SYRI: UM MARCO NA PROTEÇÃO DOS DIREITOS HUMANOS NA ERA DA INTELIGÊNCIA ARTIFICIAL

SYRI: A MILESTONE IN THE PROTECTION OF HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE

Camila Henning Salmoria[1]

Larissa Pinho de Alencar Lima[2]

RESUMO

Em 2020, o uso do SyRI foi proibido pelo tribunal holandês, marcando um dos primeiros casos de interrupção de um sistema de inteligência artificial para preservar os direitos humanos. Este artigo propõe analisar o referido caso, identificando as violações dos direitos humanos durante seu uso, contextualizando tais transgressões à luz da legislação e da jurisprudência brasileira. Através de uma abordagem metodológica dedutiva, empregando pesquisa indireta embasada em revisão bibliográfica e documental, o estudo analisa o sistema de tecnologia e, subsequentemente, o veredicto da corte. São identificados os direitos humanos violados, seguido por uma análise da proteção desses mesmos direitos no contexto brasileiro. Como conclusão, verifica-se que o Brasil dispõe de uma legislação e jurisprudência em consonância com as normas europeias.

Palavras-chave: Algoritmo; Privacidade; Poder Judiciário; Proteção de Dados; Vieses.

ABSTRACT

In 2020, the use of SyRI was banned by the Dutch court, marking one of the first cases of disruption of an artificial intelligence system to preserve human rights. This article proposes to analyze the aforementioned case, identifying human rights violations during its use, contextualizing such transgressions in light of Brazilian legislation and jurisprudence. Through a deductive methodological approach, employing indirect research based on bibliographic and documentary review, the study analyzes the technology system and, subsequently, the court's verdict. Violated human rights are

[1] Juíza do Tribunal de Justiça do Paraná, desde 2004. Titular na 5 Turma Recursal. Pós-graduanda em Direito Digital na ENFAM (Escola Nacional de Formação e Aperfeiçoamento de Magistrados). Graduada em Direito pela UFPR (2003). Graduanda em Inteligência Artificial na Universidade Positivo. Lattes: http://lattes.cnpq.br/7247288385539782. ORCID: https://orcid.org/0009-0005-8061-214X.

[2] Doutora em Ciências Políticas pela Universidade Federal do Rio Grande do Sul - UFRGS. Mestre em Educação e Políticas Públicas pela Universidade Federal de Rondônia. Juíza de Direito do Tribunal de Justiça de Rondônia. Professora e coordenadora de cursos de pós-graduação, o palestrante e pesquisadora na área de Direito Digital. Autora e coordenadora de mais de 40 (quarenta) obras, entre eles livros, artigos científicos, jurídicos, pesquisas técnicas. http://lattes.cnpq.br/4670174572952874.

identified, followed by an analysis of the protection of these same rights in the Brazilian context. In conclusion, it appears that Brazil has legislation and jurisprudence in line with European standards.

Keywords: Algorithm; Privacy; Judicial Power; Data Protection; Biases.

1 INTRODUÇÃO

O avanço tecnológico tem impulsionado a rápida adoção de modelos de inteligência artificial (IA) em diversos setores da sociedade. No entanto, como é comum em qualquer inovação tecnológica de grande impacto, a ascensão da IA traz consigo um conjunto de questões cruciais que orbitam em torno da ética, dos direitos humanos e da proteção de dados.

É nessa interseção entre a tecnologia e os direitos humanos que este artigo concentra sua atenção, explorando o caso emblemático do SyRI (Sistema de Indicação de Riscos de Informações). O SyRI, um sistema de IA originalmente desenvolvido na Holanda com o propósito de detectar fraudes e irregularidades em benefícios sociais, foi considerado ilegal por sua violação dos direitos humanos, especialmente no que se refere à proteção dos dados dos cidadãos.

