



SENADO FEDERAL
Secretaria-Geral da Mesa

ATA DA 13ª REUNIÃO DA COMISSÃO TEMPORÁRIA INTERNA SOBRE INTELIGÊNCIA ARTIFICIAL NO BRASIL DA 1ª SESSÃO LEGISLATIVA ORDINÁRIA DA 57ª LEGISLATURA, REALIZADA EM 31 DE OUTUBRO DE 2023, TERÇA-FEIRA, NO SENADO FEDERAL, ANEXO II, ALA SENADOR ALEXANDRE COSTA, PLENÁRIO Nº 7.

Às quatorze horas e quatorze minutos do dia trinta e um de outubro de dois mil e vinte e três, no Anexo II, Ala Senador Alexandre Costa, Plenário nº 7, sob a Presidência do Senador Astronauta Marcos Pontes, reúne-se a Comissão Temporária Interna sobre Inteligência Artificial no Brasil com a presença dos Senadores Carlos Viana, Veneziano Vital do Rêgo, Efraim Filho, Nelsinho Trad, Eduardo Gomes, Laércio Oliveira, Rodrigo Cunha, Izalci Lucas, Alessandro Vieira, Alan Rick, Angelo Coronel e Mecias de Jesus. Deixam de comparecer os Senadores Styvenson Valentim, Weverton, Daniella Ribeiro, Vanderlan Cardoso, Fabiano Contarato e Chico Rodrigues. Deixa de comparecer a Senadora Daniella Ribeiro, conforme Requerimento 537/2023-CDir. Havendo número regimental, declara-se aberta a reunião. A presidência submete à Comissão a dispensa da leitura e a aprovação da ata da reunião anterior, que é aprovada e será publicada no Diário do Senado Federal. Passa-se à Audiência Pública Interativa, atendendo ao Requerimento nº 4, de 2023-CTIA, de autoria Senador Eduardo Gomes (PL/TO), com a finalidade de debater os "impactos da aplicação da inteligência artificial no cibercrime e implicações da formulação de políticas para a administração do sistema de justiça criminal", as tendências atuais e o uso de sistemas e aplicativos de IA para cometer condutas criminosas e ilegais e os possíveis impactos e respostas que políticas de inteligência artificial podem ter para combatê-las, com a participação de Roberta Rodrigues Correia Pimentel, Assessora-Chefe de Proteção de Dados e Privacidade do Ministério Público Militar (MPM); Carlos José Oliveira, Administrador Principal da Direção-Geral de Comunicações, Redes, Conteúdos e Tecnologia da Comissão Europeia; Rony Vainzof, Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo (Fiesp); Tarcízio Roberto da Silva, Pesquisador de Políticas Públicas da Fundação Mozilla; e Carlos Eduardo Miguel Sobral, Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública (Senasp). O Senador Eduardo Gomes faz uso da palavra na presente reunião. O Senhor Presidente submete à Comissão a dispensa da leitura e a aprovação da ata da 11ª reunião, que é aprovada. Nada mais havendo a tratar, encerra-se a reunião às dezesseis horas e dez minutos. Após aprovação, a presente Ata será assinada pelo Senhor Presidente e publicada no Diário do Senado Federal.

Senador Astronauta Marcos Pontes
Vice-Presidente da Comissão Temporária Interna sobre Inteligência Artificial no Brasil

Esta reunião está disponível em áudio e vídeo no link abaixo:
<https://www12.senado.leg.br/multimedia/evento/117964>



SENADO FEDERAL
Secretaria-Geral da Mesa

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP. Fala da Presidência.) – Boa tarde a todos.

Declaro aberta a 13ª Reunião da Comissão Temporária Interna sobre Inteligência Artificial no Brasil, que foi criada pelo Requerimento nº 722, de 2023, com a finalidade de, no prazo de 120 dias, examinar os projetos concernentes ao relatório final aprovado pela Comissão de Juristas, responsável por subsidiar a elaboração de substitutivo sobre inteligência artificial no Brasil – ela foi criada pelo Ato do Presidente do Senado Federal nº 4, de 2022 –, bem como eventuais novos projetos que disciplinem a matéria.

Antes de iniciarmos os nossos trabalhos, proponho a dispensa da leitura e a aprovação da ata da reunião anterior.

Então, as Sras. e os Srs. Senadores que concordam permaneçam como se encontram. *(Pausa)*

A ata está aprovada e será publicada no *Diário do Senado Federal*.

Informo que esta reunião se destina à realização de audiência pública com o objetivo de debater: os impactos da aplicação da inteligência artificial nos crimes cibernéticos e implicações da formulação de políticas para a administração do sistema de Justiça criminal; as tendências atuais e o uso de sistemas e aplicativos de inteligência artificial para cometer condutas criminosas e ilegais, e os possíveis impactos e respostas que políticas de inteligência artificial podem ter para combatê-las.

Em cumprimento ao Requerimento nº 4, de 2023, da Comissão Temporária de Inteligência Artificial, de autoria do Senador Eduardo Gomes.

O público interessado em participar desta audiência pública poderá enviar suas perguntas através do Portal do Senado, www.senado.leg.br/ecidadania, ou ligar para 0800 0612211. Novamente: quem quiser participar, através de perguntas ou comentários, entre pelo Portal do Senado, www.senado.leg.br/ecidadania ou ligue para 0800 0612211.

Encontram-se presentes no plenário da Comissão:

- Sra. Roberta Rodrigues Correia Pimentel, Assessora-Chefe de Proteção de Dados Pessoais e Privacidade do Ministério Público Militar. Por favor, Dra. Roberta, queira me acompanhar aqui.

- Sr. Rony Vainzof. Depois você me ensina a falar seu nome direitinho.

O SR. RONY VAINZOF *(Fora do microfone.)* – Está perfeito.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Está certo, Vainzof? Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo (Fiesp).

Encontram-se também presentes, por meio do sistema de videoconferência:

- Sr. Carlos José Oliveira, Administrador Principal da Direção-Geral de Comunicações, Redes, Conteúdos e Tecnologia da Comissão Europeia;

- Sr. Tarcízio Roberto da Silva, Pesquisador de Políticas Públicas da Fundação Mozilla; e

- Sr. Carlos Eduardo Miguel Sobral, Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública (Senasp).

Bom, gostaríamos, nos comentários iniciais, primeiro, de agradecer a presença de todos os nossos apresentadores, debatedores, agradecer também a audiência de todos aqueles que nos acompanham através das redes do Senado e também da TV Senado e de todos aqueles que estão aqui na sala de audiências nº 7 do Senado, presencialmente, e dizer que esse tema tem uma importância muito grande.

Nós temos debatido a inteligência artificial aqui no Senado, de forma a aperfeiçoar a proposta de legislação feita por uma Comissão de Juristas em 2022. E o tema é tão amplo e tão transversal, participando nas nossas vidas atualmente – e vai participar cada vez mais – que ficou muito clara a



SENADO FEDERAL
Secretaria-Geral da Mesa

necessidade de uma Comissão Temporária específica para tratar do tema e também de trazer especialistas de vários setores para que nos deem seu ponto de vista, sua perspectiva. E a gente precisa da participação do público para que nos deem isso também, lembrando que aqui é uma Casa que representa a população do Brasil, então nós precisamos dessas participações, para que esse tema seja visto de várias perspectivas, com a participação da sociedade civil.

