnologias de rastreamento de Wi-Fi**: Orientações para controladores de dados. Maio de 2024. Disponível em: https://www.avpd.euskadi.eus/contenidos/informacion/publicaciones_avpd/es_def/adjuntos/guia_wifi_tracking-es.pdf. Acesso em: 08/05/2024.

ARENAS RAMIRO, Mónica. Brecha digital de género: la mujer y las nuevas tecnologías. **Anuario de la Facultad de Derecho**, v. 4, 2011, p. 97-125.

_____. El consentimiento en las redes sociales on line. **Derecho y redes sociales, Civitas**, 2010, p. 117-44.

_____. Nuevas Tecnologías y retos para la protección de datos personales en Europa: El rastreo de contactos durante la pandemia por covid-19. **Confluências - Revista Interdisciplinar de Sociologia e Direito**, v. 23, n. 2, p. 99-17. Disponível em: https://doi.org/10.22409/conflu.v23i2.50519. Acesso em: 07/05/2024.

_____. Pasaporte COVID, ¿libertad de circulación de forma segura o discriminación y privacidad en juego? **La Ley privacidad**, v. 8, 2021.

_____. Transparencia y partidos políticos: Las insuficiencias de la Ley 19/2013. Estudios sobre la función y el estatuto constitucional de los partidos políticos. **Marcial Pons**, 2022, pp. 361-89.

CNN Brasil. **FirstMile**: como funciona ou o software espião que vinha sendo utilizado pela Abin de Ramagem. 25 de janeiro de 2024. Disponível em: https://www.cnnbrasil.com.br/politica/firstmile-como-funciona-o-software-espiao-que-teria-sido-usado-pela-abin-de-ramagem/. Acesso em: 07/05/2024.

MENÉNDEZ, María. Espionaje Pegasus. El Gobierno denuncia que Sánchez y Robles fueron espiados por Pegasus: "Son escuchas ilícitas y externas". **RTVE**, 2 de maio de 2022. Disponível em: https://www.rtve.es/noticias/20220502/gobierno-anuncia-sanchez-robles-espiados-pegasus/2345960.shtml. Acesso em: 07/05/2024.

★