O objetivo deste estudo é analisar o caso, aprofundando-se na compreensão do funcionamento do SyRI e identificando quais direitos humanos foram desrespeitados durante sua utilização. A pesquisa investigará as complexidades associadas à coleta e ao uso de conjuntos de dados, que podem inadvertidamente perpetuar desigualdades e preconceitos.

Além disso, o artigo contextualizará essas violações à luz da legislação e jurisprudência brasileira, uma vez que o Brasil também enfrenta desafios significativos no que se refere à proteção de dados em meio à era da Big Data. O propósito final é contribuir para enriquecer o debate em torno do delicado equilíbrio entre o uso de sistemas de IA e a preservação dos direitos fundamentais dos indivíduos em uma sociedade cada vez mais impulsionada pela tecnologia.

2 O SISTEMA

SyRI, "*SysteemRisicoIndicatie*" (Appelman; Fathaigh; Van Hoboken,2021), era um sistema de análise de risco do governo holandês implementado em 2014 e que permaneceu em uso até 2020, quando foi proibido por ordem judicial. O processo tornou-se histórico, pois foi um dos primeiros casos que um sistema de tecnologia teve seu uso interrompido para salvaguardar direitos humanos (Van Bekkum; Borgesius, 2021)

O SyRI consistia em um algoritmo para detectar fraudes do sistema da seguridade social e prever riscos do uso ilícito de fundos e benefícios governamentais, no sistema tributário e trabalhista. Desde sua criação, o algoritmo e toda sua estrutura não tiveram informações públicas. A legislação e os regulamentos para sua implementação não deixavam claro como o sistema operava (Hague, 2020).

Apenas durante o curso do processo judicial foi possível obter um entendimento mais claro sobre a arquitetura do sistema SyRI. No entanto, nunca ficou claro se era um algoritmo supervisionado ou não, se utilizava aprendizado profundo ou como realizava a mineração de dados (Appelman; Fathaigh; Van Hoboken, 2021). O sistema possuía um ciclo complexo, envolvendo várias etapas, que começavam com a coleta de dados, anonimização, análise, comparação de riscos e, posteriormente, desanonimização. Os dados eram coletados de mais de 17 fontes estatais distintas, abrangendo informações relacionadas a emprego, multas, impostos, propriedades, moradia, educação, saúde, entre outros. Uma vez reunidos, os dados eram anonimizados pelo *Information Bureau* (Van Bekkum; Borgesius, 2021). A análise dos dados pelo algoritmo era terceirizada, com uma fundação privada conhecida como "*The Intelligence Agency*" sendo responsável por conduzir esse serviço em nome do governo.

A fundação, fazendo uso do algoritmo processava e analisava os dados, produzia um arquivo que identificava casos suspeitos. Somente após a conclusão dessa comparação e a identificação da lista de casos que se destacam como sendo de risco elevado, é que o processo de desanonimização era iniciado (Van Bekkum; Borgesius, 2021). Nessa etapa, o Ministério, responsável pelo sistema SyRI, notificava as autoridades competentes apresentando a lista de casos identificados (Hague, 2020).

Os relatórios de risco permaneciam ativos em um cadastro por dois anos. As pessoas nela incluídas não eram notificadas, embora pudessem ter acesso a suas informações se fizessem um pedido específico (vanVeen, 2019). O sistema era operado na sequência com supervisão humana, assim, a identificação de risco não gerava consequências legais diretas e automáticas como a revogação de um benefício ou a imposição de uma multa.

O legislador holandês definiu alguns modelos de risco dos quais a doutrina (Bekkum, 2021) colaciona algumas hipóteses. Por exemplo, considerava-se suspeito se duas pessoas compartilhassem o mesmo domicílio, mas reportassem endereços diferentes às autoridades, sugerindo a possibilidade de reivindicações excessivas de benefícios sociais, uma vez que, na Holanda, um casal que vive separadamente pode receber mais benefícios. Além disso, um aumento significativo no saldo de uma conta bancária em um curto período de tempo levantaria suspeitas de ocultação de ativos. Da mesma forma, a posse de várias garagens e veículos era vista como um indicativo de ativos ocultos.