É um tema amplo, como eu falei, envolve aspectos de tecnologia, envolve aspectos de aplicação dessa tecnologia em vários setores, envolve implicação, ou as implicações da aplicação dessa tecnologia nesses diversos setores e, finalmente, o invólucro, vamos chamar assim, jurídico adequado para que ele não só seja efetivo, mas também protetivo. Como é que eu vou colocar isso? Nós não podemos, por exemplo, numa legislação, incluir tudo de todos os setores, lembrando que é uma ferramenta que é utilizada em todos os setores, e os setores já têm as suas regulações específicas. Por exemplo, a saúde tem a Anvisa, que cuida da regulação, da fiscalização necessária do setor de saúde; nós temos a Anatel para o setor de telecomunicações; a ANP no setor de petróleo; para a mineração tem a Agência Nacional de Mineração; e assim por diante. Nós temos as agências reguladoras, e temas como segurança cibernética e inteligência artificial são transversais, participam de todos esses setores.

Então, uma coisa com que a gente tem que tomar muito cuidado é de não haver choque entre esses diversos setores. Por exemplo, se a gente institui uma agência de inteligência artificial, ela não pode entrar em choque com a Anvisa, não pode entrar em choque com a Anatel, que já tem essas funções, ou com a Justiça, ou com as leis já existentes, como a Lei Geral de Proteção de Dados, com a agência de proteção de dados. Um cuidado muito grande que a gente tem que ter no desenvolvimento dessa legislação é que ela respeite as leis já existentes, não entre em choque, e também a estrutura desse sistema no Brasil para que haja a participação dos diversos setores e não a interferência nos diversos setores. Então, esse é um ponto em que a gente tem que tomar muito cuidado.

Hoje de manhã, nós tivemos uma audiência, aqui nesta mesma sala, sobre o tema, mas falando de jornalismo, falando de *fake news*, falando de efeito da inteligência artificial para eleições, o que também é importante. Você vê como o tema vai por muitos lados. Nós já tivemos sobre saúde, sobre educação, sobre desenvolvimento de ciência e tecnologia, e é muito importante essa participação geral.

Então, eu quero agradecer de antemão aos nossos apresentadores e debatedores aqui, aos que estão também no remoto falando conosco e também a todas as pessoas que participam e têm se interessado por esse tema, porque o tema faz parte da nossa vida.

Para dar sequência, então, deixe-me explicar como que vai ocorrer aqui com a dinâmica desta audiência pública. Eu vou passar a palavra, por dez minutos, para cada um dos debatedores na sequência que eu tenho aqui. A sequência será a seguinte: primeiro, o Sr. Carlos Oliveira; depois, o Sr. Tarcízio Roberto da Silva; depois a Sra. Roberta Rodrigues Correia Pimentel; depois o Sr. Rony Vainzof; e depois o Sr. Carlos Eduardo Miguel Sobral. Nessa sequência, então, cada um dos debatedores terá dez minutos para sua apresentação.

Aqui nesta sala, fica mais fácil para as pessoas falarem, porque, faltando um minuto, vai tocar um alarme como este daqui.

(Soa a campainha.)

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Faltando um minuto, não sou eu que toco, o sistema é automático. Faltando 15 segundos, vai aparecer uma voz feminina bastante convincente falando que faltam 15 segundos.



SENADO FEDERAL
Secretaria-Geral da Mesa

Quem está aqui vai ver o relógio, vai ouvir essa campainha e vai ouvir a voz feminina. Quem está no remoto, obviamente, não tem acesso aqui ao relógio que está na parede, não vai ouvir o toque da campainha de um minuto, mas vai ouvir o toque dos 15 segundos. Então, eu peço para quem está no remoto acompanhar, coordenar o seu tempo de dez minutos. Obviamente, esse tempo não é tão restrito assim. Termine a ideia, etc. Eu consigo aumentar aqui um minuto, dois minutos, consigo controlar isso aqui. Então, não se prenda tanto a isso aí, mas é importante, dada a quantidade de debatedores, para que a gente não fique aqui muito além.

No final, eu espero até lá, então, já ter recebido as questões que virão da população pelo e-Cidadania, e aí eu vou ler essas perguntas, distribuir para os que estão presentes, ler para os que estão distantes, no remoto, e aí a gente vai ter as considerações finais com as respostas dos debatedores para as perguntas do público também.

Então, funcionando isso aí, a gente está estimando um tempo aproximadamente de duas horas, um pouco menos de duas horas; a gente deve terminar em torno das 16h aqui, uma hora e quarenta.

O.k.. Dito tudo isso, combinados, eu passo a palavra, então, eu concedo a palavra para o nosso primeiro debatedor, primeiro apresentador, que será, então, o Sr. Carlos Oliveira, Administrador Principal da Direção-Geral de Comunicações, Redes, Conteúdos e Tecnologia da Comissão Europeia.

Carlos, é bom te ver novamente. Nós tínhamos mais contato no tempo do Ministério. É bom te ver novamente.

Por favor, você tem a palavra por dez minutos.

O SR. CARLOS JOSÉ OLIVEIRA (Para expor. *Por videoconferência.*) – Boa tarde.

Senador, permita-me começar por agradecer desde já o convite que nos foi endereçado para estar presente nesta audiência pública, e endereçado também um cumprimento especial... O Senador Marcos Pontes foi a pessoa com quem eu tive o grato privilégio de ter vários encontros muito profícuos e frutuosos no passado, durante as minhas funções enquanto Ministro Conselheiro da União Europeia e no Brasil.

É um enorme prazer saudá-lo, Senador, e peço-lhe também que em sua pessoa eu endereça uma saudação a todos os demais presentes nessa sala. Há mais nomes conhecidos. Por uma questão de tempo, eu vou pedir desculpa por passar rapidamente a minha apresentação. Mas parece-me que esse contributo possa ser útil para o debate que está a ocorrer nesta Casa.

Nós temos que ir, com especial interesse, a audiências públicas organizadas pelo Senado Federal no Brasil. E a União Europeia, tal como o Brasil, faz parte de um grupo de países e organizações internacionais que estão empenhadas numa discussão multilateral sobre o tema de inteligência artificial. Uma das instâncias em que esse tema tem vindo a ser discutido é o G20, e é para nós muito bom saber que o Brasil vai presidir, no próximo ano, esta entidade, e esperamos que possa influenciar um pouco a discussão, para que nessa... vai ter lugar.

Como provavelmente sabem, está atualmente em curso uma intensa atividade legislativa, no seio da União Europeia, que tem como objetivo a adoção do chamado regulamento sobre inteligência artificial. Em inglês, tem um nome um bocadinho mais estranho, que é o AI Act, e pode vir a ser a primeira legislação abrangente sobre inteligência artificial.

Nós vemos, uma vez mais, o Brasil e a União Europeia como dois países – vamos dizer assim – que partilham valores comuns. Isso foi particularmente patente durante o processo que culminou na Lei Geral de Proteção de Dados e esses valores contribuem para uma abordagem convergente sobre os desafios e oportunidades de ter a transformação digital que mantenha o ser humano no centro do debate.



SENADO FEDERAL
Secretaria-Geral da Mesa

Para poder plenamente realizar o potencial enorme de benefícios que encaminhem a sociedade em geral e podem obter até um aumento da inteligência artificial, é essencial que se promova, no âmbito dos nossos países, mas sobretudo na escala global, uma visão da inteligência artificial confiável e sustentável. A confiança é crucial e significa privilegiar o ponto de vista e os direitos dos cidadãos.

Esta visão centrada no ser humano vai estar como uma garantia de proteção de direitos humanos, nomeadamente em aspectos como a não discriminação, a privacidade, a proteção de dados, as particularidades pessoais e também a sustentabilidade nos eficientes recursos.

Com isso, outros domínios da transformação digital, uso de dados, está no centro das nossas discussões. O Brasil, tal como a União Europeia, reconhece o direito à proteção de dados como uma garantia constitucional e adotou um quadro legislativo avançado sobre esta matéria.

É igualmente importante estar atento aos riscos associados a alguns sistemas de inteligência artificial. Enquanto a maioria das aplicações apresentam riscos limitados e, de uma certa forma, vamos dizer que têm um potencial para contribuir para a assunção de muitos problemas com que estamos confrontados no nosso quotidiano, há alguns sistemas em que a inteligência artificial requer uma atenção especial para evitar resultados indesejáveis. Por exemplo, é muitas vezes impossível compreender o raciocínio que leva um sistema baseado em inteligência artificial a tomar uma decisão, a fazer uma previsão ou a desencadear uma ação. Opacidade ou falta de transparência de muitos algoritmos podem criar incerteza e limitar a proteção dos nossos direitos enquanto cidadãos.

Para responder a estes desafios, o regulamento sobre inteligência artificial, cujo processo legislativo está em curso, propõe um enfoque nos requisitos de responsabilidade e transparência. Com este propósito, eu gostaria de mencionar que a União Europeia instituiu a criação de um Centro Europeu para a Transparência Algorítmica, que visa precisamente investigar a forma como funcionam os algoritmos e, em especial, os processos baseados em inteligência artificial, para melhor compreender o impacto ético e social do seu uso, mas também os seus riscos e contribuir para melhorar a transparência, instituindo boas práticas e regras de funcionamento sobre esta matéria.

Mas na Justiça, em particular na administração do sistema judicial, o nível de risco associado ao uso de inteligência artificial assume especial importância. Com efeito, se bem que o uso da inteligência artificial possa apresentar um aumento de eficiência do sistema, através da autonomia e aquisição das tarefas correntes e repetitivas, a anonimização, a tradução, trata-se de processos que podem interferir com conceitos fundamentais ligados à democracia, ao Estado de direito, aos direitos individuais, como, por exemplo, o direito a um julgamento justo e a um recurso efetivo.

Tendo em consideração estes riscos e, em particular, o possível viés e a opacidade dos sistemas de inteligência artificial, a União Europeia propõe classificar o uso da inteligência artificial da administração da Justiça como o que nós chamamos de um risco elevado.

Com efeito, mesmo que existam provisões legais para proteger os direitos fundamentais, a abordagem do tipo caixa negra, que alguns sistemas de inteligência artificial apresentam, revela-se muitas vezes demasiado complexa e opaca. E isso pode traduzir-se em preconceitos e funcionamento um pouco imprevisível. É por isso que os nossos legisladores estão a atuar de forma a desenvolver regras e salvaguardas adicionais, que tragam mais transparência a estes sistemas de elevado risco e em relação às condições em que eles podem ser utilizados.

Ainda retomando esta discussão sobre o uso da inteligência artificial na administração judicial e investigação criminal, reconhecemos, uma vez mais, que são ferramentas que podem constituir um auxílio importante, mas não podem ser usadas para toda e qualquer tarefa. É por esta razão que a União Europeia não autorizará que decisões, no meio da justiça e investigação criminal, sejam exclusivamente



SENADO FEDERAL
Secretaria-Geral da Mesa

baseadas em sistemas automatizados. Para assegurar que a inteligência artificial é usada de forma responsável e proporcional, é importante que se adote uma abordagem única e genérica sobre IA, com condições específicas e salvaguardas baseadas na natureza das aplicações, nos riscos associados, para limitar o impacto nos direitos e liberdades das pessoas envolvidas.

Para dentro destas considerações associadas à concepção e desenvolvimento dos sistemas baseados em IA, é igualmente importante ter presente de que forma eles vão ser usados. Uma vez mais, recorrendo ao caso do sistema judicial, é essencial facultar a todos os atores, advogados, juízes, polícias, uma formação adequada para assegurar uma boa compreensão dessas ferramentas. É essencial que as pessoas tenham consciência dos riscos, em particular do chamado viés de automação, e sejam capazes de ter o seu espírito crítico na utilização dos sistemas e, em alguns casos, devidamente fundamentados, ter mesmo a possibilidade de decidir não os usar.

Finalmente, como qualquer legislação, as regras adotadas necessitam ser aplicadas de forma clara, firme e coerente, com a regulação da inteligência artificial tendo em consideração questões que vão desde proteção de dados, segurança de produtos e outros direitos fundamentais, direitos de consumidores, porque há várias entidades envolvidas nesta discussão. Por esta razão, os legisladores da UE refletem sobre a forma mais apropriada de assegurar uma plena aplicação da legislação, tendo em consideração o conhecimento já adquirido por organismos de regulação que atuam em áreas conexas, como é o caso da proteção de dados.

O modelo de governança da inteligência artificial tem por objetivo facultar um quadro que dê aos cidadãos, e às administrações, e às empresas confiança na sua utilização, encorajando o seu uso e investimentos no desenvolvimento destes sistemas. É por isso que gostaria de relembrar uma afirmação anterior: para que possamos realizar plenamente os benefícios para a sociedade da inteligência artificial, temos de criar um ambiente de confiança, uma utilização responsável, mitigando os riscos que estão associados. Estamos empenhados em continuar a trabalhar com parceiros internacionais, em particular com o Brasil, para atingir estes objetivos. A União Europeia mostra, uma vez mais, o seu empenho em usar esta conversa como um exemplo de cooperação e gostaríamos de continuar e promover um entendimento mais geral sobre os desafios e oportunidades de inteligência artificial.

Quero terminar renovando o meu agradecimento e o da União Europeia pelo convite para participar desta audiência e, uma vez mais, felicitar o Senado Federal por esta iniciativa, reafirmando a nossa disponibilidade para continuar este diálogo com o Brasil, sobre as questões de inteligência artificial nas suas múltiplas dimensões.

Muito obrigado. Retorno a palavra ao Sr. Senador Marcos Pontes.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado, obrigado ao Sr. Carlos Oliveira, Administrador Principal da Direção-Geral de Redes de Comunicação, Conteúdos e Tecnologias da Comissão Europeia. Parabéns pela apresentação, foi muito bom vê-lo novamente.

Eu gostaria de aproveitar esse momento para registrar a presença aqui conosco, na sala de audiências nº 7 do Senado, do Dr. Cid Silveira. Ele é Diretor de Relações Institucionais da Câmara de Comércio Brasil-Texas. Obrigado pela presença aqui conosco. Nós temos, inclusive, muitas relações importantes não só no setor de óleo e gás com a região de Houston, mas também no setor espacial, também no setor de transformação digital, no setor da educação, com a Universidade de Houston, a universidade Rice University também. Então, obrigado pela presença aqui conosco.

Neste momento, eu gostaria de passar a palavra ao Sr. Tarcízio Roberto da Silva. Ele é Pesquisador de Políticas Públicas da Fundação Mozilla.



SENADO FEDERAL
Secretaria-Geral da Mesa

Sr. Tarcízio, o senhor tem dez minutos para a apresentação. Peço que controle o tempo aí do seu lado, o.k.? Obrigado.

O SR. TARCÍZIO ROBERTO DA SILVA (Para expor. *Por videoconferência.*) – Muito obrigado. Só compartilhando aqui a tela um segundinho. Maravilha, funcionou.