Para além poucos exemplos, o governo holandês negava-se a dar maiores informações sobre o sistema, temendo que assim os fraudadores buscassem burlar o sistema (vanVeen, 2019), adaptando seu comportamento caso o modelo de risco fosse divulgado (Algorithm, 2020). A decisão de manter o algoritmo e o modelo de risco sigilosos, sem dados públicos, comprometia sua transparência, pois dificultava avaliações externas sobre as operações do sistema, assim como a análise de sua eficácia em cumprir seus objetivos.

3 O JULGAMENTO

Em 2018, logo após a entrada em vigor do Regulamento Geral sobre a Proteção de Dados -RGPD- (União Europeia, 2016), um pequeno grupo de pessoas ingressou com uma ação perante a justiça holandesa alegando que tinham seus direitos fundamentais violados pelo uso do sistema SyRI. Nos meses subsequentes, o caso ganhou relevância como ingresso de novas partes no processo, além de organizações não governamentais locais, o Relator da ONU sobre pobreza extrema e direitos humanos, ingressou na

qualidade de *amicuscuriae* (vanVeen, 2019). A audiência de julgamento foi realizada em 29 de outubro de 2019, no Tribunal Distrital de Haia, e a sentença foi proferida em fevereiro de 2020.

No curso do processo se comprovou que o SyRI era utilizado para detectar fraudes e irregularidades, focando em bairros pobres, de quatro cidades (vanVeen, 2019), entre elas Roterdã, a qual detém a mais alta taxa de pobreza do país (Toh, 2019). Durante o julgamento, o advogado do governo admitiu que os bairros foram escolhidos por terem o maior número de pessoas recebendo benefícios sociais, embora não houvesse qualquer prova de que naqueles locais houvesse um maior número de fraudes, demonstrando, assim, um envieasamento baseado no contexto socioeconômico (Hussain, 2020) e migratório, focando em turcos e marroquinos (Heikkila, 2022).

O tribunal proibiu o uso do SyRI, por considerar que ele violava o parágrafo 2º do artigo 8º da Convenção Europeia dos Direitos Humanos, não tendo passado pelo teste do justo equilíbrio. A limitação dos direitos e liberdades poderia ocorrer caso houvesse um risco aos interesses da segurança nacional, segurança pública, prevenção da desordem ou crime. O direito à privacidade, a proteção de dados, a um julgamento justo, com transparência, foram alguns dos tópicos analisados. Concluindo, o Tribunal de Haia que no caso do SyRI, a violação a direitos e liberdades ocorreu em um grau superior ao interesse que visava salvaguardar, qual seja a prevenção de fraudes (Hague, 2020).

Com relação a privacidade de dados, reconheceu o tribunal que os dados não devem circular livremente e que cada cidadão deve ser capaz de acessar facilmente quem acessou seus dados e por qual motivo esse foram usados (Hague, 2020).

O tribunal entendeu que o problema não estava em um algoritmo buscar detectar fraudes, mas sim no formato opaco que esse possuía. Para além da violação ao direito de privacidade, a falta de transparência quanto a estrutura e funcionamento do sistema, que não explicita o modelo de risco e seus indicadores nem para o público, nem para os titulares dos dados comprometa o direito a um julgamento justo. O fato dos cidadãos não serem notificados sobre sua inclusão no cadastro de risco, impedia que esses se defendem-se, afetando o direito a um julgamento justo, ocorrendo uma assimetria de informações (Algorithm, 2020).