Bom, primeiro eu queria só colocar o meu cronômetro aqui para respeitar o nosso tempo para o debate. Um segundo.

Eu queria agradecer a oportunidade de colaborar também no debate desta Comissão. Temos tentado dialogar sobre essa matéria já há algum tempo, inclusive na comissão anterior, que resultou no PL 2.338. Então, queria saudar toda a Comissão, especialmente, na pessoa do Dr. Senador Marcos Pontes, e inclusive, puxar um gancho aqui para dizer que é a primeira vez que estamos nos falando diretamente, mas já fomos coautores em uma coletânea do Prof. André Ramos Tavares, que foi uma coletânea justamente sobre o centenário do Isaac Asimov, que foi, para quem não o conhece, um grande escritor e pensador da tecnologia que inventou, por exemplo, as leis de segurança da robótica. E é muito salutar a gente poder fazer uma referência ao acúmulo de conhecimento que temos sobre tecnologia na academia, na sociedade civil e em outros ambientes, inclusive na literatura.

Então, eu sou atualmente pesquisador em tecnologias focado em políticas públicas na Fundação Mozilla, mas tenho um histórico no setor privado, o que me faz um grande entusiasta da inteligência artificial. Utilizei recursos de visão computacional em vários tipos de serviços que desenvolvemos para finalidades como *marketing*, como gerenciamento de arquivos, mapeamento de dados em grandes bases de dados, mas, além desses tipos de utilização da visão computacional, defendo, sobretudo, a cautela em alguns outros tipos de uso, onde talvez não seja adequada a utilização de visão computacional ou outras modalidades da inteligência artificial, como é o caso, parece-me, na justiça criminal e na persecução penal, sobretudo na figura de tecnologias como reconhecimento facial.

Ao longo dos últimos meses, sobretudo com o debate sobre a generativa, voltou à baila a ideia de que tecnologias seriam ou não neutras. Então, eu queria abrir a minha fala evocando o acúmulo que temos nos campos de ciência, tecnologia e sociedade sobre o fato de que tecnologias não são neutras no mundo real, porque todo tipo de tecnologia é implementada num mundo que já existe, com históricos de informações, dados e relações sociais que já existem. Então, é uma espécie de consenso em alguns campos de estudo de tecnologia e políticas públicas que o desenvolvimento tecnológico, o desenvolvimento da inovação é condicionado por valores, porque qualquer tecnologia, qualquer inovação está estabelecida em contextos específicos, mas também é controlável pelo homem de uma forma bem complexa, afinal de contas, a gente precisa negociar interesses de vários setores, de vários países, de várias ideologias, mas diálogos como esse permitem que a gente controle os futuros e as visões de futuro que temos da tecnologia.

Resgato esse ponto para relembrar alguns avanços que tivemos nos últimos anos no debate sobre regulação de inteligência artificial no sentido da percepção de que uma perspectiva principiológica não é suficiente, e isso se dá por vários motivos. Um deles é o fato de que danos individuais e coletivos que podem ser causados pelo modo pelo qual sistemas algorítmicos têm sido desenvolvidos, sobretudo nos últimos dez anos, com as abordagens conexionistas, podem gerar danos que são amplamente registrados na literatura científica, no jornalismo e nas relações políticas.

Esta apresentação vai estar disponível na página da Comissão.

Queria citar, por exemplo, um mapeamento que eu realizo no meu projeto desvelar.org, que é um projeto financiado pela Fundação Mozilla, em que realizamos um mapeamento de casos de danos e designação algorítmica, e também mencionar a AI Incident Database, que é uma base de dados de



SENADO FEDERAL
Secretaria-Geral da Mesa

incidentes de inteligência artificial que já tem mais de 1,6 mil casos registrados de coisas que vão de influência da IA generativa até precificação discriminatória em aplicativos de entrega, por exemplo. Então, temos esse acúmulo sobre quais seriam os danos possíveis na inteligência artificial. E a regulação pode ser realizada a partir do reconhecimento dessas possibilidades de danos.

É muito bacana falar logo depois do colega da União Europeia, justamente porque essa abordagem de riscos que a União Europeia implementou foi adaptada de uma forma muito interessante pelo PL 2.338, combinando a abordagem de riscos e defesa de direitos. E um argumento, nas últimas semanas, nesta Comissão ou em outros espaços, que volta e meia aparece é a ideia de que não poderíamos nos inspirar na regulação europeia porque o Brasil é mais complexo, porque o Brasil tem interesses próprios. Eu concordo, mas me parece que o Brasil não é a Europa nesse sentido, na direção de que precisamos desenvolver mais mecanismos de defesa de direitos humanos e de defesa da própria soberania do Brasil, além de fomento, não só regulação, não só legislação, mas também fomento. O Brasil, em comparação à União Europeia, tem índices absolutamente maiores relacionados à infração de direitos humanos, à falta de respeito a pontos como o devido processo na Justiça Criminal e outros fatores.

Então, queria reforçar que boa parte da sociedade civil eventualmente concorda que o Brasil deve ter mecanismos específicos, mas na direção de mais defesa. Então, a legislação europeia é uma grande referência, tem grandes avanços e talvez possa ser até avançada no Brasil.

E aí o Estado brasileiro, falando de Justiça Criminal e impactos do racismo, por exemplo, eu não quero ser redundante com a ótima fala que a colega Fernanda Rodrigues, do Iris, fez nesta própria Comissão, mas queria lembrar aqui e trazer à baila, para o avanço desta proposta, alguns compromissos que o Estado brasileiro tem sobre o combate a impactos do racismo. Pensando, seja o Estatuto da Igualdade Racial, seja a Convenção Interamericana contra o Racismo, que tem *status* constitucional, temos a percepção, na verdade, a obrigação de reconhecer que o Estado e a sociedade devem garantir a igualdade de oportunidades através de diversos mecanismos, mas não só; devem realizar pesquisas sobre a natureza, as causas e as manifestações do racismo, discriminação e outras formas de intolerância, inclusive relacionadas às tecnologias digitais emergentes, que é algo em que o Brasil ainda carece de políticas para estudar esse tipo de impacto negativo, mas também para promover alternativas.

Essas considerações podem ser conectadas a uma consideração a um excelente relatório que vai estar lincado no *slideshow*, para quem tiver interesse, que é um relatório sobre tecnologias digitais emergentes, publicado pelas Nações Unidas e produzido pela Relatora das Nações Unidas, Tendayi Achiume, que reforça os necessários compromissos dos Estados em torno do mundo em promover mecanismos de combate aos danos possíveis de sistemas algorítmicos, em consonância e em diálogo com históricos de discriminações de gênero, raça, capacitismo e outras.

Então, trazendo especificamente recomendações, como foi solicitado no convite, queria mencionar novamente, na nota técnica desenvolvida pela Coalizão de Direitos na Rede, de que eu também faço parte, que a colega Tainá Junquillo e outros colegas mencionaram ao longo desta Comissão, que traz algumas sugestões de melhoria do PL 2.338, mas aqui, de um ponto de vista particular, eu queria defender que o PL 2.338 trouxe alguns avanços inestimáveis para o debate sobre inteligência artificial no Brasil, tem diversos pontos positivos sobre a abordagem baseada em riscos e direitos e pode ser aperfeiçoado em alguns pontos.

Então, como o meu tempo está acabando, só queria reforçar, então, duas recomendações bem enxutas e que vão estar disponíveis no material. A primeira delas é a inclusão em implementações de



SENADO FEDERAL
Secretaria-Geral da Mesa

risco inaceitável de tipos de tecnologias que estão sendo rechaçadas em torno do mundo, como o reconhecimento facial em espaço público, que é algo que pode erodir direitos de toda a população em diversas camadas, e pesquisas do Reino Unido, do Brasil e de diversos outros países – aqui eu vou ter algumas lincadas – demonstram esses danos. Precisamos também, parece-me, discutir alguns pontos relacionados a como os relatórios de avaliação de impacto algorítmico podem ser um mecanismo de participação social e a composição das entidades supervisoras, porque precisamos de uma participação social ampla e com decisão, sobretudo nos grupos historicamente vulnerabilizados.

Então, agradeço o espaço e me coloco à disposição da Comissão e dos diversos setores envolvidos.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado, Sr. Tarcízio Roberto da Silva, Pesquisador de Políticas Públicas da Fundação Mozilla.

Na sequência, eu passo a palavra à Sra. Roberta Rodrigues Correia Pimentel, Assessora-Chefe de Proteção de Dados e Privacidade do Ministério Público Militar.

A senhora tem dez minutos.

Obrigado.

A SRA. ROBERTA RODRIGUES CORREIA PIMENTEL (Para expor.) – Boa tarde a todos.

É uma honra poder contribuir e ser útil, ainda mais agora que nós comemoramos o Dia do Servidor Público no final de semana. Então, é muito rico, para mim, poder ser útil aqui com essa temática extremamente importante.

Com relação especificamente ao cibercrime e à cibersegurança, o que é que eu visualizo atualmente de extremamente importante para trazer para contribuição dos debates é o relatório do Fórum Econômico Mundial que saiu este ano de 2023, lá no início do ano, que trouxe o risco cibernético, especificamente os ataques cibernéticos às infraestruturas críticas como o segundo fator de risco entre os *top five*, e com isso eu realmente fiquei muito impressionada, embora, nos anos anteriores, o fórum já tenha atentado para esse problema, com o qual nós precisamos lidar, mas ele também chegar ao segundo fator foi realmente impactante.

Então, eu queria começar minha fala chamando a atenção para isso. Nós não temos tempo para poder entrar em detalhes, mas eu preciso chamar a atenção para isso, porque eu acredito muito que a legislação precisa ser robusta, mas ela não pode limitar, ela não pode trazer entraves para o desenvolvimento da inteligência artificial para a utilização dentro da persecução penal como um todo, na parte toda investigatória, dentro de todas as camadas que fazem parte da persecução penal, desde lá os investigadores, os peritos cibernéticos, os delegados, o Ministério Público, o Judiciário, enfim, toda a cadeia da persecução penal. A gente precisa ter soluções, utilizar a inteligência artificial para soluções que propiciem que a persecução penal seja eficaz realmente contra a criminalidade ostensiva que nós estamos vivendo atualmente. Quem aqui não recebe quase que diariamente uma tentativa de fraude ou algum tipo de ataque? E isso passa tanto por nós, pessoas físicas, quanto por instituições, estados e impacta absurdamente as pesquisas que a gente tem estudado, fala bastante sobre a dificuldade que os estados têm na sua parte econômica, na parte social...

Então, o cibercrime e a cibersegurança são um assunto – e claro, os outros relacionados à inteligência artificial, como saúde e educação, são igualmente relevantes – que tem esse alerta mundial de que "olha, estamos sofrendo com esse ataque massivo; são organizações criminosas que estão investindo nisso". Eles não são apenas aquele estereótipo da pessoa lá com capuzinho, são instituições que estão investindo nisso, inclusive a ponto de estudar... Os *crackers* estão lá prontos para esse tipo de ataque e para o desenvolvimento de inteligência artificial próprio.



SENADO FEDERAL
Secretaria-Geral da Mesa

Qual é o ponto aqui para o qual eu gostaria de chamar a atenção? Qual é a dificuldade da persecução penal? Na criminalidade, eles podem desenvolver uma inteligência artificial própria que não passe pelas formalidades, por exemplo, que a nossa regulamentação traz, e traz muito bem, mas, por óbvio, a criminalidade não vai obedecer aos requisitos legais. Então, os institutos, as camadas da persecução penal precisam ter a sua... Eu não queria utilizar a palavra... Eu pensei numa palavra um pouco violenta. (*Risos.*)

Não, mas a persecução penal precisa ser eficaz – pronto, encontrei aqui uma palavra mais delicada para poder falar. Ela precisa ser eficaz para combater isso, para combater a inteligência artificial que muito possivelmente... E já está acontecendo atualmente, porque já foram encontradas por peritos cibernéticos inteligências artificiais desenvolvidas por *crackers*. Então, a gente precisa se atentar para isso.

Com relação a esse tema, eu encontrei... Acredito que os dispositivos trazidos ali no art. 17 do PL 2.338, quando casados com a principiologia vinda do PL 21, de 2020, especificamente quanto aos incisos XI e XIII, que têm ali uma discussão grande sobre policiamento preditivo e tudo mais... Eu entendo, em princípio, que esses artigos são importantes para a viabilidade da persecução penal, mas isso precisa... Uma sugestão que eu faria com relação a esse tema é um pouco utilizar o exemplo dos Estados Unidos, que ontem mesmo publicaram o seu ato executivo. O que os Estados Unidos fizeram? Eu achei um modelo muito interessante. Criaram uma espécie de grupos de trabalho, são vários com prazos diferenciados e uma finalidade própria para cada um. Eu acredito que poderia ser criado um grupo de trabalho para tratar, por exemplo, desses temas, desses dois incisos especificamente, porque existe também a resolução do CNJ atualmente que fala especificamente de análise preditiva. Pelo que eu já vi os peritos cibernéticos falando, isso é importante para eles na investigação. Então, eu acho que é um tema que precisa ser discutido. Eu vejo com bons olhos, mas, é claro, se o CNJ trouxe, existe uma razão para constar lá.

O segundo ponto para o qual eu acredito que a gente precisa se atentar também é com relação à proteção de dados e privacidade *versus*, digamos assim, à eficácia ou à precisão da inteligência artificial. São dois elementos que ficam frente a frente. Os especialistas em inteligência artificial mesmo, desenvolvedores falam, já vi muitos deles falando e concordando entre si, que o aumento da precisão das aplicações da inteligência artificial gera automaticamente uma baixa na transparência ou na explicabilidade daquela aplicação. E isso, obviamente, requer uma ponderação entre a proteção dos dados pessoais – dos dados gerais, mas especificamente quanto aos pessoais para atender às determinações da Lei Geral de Proteção de Dados – e a proteção da privacidade, mas a proteção dos dados pessoais e da privacidade não pode trazer um entrave ao desenvolvimento da inteligência artificial.

Então essa ponderação, eu acho, também deveria ser estudada mais a fundo em um grupo de trabalho com esse fim, exatamente para poder treinar a inteligência artificial para que os desenvolvedores... Do que eles precisam? Eles precisam de *datasets* robustos e, para isso, eles precisam de dados e de uma quantidade grande de dados; não é de uma quantidade ínfima.