A falta de transparência expôs também preocupações éticas e legais sobre privacidade, vigilância e uso indevido de dados do sistema, bem como seu potencial para aumentar o risco de enviesamento em seu uso. Como de fato ocorreu no uso do SyRI, que foi direcionado apenas a bairros podres, migrantes e minorias étnicas (Appelman; Fathaigh; Van Hoboken, 2021), focando sobretudo nos turcos e marroquinos (Heikkila, 2022). Sem dados públicos o sistema não podia ser auditado e fiscalizado por terceiros.

Mais dois critérios essenciais para garantir a proteção completa de dados em uma sociedade democrática também foram examinados. Primeiro, a limitação de finalidade, que estipula que os dados pessoais devem ser coletados apenas para propósitos específicos, explícitos e legítimos, não podendo ser processados de maneira contrária a esses propósitos. Segundo, a minimização de dados, que requer que os dados sejam adequados, relevantes e restritos ao mínimo necessário para alcançar o objetivo pretendido (Van Bekkum; Borgesius, 2021).

O julgamento ensejou ainda críticas sobre a digitalização governamental atingir sobretudo os grupos mais pobres e marginalizados da sociedade. Com estudiosos ressaltando que o desenvolvimento tecnológico governamental tem se pautado em um pensamento neoliberal de eficiência, buscando apenas reduzir gastos com assistência social, sem uma efetiva preocupação no investimento e melhoria da qualidade de vida da população (van Veen, 2020).

4 OS DIREITOS HUMANOS

Neste capítulo, será abordado os fundamentos pelos quais o sistema SyRI foi considerado violador dos direitos humanos. O debate jurídico e social entrelaça diversas áreas do direito, incluindo a proteção de dados pessoais, o direito à privacidade e o devido processo legal. Essa análise do SyRI não apenas ilustra os desafios inerentes à governança de dados na era digital, mas também reflete a crescente conscientização global sobre a importância da proteção de dados, um tema que transcende fronteiras e influencia legislações e práticas em todo o mundo, incluindo o Brasil.

4.1 A PROTEÇÃO DE DADOS

O principal direito humano que se reputou como violado pelo sistema SyRI foi o direito à proteção de dados, que tem sua origem tanto no sistema universal de proteção da ONU, quanto o âmbito do Direito europeu[3]. Embora seja fortemente relacionado com o direito à privacidade, o direito à proteção de dados é autônomo e foi expressamente reconhecido pelo artigo 8º da Carta de Direitos Fundamentais da União Europeia de 2000, que passou a ser vinculante para os Estados membros da União Europeia após a entrada em vigor do Tratado de Lisboa em 2009 (Sarlet, 2020).

O artigo 8 da Carta de Direitos Fundamentais da União Europeia estabelece que:

> 1. Todas as pessoas têm direito à proteção dos dados pessoais que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de acessar os dados coligidos que lhes digam respeito e de obter a respetiva retificação. (Parlamento, 2000)

Em 2016, a Europa amplia a proteção de dados com a aprovação do Regulamento Geral de Proteção de Dados (RGPD) (União Europeia. Regulation (EU) 2016/679). O RGPD estabelece regras rigorosas para o processamento de dados pessoais sensíveis, com o objetivo de preservar os direitos e liberdades individuais do cidadão no que diz respeito aos seus dados. Possui aplicação para todas as organizações que processam dados pessoais de residentes na União Europeia, independentemente de sua localização, o que significa que empresas em todo o mundo podem estar sujeitas a ele. Seu escopo é equilibrar a proteção de dados com outros direitos fundamentais, como a liberdade de expressão, reconhecendo que o direito à privacidade deve ser ponderado em relação a outros interesses legítimos, como a segurança pública e a liberdade de informação

[3] A Comissão da ONU para Direitos Humanos desempenhou um papel crucial ao interpretar o artigo 17 do Pacto Internacional de Direitos Civis e Políticos, assim como a jurisprudência da Corte Europeia de Direitos Humanos (CEDH) e do Tribunal de Justiça da União Europeia (TJUE) contribuíram para esse desenvolvimento. No entanto, somente com a Convenção nº 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais em 1981 e, quase vinte anos depois, com o artigo 8º da Carta de Direitos Fundamentais da União Europeia em 2000.