(*Interrupção do som.*)

A SRA. ROBERTA RODRIGUES CORREIA PIMENTEL – E, para ter qualidade desses dados, para que a inteligência artificial seja bem treinada, treinada com valores, com virtudes, ética e moral – isso já foi amplamente discutido aqui –, mas que só nós humanos podemos trazer para inteligência artificial. Valores e virtudes são nossos, não são da máquina em si. E a gente colocando valores e virtudes, por



SENADO FEDERAL
Secretaria-Geral da Mesa

exemplo, já trazendo um pouco da filosofia para cá, que é um tema por que eu sou muito apaixonada, a gente trazendo valores e virtudes consegue inclusive impactar na educação do nosso país como um todo e diminuir o cibercrime inclusive, diminuir a tensão que existe, essa intenção de cometer cibercrime, de cometer crime digital, e a educação ajuda muito nisso. Então um bom treinamento da inteligência artificial com dados robustos também traria muitos benefícios.

Então eu também sugiro que seja criado um grupo de trabalho para tratar isso de modo aprofundado.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Muito obrigado, Sra. Roberta Rodrigues Correia Pimentel, Assessora-Chefe de Proteção de Dados Pessoais e Privacidade do Ministério Público Militar.

Aliás, eu gostaria de colocar alguns pontos sobre isso que eu venho anotando aqui.

Eu faço parte da Comissão de Educação também. Então pode-se até dizer que eu tenho um certo viés para educação, mas o fato é que, se a gente for pensar em todas as atividades humanas, a educação entra como um fator fundamental, uma base de onde a gente constrói uma série de coisas, tanto do conhecimento necessário para o desenvolvimento de novas tecnologias, de novas metodologias, e assim por diante, quanto numa questão mais difícil de se tratar na educação, mas que tem sido de certa forma aflorada com essas discussões de inteligência artificial como ferramenta, que estaria relacionada à natureza – vamos chamar de natureza humana –, que vem através de emoções e de uma série de coisas que acabam norteando o nosso comportamento, tanto para o bem, quanto para o mal.

E isso, a inteligência artificial, eu vejo como um multiplicador dessas tendências. Vou dar um exemplo aqui que deram outro dia, que foi da faca, uma faca – como é que chama? – Tramontina, uma faca. Você pode utilizar essa faca para fazer um alimento, pode utilizar de uma maneira correta, ou as pessoas que têm uma má intenção podem utilizar para ferir outra pessoa ou para ameaçar outra pessoa, e assim por diante. A inteligência artificial tem essa capacidade de multiplicar as intenções humanas, e as intenções humanas aparecem pelas emoções. E vamos lembrar que a inteligência artificial não tem emoção: ela faz aquilo para o qual ela foi, entre aspas, "programada" para fazer; não é exatamente programada, mas ela é treinada para fazer.

E aí vem a questão do treinamento, que é outro ponto que surge. Se você fala em *machine learning*, por exemplo, aprendizado de máquina, específico para uma certa tarefa, a gente está falando de um conjunto relativamente pequeno de dados necessários para que aquele sistema aprenda o que é necessário para cumprir aquela função específica. Quando a gente entra em sistemas mais complexos, como o *deep learning*, por exemplo, aprendizado profundo, nós estamos falando de uma quantidade de dados muito maior, e o aprendizado vai depender justamente da utilização desses dados e da qualidade desses dados. E aí que vem um ponto importante, porque, se esses dados forem parciais – parciais no sentido de não serem completos – e se eles forem parciais no sentido de serem, de certa forma, discriminatórios ou, de certa forma, tiverem algum viés ali dentro, aquela máquina – ela não tem emoção, ela não tem um objetivo nenhum com aquilo – vai aprender com aquilo que ela tem disponível. E isso pode causar distorções sérias na utilização.

Portanto, não só o desenvolvimento dos sistemas, mas também o desenvolvimento dos bancos de dados ou da qualidade desses dados, assim como esses dados são adquiridos, tudo isso é uma coisa muito importante nesse contexto, pensando em tecnologia. Aí tem todas as aplicações.

Como a gente não consegue, com uma lei, por exemplo, regulamentar a tecnologia nos seus detalhes, porque ela vai acontecer... É igual querer segurar a água, ela vai acontecer em algum lugar do planeta, ela vai continuar acontecendo, mas a gente pode, sim, regulamentar a utilização daquilo, da



SENADO FEDERAL
Secretaria-Geral da Mesa

forma correta, da forma ética, da forma não discriminatória e assim por diante. Isso a gente precisa fazer com certeza, precisa se dar essa caracterização, também sempre pensando no ser humano como centro. Eu tenho repetido isso várias vezes aqui para que isso fique bem claro. O ser humano tem que ser o ponto central de tudo isso. Afinal de contas, todo esse desenvolvimento para o bem tem que ser a favor da qualidade de vida, da melhora da eficiência dos sistemas para o ser humano, e não para o sistema em si. A inteligência é só uma ferramenta, ela não pode ser além disso aí. Então, é bom a gente ter em mente esses pontos que acabaram sendo ressaltados na sua fala, e eu acho importante a gente lembrar isso de tempos em tempos aqui.

Então, talvez, de novo, voltando para a parte da educação, deva-se trabalhar com a educação para dar uma formação adequada para as nossas crianças e jovens, para que eles entendam bem as questões de ética, para que eles saibam a diferença entre o bem e o mal, para que eles entendam as questões de moral, o que é o certo e o que é errado e que eles consigam traduzir isso para dentro dos sistemas, que são sempre operados por seres humanos. Isso vai ser muito importante agora, acho que é uma coisa que tem ressaltado bastante, e cabe a nós pais, avós, professores e todos mais prestar atenção a esses detalhes.

Bom, eu passo agora, então, a palavra para o Sr. Rony Vainzof, Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo, por dez minutos, por favor.

Obrigado.

O SR. RONY VAINZOF (Para expor.) – Muito obrigado, Senador Marcos Pontes.

Acho que, com essas suas palavras agora, Senador, eu já saio bastante contente aqui dos nossos debates. Como é bom ter um Parlamentar com tanto conhecimento técnico assim sobre o assunto, cuidando...

Parabéns ao Senado Federal por abrir essa oportunidade e trabalhar com a cautela necessária em relação ao tema inteligência artificial, não só o Sr. Senador Marcos Pontes – estivemos juntos na Fiesp e na Fecomércio –, mas também o Presidente da Comissão Temporária, o Senador Carlos Viana, e o Relator Senador Eduardo Gomes.

Eu queria também agradecer aqui ao colega Marcelo Morales pelo convite. Está aqui a minha colega de Fecomércio Izabel Collor de Mello, também a colega advogada Natalia Peppi e os demais colegas que participaram aqui.

Enfim, acho que essa discussão é mais do que necessária. Como foi apontado aqui, a inteligência artificial é uma tecnologia de propósito geral, depende muito do seu uso. A última vez que a gente discutiu uma tecnologia de propósito geral em termos de regulação foi a internet e estivemos aqui participando de um longo debate sobre o Marco Civil da Internet, uma legislação mais principiológica, porque justamente é complicado regular uma tecnologia e não um direito em si. Diferentemente da proteção de dados pessoais, que é um direito, aqui a gente está regulando a inteligência artificial.

Quando a Europa estava debatendo esse tema e estava chegando a uma conclusão, veio a IA generativa recentemente, e a discussão lá foi redobrada. Tiveram que parar toda a discussão mais seis meses, etc., porque é uma tecnologia. Então, realmente é um tema bastante complexo.

Agora a gente está aqui para discutir a IA no cibercrime. Como o senhor muito bem comentou, infelizmente a tecnologia, que proporciona tanto, também proporciona para as pessoas mal-intencionadas, que é o objeto aqui da nossa discussão.

Não está passando? (*Pausa.*)

Foi.



SENADO FEDERAL
Secretaria-Geral da Mesa

A colega Roberta aqui comentou bastante sobre a discussão que se teve no Fórum Econômico Mundial, em Davos, e é realmente impressionante: 93% dos líderes de *cyber* falaram que o tema de cibersegurança é um dos temas prioritários e 86% dos líderes em geral também comentaram sobre isso.

Um relatório da Cybersecurity Ventures prevê que os custos globais do cibercrime chegarão a 10,5 trilhões por ano até 2025. Esse número é maior que o de danos por desastres naturais e mais lucrativo do que o comércio global de todas as principais drogas ilegais combinadas. Então, é um número, infelizmente, astronômico.

Quando a gente vai para a inteligência artificial, uma consequência natural, infelizmente, do uso massivo da tecnologia é o aumento dos incidentes envolvendo inteligência artificial. Esse aqui é um relatório da Universidade Stanford que mostra o aumento gradativo dos incidentes envolvendo inteligência artificial. Esse número é até 2021, mas o colega que me antecedeu comentou sobre uma base de dados de mais de 1,6 mil casos envolvendo incidentes de inteligência artificial.

E acho que é interessante a gente tratar aqui sobre as principais questões que trazem risco em relação ao uso da inteligência artificial e como as organizações estão mitigando esses riscos.

Esse é um relatório bastante interessante da Mackenzie, que foi feito com mais de 1,6 mil empresas no mundo inteiro, de diferentes tamanhos e de diferentes indústrias. E o principal risco apontado por elas ali foi a questão de falta de precisão: 56%. E qual percentual que está sendo utilizado para mitigar esse risco? Trinta e dois por cento. Depois, cibersegurança, que é o nosso tema aqui, 53%, e 38% estão lidando para mitigar esse risco. O outro risco é a questão de violações de propriedade intelectual. Essa é outra grande discussão global que tem nesse tema, principalmente em razão da proteção do conteúdo que é utilizado para treinar a inteligência artificial, a inteligência artificial generativa. Esses são alguns dos principais riscos, sob a perspectiva das empresas.

Mas o que é mais temerário aqui é esse dado da Europol: a previsão até 2026 é de que 90% do conteúdo *online* vão ser gerados por inteligência artificial, ou seja, conteúdo sintético, não conteúdo gerado por ser humano. A gente está lidando aqui com uma perspectiva de apocalipse da informação. Se a gente já lida com a temeridade de guerra de narrativas, da discussão sobre *fake news*, a gente tem o âmbito da *deepfake* trazendo um desafio ainda maior. Ou seja, quando a gente lida com uma questão da complexidade de moderação de conteúdo *online*, imagine só a gente lidar com a moderação de conteúdo de *deepfake* e também com a moderação de conteúdo daquilo que é gerado por inteligência artificial. Já como o colega adiantou antes, não há neutralidade da tecnologia, ou seja, tudo vai depender daqueles *inputs* e dos *outputs* que são gerados. A gente está falando de dados utilizados para os treinamentos, como o Senador comentou aqui, somados à questão do próprio algoritmo. E, se não há neutralidade e há uma questão de alucinação também da inteligência artificial, ou seja, os próprios erros da inteligência artificial, como a gente vai lidar com essa questão de guerra de narrativas?

Eu vou buscar aqui trazer não só problemas, mas também algumas ideias aqui em relação a perspectivas.

Então, questões de cibercrime: *deepfake* com pornografia, uma temeridade; extorsão – imagine três segundos para fazer uma *deepfake* da voz de alguém se passando por um sequestro, imagine um pai ou uma mãe recebendo isso, ou um vídeo, recebendo isso –; crimes contra a honra; engenharia social – *know your customer, know your client*; hoje tudo é feito com reconhecimento facial, imagine só o potencial desse tipo de situação –; falsificação de provas e documentos; questão de terrorismo e manipulação da opinião pública – a gente está vivendo, infelizmente, duas guerras, a gente já tem uma questão de desinformação muito profunda, imagine só com a utilização de *deepfake*, o que isso pode ocasionar. E, como a colega Roberta comentou, do *deepfake as a service*, porque obviamente as



SENADO FEDERAL
Secretaria-Geral da Mesa

organizações que estão dentro de âmbito de governança vão querer cumprir todas as legislações, mas e as que não estão?

E aqui é só um exemplo de algo bacana da inteligência artificial: uma fábrica de *software* por agentes autônomos, ou seja, você tem o chefe, o gerente de produto, o arquiteto de tecnologia, o gerente de projeto, o engenheiro de *software* e o engenheiro de teste, todos engenheiros autônomos, todos agentes autônomos ali em relação ao desenvolvimento de *softwares*. Imaginem só se os criminosos também operam da mesma forma, por meio de agentes autônomos, numa organização criminosa feita por inteligência artificial.

E a grande questão aqui que a gente está conversando – e talvez uma das grandes iniciativas aqui – é a discussão sobre mecanismos de detecção automatizada e confiável do conteúdo gerado por inteligência artificial.

Esses são alguns *papers* bastante interessantes que depois eu deixo à disposição aqui para estudos. Um deles é da Global Partnership on Artificial Intelligence, e outros dois... Um é outro *paper* que saiu ontem, do G7, e também a colega Roberta comentou sobre a iniciativa dos Estados Unidos também, de ontem. Todos eles trazem a importância sobre mecanismos de detecção automatizada e confiável do conteúdo gerado por IA, ou seja, sobre como a gente pode lidar com essa questão de marcas d'água, selos para se identificar aquilo que é gerado por inteligência artificial. E claro que isso não é para o ser humano – porque a gente não vai conseguir identificar e nem ter a velocidade para se identificar –, mas sim para máquinas. Talvez essa seja uma grande questão.

Então, já conduzindo aqui para o final da minha fala em relação a algumas sugestões... E queria saudar aqui, agora, a presença do Senador querido, Eduardo Gomes, também.

Primeiro, a gente fala muito de regulação, e ela é superimportante. Estamos discutindo aqui regulação. Mas também precisamos discutir um plano de nação para a inteligência artificial, ou seja, sobre como a gente investe aqui no Brasil em pesquisa e desenvolvimento. E a gente estava falando aqui de educação e capacitação de mão de obra qualificada. Então, esse é um dos principais pontos aqui em relação a pensarmos não somente nessa regulação de governança que, sim, é muito importante, mas nesse grande plano de nação para inteligência artificial.

Outro ponto. Esta cautela, Senador, que inclusive o senhor comentou aqui no início: nós regularmos o uso e não a tecnologia. Inclusive, a IA é uma tecnologia de propósito geral, como eu comentei, que está em pleno e constante desenvolvimento, ou seja, é preciso extrema cautela ao regular tecnologias, para que a norma seja suficientemente flexível e adaptável a essas rápidas mudanças que nós estamos acompanhando.

A terceira questão é uma abordagem, sim, baseada em risco. Dependendo do risco, você tem ali uma necessidade de impor uma maior energia sobre a perspectiva de governança. Mas esse risco não deve ser chancelado taxativamente na legislação. Quem deve avaliar o risco, por meio de critérios legais, é o setor que usa IA. Você tem IA para área da saúde; obviamente que muitas das finalidades do uso da IA na área da saúde podem trazer um risco alto, mas algumas outras não. Talvez só a área da saúde é que vá conseguir ali aperfeiçoar esse tipo...

(*Soa a campainha.*)

O SR. RONY VAINZOF – ... de amadurecimento.

Uma flexibilidade regulatória trazendo balizas gerais de governança, e a gente lidar muito com códigos de conduta setorial, e também a possibilidade de correção, ou seja, esses códigos de conduta setoriais que possam ser ali chancelados.