(Rachovitsa; Johann, 2022). O RGPD é fundamentado em diversos princípios, entre eles o da finalidade e da minimização de dados que ganharam relevo com o julgamento do caso SyRI.

4.1.1 Princípio da finalidade

O RGPD incorpora princípios fundamentais destinados a fortalecer a segurança e a confiança dos titulares de dados, ao mesmo tempo em que estabelece restrições claras quanto às finalidades específicas para as quais o tratamento de dados pessoais deve ser direcionado (Morais, 2023).

Um dos princípios mais notáveis é o da limitação da finalidade, que determina que os dados devem ser coletados com propósitos precisos, explícitos e legítimos, proibindo seu subsequente processamento de forma incompatível com essas finalidades (art. 5).

O RGPD também destaca a importância do consentimento do titular dos dados (art. 6), que deve ser obtido de maneira voluntária, informada e inequívoca, conferindo ao titular o direito de revogar seu consentimento a qualquer momento. Essa abordagem rigorosa do princípio da finalidade no RGPD visa proteger os direitos individuais e garantir que informações pessoais sejam usadas de maneira adequada e legal (Van Bekkum; Borgesius, 2021).

No contexto do sistema SyRI, surgiu uma controvérsia significativa devido ao fato de o sistema coletar e analisar dados de várias fontes governamentais, como registros fiscais, de habitação e de assistência social, com o objetivo de identificar possíveis fraudes em benefícios sociais.

O problema essencial estava relacionado ao fato de o sistema SyRI processar uma quantidade substancial de dados pessoais sem consentimento do titular e sem uma finalidade clara e específica, o que representava uma violação direta do princípio da finalidade (Appelman; Fathaigh; Van Hoboken, 2021).

No julgamento o tribunal concluiu que a coleta indiscriminada de dados, com compartilhamento entre diversas entidades governamentais sem consentimento expresso do titular e a falta de uma finalidade clara violavam os princípios fundamentais da

proteção de dados, na sua perspectiva finalística. O sistema SyRI foi proibido e teve seu uso descontinuado pelo governo holandês, o qual não recorreu da decisão.

4.1.2 Princípio da minimização de dados

O princípio da minimização de dados desempenha um papel crucial na proteção de dados pessoais, garantindo que apenas as informações estritamente necessárias sejam coletadas e processadas para a finalidade pretendida (Appelman; Fathaigh; Van Hoboken, 2021). Assegura que os dados sejam adequados, pertinentes e limitados ao mínimo necessário em relação às finalidades para as quais são processados (art. 5º do RGPD).

No caso do sistema SyRI, o problema crucial residia na maneira como ele coletava e analisava os dados. O sistema processava uma ampla variedade de informações pessoais de várias fontes governamentais, em larga escala, sem se concentrar apenas nos casos suspeitos. Isso resultou em uma coleta indiscriminada de dados de cidadãos, inclusive daqueles que não eram alvos de investigações por fraude. A coleta excessiva de dados, desprovida de uma finalidade específica e apropriada, claramente violava o princípio da minimização (Van Bekkum; Borgesius, 2021). Os dados coletados, no caso holandês, excediam o estritamente necessário para identificar fraudes em benefícios sociais, e, como resultado, representavam uma intrusão demasiada na privacidade dos cidadãos.

4.1.3 Devido processo legal

O devido processo legal é uma garantia fundamental que assegura que os indivíduos tenham procedimentos justos e equitativos, incluindo o direito de serem informados e de contestar decisões que possam afetá-los, especialmente em contextos nos quais sistemas de inteligência artificial (IA) são utilizados para a tomada de decisões automatizadas (Appelman; Fathaigh; Van Hoboken, 2021).

Para assegurar o devido processo legal em casos envolvendo coleta e processamento de dados por sistemas de IA, é essencial garantir transparência e informação adequada aos cidadãos. Isso significa que os indivíduos têm o direito de serem

informados sobre como seus dados serão usados, com que finalidades e quais medidas estão em vigor para proteger sua privacidade e direitos fundamentais. A falta de transparência e clareza nesse processo resulta em uma assimetria de informações, onde os cidadãos não têm conhecimento completo sobre como seus dados estão sendo tratados, o que compromete sua capacidade de tomar decisões informadas sobre o compartilhamento de suas informações pessoais.

No caso específico do sistema SyRI, ele descumpriu a garantia do devido processo legal com a falta de transparência em sua operação e a ausência de notificação aos cidadãos sobre sua inclusão no cadastro de risco, os quais sem notificação, não podiam contestar o uso e as conclusões do sistema e, assim, tiveram prejudicados sua capacidade de buscar um julgamento justo em relação ao sistema SyRI (Van Bekkum; Borgesius, 2021).

4.2 A Proteção de dados no Brasil

A proteção de dados no Brasil se positivou com a implementação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709 de 14 de agosto de 2018 (BRASIL, 2018), mas que entrou em vigor apenas em setembro de 2020, com forte inspiração na RGPD.

A LGPD estabelece diretrizes e requisitos semelhantes a RGPD assegurando a necessidade de consentimento explícito para o processamento de dados, a transparência nas práticas de tratamento, a finalidade específica para a coleta de dados e a minimização dos dados coletados, de acordo com o que é estritamente necessário para a finalidade pretendida.

O julgamento do STF, em 2020, na Ação Direta de Inconstitucionalidade (ADIn) 6387 (Brasil, 2020a) desempenhou um papel fundamental no reconhecimento da importância da proteção de dados no Brasil. Ao suspender a eficácia da Medida Provisória (MP) nº 954/2020(Brasil, 2020b), que exigia o compartilhamento de dados pessoais com o IBGE sem o consentimento dos titulares, o STF reforçou a necessidade de proteção da privacidade e dos direitos dos cidadãos em relação às suas informações pessoais.

A decisão da ADIn 6387(Brasil, 2020a) fundou-se também no reconhecimento da proteção dos direitos humanos frente ao pedido de compartilhamento de dados pessoais ressalvando, sobretudo, a proteção de dados e devido processo legal. Reconheceu-se que o tratamento de informações pessoais deve respeitar os limites estabelecidos pelas cláusulas constitucionais que garantem a liberdade individual e a privacidade, enfatizando a necessidade de limitar e minimizar dados no tratamento de informações pessoais.

A MP nº 954/2020(Brasil, 2020b), ao não definir apropriadamente como e para que seriam utilizados os dados coletados, desatendeu à garantia do devido processo legal, tanto na dimensão substantiva quanto na procedimental. Isso porque não ofereceu condições de avaliação quanto à adequação e necessidade do tratamento dos dados, assim como não apresentou mecanismos técnicos ou administrativos adequados para proteger a segurança e o sigilo dos dados pessoais compartilhados.

O julgamento pelo STF da ADIn 6387(Brasil, 2020a) reconheceu a importância da proteção de dados pessoais, com base nos princípios da limitação e minimização desses dados, bem como do devido processo legal, de maneira semelhante ao que foi reconhecido no caso do sistema SyRI. Este episódio ilustra a crescente conscientização sobre a proteção de dados no Brasil, alinhando-se com os princípios da LGPD e com padrões internacionais de privacidade, como os da União Europeia.

5 CONSIDERAÇÕES FINAIS

O caso do sistema SyRI lançou luz sobre os complexos desafios éticos e legais que surgem quando a tecnologia é empregada na análise de dados em um ambiente caracterizado pela opacidade. A ausência de transparência acerca do funcionamento do algoritmo e dos processos operacionais mina a confiança nas decisões geradas pelo sistema, levantando sérias preocupações em relação à privacidade e aos direitos individuais. Diante dessas inquietações, é essencial buscar um equilíbrio entre a necessidade legítima de combater fraudes e atividades ilícitas e a preservação dos direitos e liberdades dos cidadãos.

No contexto atual, muitos acadêmicos debatem as ameaças à privacidade de grupos, reconhecendo que a noção individualista de privacidade, assegurada pelos regimes de proteção de dados existentes, não é adequada para abordar os desafios impostos pela análise sofisticada de dados, incluindo a realização de inferências e previsões em grande escala. Esses desafios não apenas evidenciam as limitações do direito substantivo dos direitos humanos, como também levantam questões cruciais relacionadas à admissibilidade de reivindicações de violações dos direitos dos grupos, evidência e ônus da prova necessários para fundamentar tais alegações.

O julgamento do STF na ADIn 6387 representa um marco importante na conscientização e no reconhecimento da proteção de dados pessoais no Brasil. A decisão, baseada nos princípios da limitação e minimização de dados, bem como do devido processo legal, assemelha-se ao que já foi reconhecido em situações semelhantes, como no caso do sistema SyRI. Essa tendência reflete uma mudança significativa na sociedade brasileira, onde a proteção da privacidade e dos dados pessoais está se tornando cada vez mais valorizada e alinhada com as diretrizes da LGPD e com os padrões internacionais de privacidade, notadamente os da União Europeia.

Em uma sociedade digital em constante transformação, o Poder Judiciário desempenha um papel crucial, não apenas na definição, mas também na aplicação das normas de privacidade. À medida que a sociedade avança em direção a um ambiente digital cada vez mais complexo e interconectado, o Poder Judiciário será mais cobrado a salvaguardar proteção de dados e garantir que os direitos dos cidadãos sejam preservados.

REFERÊNCIAS

ALGORITHM WATCH. SYRI: **A digital welfarestate experiment.** 2020 Disponível em: https://algorithmwatch.org/en/syri-netherlands-algorithm/. Acesso em: 31 ago. 2023.

APPELMAN, Naomi; FATHAIGH, Ronan O.; VAN HOBOKEN, Joris. **Social Welfare, Risk Profiling and Fundamental Rights:** The Case of SyRI in theNetherlands. J. Intell. Prop. Info. Tech. &Elec. Com. L., v. 12, p. 257, 2021.

BEKKER, S. Digital Welfare **States:** Boundaries and Opportunities. Social Europe. Disponível em: https://www.socialeurope.eu/digital-welfare-states-boundaries-and-opportunities. Acesso em: 31 ago. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.**Dispõesobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6387** Medida Cautelar-Referendo. Relatora Ministra Rosa Weber. Tribunal Pleno. Julgado em 07/05/2020. Diário da Justiça Eletrônico, nº 270, Divulgação em 11-11-2020, Publicação em 12-11-2020a. Processo Eletrônico.

BRASIL. **Medida Provisória nº 954/2020.**Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística. Diário Oficial da União, Brasília, DF, 17 abr. 2020b.

EKKER LEGAL. **SyRI**. 02 de fevereiro de 2020. Disponível em: https://ekker.legal/en/2020/02/02/syri/. Acesso em: 31 ago. 2023.

HOLANDA. HAGUE DISTRICT COURT. Tribunal Distrital de Haia. Número do processo C-09-550982-HA ZA 18-388. Sentença foi proferida pelo Sr. MC Ritsema van Eck-van Drempt, Sr. JS Honée e Sr. HJ van Harten e pronunciada em audiência pública em 5 de fevereiro de 2020. Disponível em: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878. Acesso em: 31 ago. 2023.

HEIKKILÃ, Melissa. **DutchScandal Serves as a Warning for EuropeoverRisks of UsingAlgorithms. 29 de março de 2022.** Político. Disponível em: https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/. Acesso em: 31 ago 2023.

HUSSAIN, H. **Human Rights Pulse. Dutch Court Finds SYRI Algorithm Violates Human Rights Norms in Landmark Case**. Human Rights Pulse. 22 março de 2020. Disponível em: https://www.humanrightspulse.com/mastercontentblog/dutch-court-finds-syri-algorithm-violates-human-rights-norms-in-landmark-case. Acesso em: 31 ago. 2023.

LEITÃO, Rômulo Guilherme; BELCHIOR, Wilson Sales. Diretrizes Regulatórias para sistemas de inteligência artificial: análise documental das iniciativas dos Estados Unidos e União Europeia. **Revista Eletrônica Direito e Sociedade-REDES**, v. 10, n. 3, p. 187-204, 2022.

MORAIS JÚNIOR, Ricardo Maia de. **Accountability e Direito Fundamental à proteção de dados pessoais enquanto limites ao uso da Inteligência Artificial na relação de emprego**, 2023. Disponível em: https://www.academia.edu/108390065/Accountability_e_Direito_Fundamental_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais_enquanto_limites_ao_uso_da_Inteligência_Artificial_na_rela%C3%A7%C3%A3o_de_emprego. Acesso em: 31. ago. 2023.

PARLAMENTO EUROPEU. Carta dos Direitos Fundamentais da União Europeia. 18 de dezembro de 2000. **Jornal Oficial das Comunidades Europeias**. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 31 ago. 2023.

RACHOVITSA, Adamantia; JOHANN, Niclas. The human right simplications of the use of AI in the digital welfarestate: LessonslearnedfromtheDutchSyRI case. **Human Rights Law Review**, v. 22, n. 2, p. ngac010, 2022.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. **Revista Direito Público**, Brasília, Volume 17, n. 93, 33-57, maio/jun. 2020.

SIMONITE, T. **EuropeLimitsGovernment Use of AI. Wired.** Disponível em: https://www.wired.com/story/europe-limits-government-algorithm-us-not-much/?mbid=social_twitter&utm_brand=wired&utm_campaign=wired&utm_medium=social&utm_social-type=owned&utm_source=twitter. Acesso em: 31 ago. 2023.

TOH, Amós. **Dutch Ruling a Victory for Rights of the Poor.** 06 de fevereiro de 2020. Human Rights Watch. Disponível em: https://www.hrw.org/news/2020/02/06/dutch-ruling-victory-rights-poor. Acesso em: 31 ago. 2023.

TOH, Amós. **Welfare Surveillanceon Trial in the Netherlands.** Can EuropeMakeIt?.08 de novembro de 2019. Disponível em: https://www.opendemocracy.net/en/can-europe-make-it/welfare-surveillance-trial-netherlands/. Acesso em: 31 ago. 2023.

UNIÃO EUROPEIA. **Regulation (EU) 2016/679 (General Data Protection Regulation) do Parlamento Europeu 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, e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj . Acesso em: 31 ago. 2023.

VAN BEKKUM, Marvin; BORGESIUS, FrederikZuiderveen. **Digital welfare fraud detection and theDutch SyRI judgment.** EuropeanJournal of Social Security, v. 23, n. 4, p. 323-340, 2021.

VAN VEEN, Christiaan. **Landmark Judgment from the Netherlandson Digital Welfare Statesand Human Rights.** 19 de março de 2020. Open Global Rights. Disponível em: https://www.openglobalrights.org/landmark-judgment-from-netherlands-on-digital-welfare-states/. Acesso em: 31 ago. 2023.

VAN VEEN, Christiaan. **Profiling the Poor in the Dutch Welfare State.** 1º de novembro de 2019. NYU Center for Human Right sand Global Justice. Disponível em: https://chrgj.org/2019/11/01/profiling-the-poor-in-the-dutch-welfare-state/. Acesso em: 31 ago. 2023.