SENADO FEDERAL
Secretaria-Geral da Mesa

Incentivar a inovação responsável. Então, a gente está falando muito aqui em relação à importância da confiança no ambiente digital e na tecnologia. Um médico não vai usar uma inteligência artificial se ele não souber como ela funciona para avaliar um diagnóstico de um paciente. Um comerciante da mesma forma também não vai fazê-lo se não souber como funciona. A gente precisa investir em conscientização das pessoas sobre a tecnologia e privilegiar aqueles que têm uma governança responsável.

Padronização global. A gente tem iniciativas da ONU, da OCDE, G7, União Europeia, Estados Unidos, e no Brasil, felizmente. Isso é muito importante porque é uma tecnologia global.

E, para finalizar, soberania digital e acordos de cooperação internacionais, ou seja, como efetivamente a gente vai fazer *law enforcement*, como a gente vai dar efetividade às investigações e às decisões judiciais em relação às plataformas e também à questão do uso da inteligência artificial pelos criminosos.

Muito obrigado. Por enquanto era isso, Senador.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado. Obrigado ao Sr. Rony Vainzof, ele é Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo.

Eu registro aqui a presença do nosso Senador Relator da Comissão Temporária de Inteligência Artificial, Senador Eduardo Gomes, aqui conosco também.

Só alguns comentários a respeito – antes de passar a palavra para o Senador, que eu gostaria que falasse também aqui neste momento – de uns pontos importantes que eu acho que a gente pode registrar aqui também: a necessidade de um plano nacional. Nós temos a Estratégia Brasileira de Inteligência Artificial, que foi lançada inclusive na época que eu era Ministro, mas ainda precisa de aperfeiçoamentos. É importante que a gente verifique que tecnologias dessa natureza evoluem muito rapidamente, e certamente nós precisamos nos adaptar rapidamente também a essas evoluções.

Como foi citado o GPAI – e eu era o representante do Brasil no The Global Partnership on Artificial Intelligence –, ali a gente discutia muitos desses temas, mas aí a discussão é evolução constante, porque, à medida que a gente está discutindo um tema, de repente você já tem uma tecnologia nova sobre aquele tema, ampliando aquele escopo.

Formação e educação. Já falei aqui 100% da necessidade de nós treinarmos, formarmos os nossos jovens já pensando não só no aspecto técnico, mas também no aspecto cultural e intrapessoal, para que eles entendam realmente que a ética começa ali, começa na pessoa, sempre, e isso que é importante que nós tenhamos.

A parte de segurança cibernética. Tradicionalmente a segurança cibernética é sempre pensada ali para proteger os dados e os sistemas em termos de confidencialidade; em termos de integridade dos dados, para que não sejam alterados lá dentro; ou em termos de viabilidade de uso, de estar o tempo todo disponível para utilização, para não travar o sistema, por exemplo, com um ataque cibernético. Mas aí a gente amplia, porque cada uma dessas raízes dá ali uma série de ramificações, que agora, com inteligência artificial, passam a ser mais complexas de se tratar.

A gente pode utilizar a inteligência artificial para defesa, mas também para o ataque, ou seja, esse trato aparece na sua apresentação, no eslaide, bem claro isso aí. Muitos pontos a serem tratados agora com a amplificação, a ampliação dessas possibilidades com a inteligência artificial.

Aliás, eu acho, falando de segurança cibernética, que, da mesma forma que nós temos nossos antivírus no computador, funcionando diretamente... Tem duas coisas que a gente pode pensar do antivírus. Ele precisa ser eficiente e suficiente para te proteger dos vírus, de ataques cibernéticos aos



SENADO FEDERAL
Secretaria-Geral da Mesa

seus dados, ao seu computador, mas também não pode ser tão pesado que ele pare o seu computador, que você não consiga operar. Acho que todo mundo já deve ter tido essa experiência aqui de se botar um antivírus que funciona bem, mas nada mais funciona no computador, só o antivírus. (*Risos.*)

Aí fica complicado.

Por outro lado, também, como você vê a capacidade da inteligência artificial. Nós estávamos tratando disso de manhã. Por exemplo, em *deepfake*, de criar imagens, vídeos, vozes de pessoas ali, não é? Para você distinguir se aquilo é verdade ou se não é verdade, a inteligência artificial também pode... como se fosse um antivírus contra a própria inteligência artificial, ou seja, buscando maneiras de identificar o que está errado naquilo lá, o que não é verdadeiro, o que é falso, e realmente bloquear esse tipo de atividade.

E, finalmente, o risco setorial. Isso é uma coisa que nós também identificamos aqui. Nós temos, obviamente, todos os setores trabalhando com inteligência artificial, o setor da saúde, o setor de telecomunicações, petróleo e tanto mais, e cada um tem a sua agência de regulação já, responsável em fiscalizar – punir, se for o caso – as atividades incorretas naquele setor, e tudo isso vai ter que ser premiado pela inteligência artificial.

Então, cada um desses setores tem que ter o seu departamento, seja lá o que for, departamento, divisão de inteligência artificial, segurança cibernética, que tudo isso converse com essa centralização no risco e que o risco seja cuidado – esse é um ponto importante também que nós detectamos aqui –, diferentemente do que se prevê na legislação, nesse projeto de lei, não por setor, por exemplo, o setor de educação é um setor de alto risco, o setor de saúde é um setor de alto risco; não é exatamente o setor, mas as atividades que podem estar dentro daquele setor. Por exemplo, se a gente faz uma inteligência artificial para fazer diagnóstico, por exemplo, diagnóstico de câncer de mama, com participação da inteligência artificial, ela auxilia o médico a tomar uma decisão, ela não aumenta o risco, ela diminui o risco, na verdade. Agora, se ela vai fazer uma cirurgia, a inteligência artificial fazendo, assim, obviamente aí o risco fica bastante alto e tem que ser visto, e assim vai.

A soberania também é outro ponto importantíssimo. A inteligência artificial tem se desenvolvido em todos os países. Se a gente não acompanhar essa tendência, a gente vai ficar para trás, e isso fere muito a nossa possibilidade de soberania, porque ela vai ser literalmente introduzida, aqui, por várias fontes diferentes, e aí o controle dos nossos sistemas críticos, etc. passa a ficar bastante arriscado. Basta ver o que aconteceu na Ucrânia, atrás, com a segurança cibernética, com relação à parte de energia elétrica em 2015, quando um *malware* foi colocado por um vírus em um *e-mail*; a pessoa abriu aquele *e-mail*, e aquilo lá abriu as portas para que os adversários, vamos chamar assim, conseguissem entrar dentro do sistema e desligar a energia elétrica para mais de 250 mil pessoas, além de bloquear o acesso dos usuários ao sistema de reclamação, ou seja, o caos foi estabelecido lá, um ataque coordenado. Então, tem que se tomar muito cuidado com isso.

Antes de continuar, antes de passar a palavra ao Sr. Carlos Eduardo Miguel Sobral, eu vou passar a palavra aqui, se me permite, ao nosso Senador Eduardo Gomes, Relator da Comissão, que, com muita honra, nos dá a sua presença aqui.

Obrigado.

O SR. EDUARDO GOMES (Bloco Parlamentar Vanguarda/PL - TO. Pela ordem.) – Sr. Presidente, Senador Marcos Pontes, que preside esta sessão, esta audiência pública, a todos os expositores meus cumprimentos, aos que estão aqui presentes, aos que estão participando por videoconferência.

Presidente, apenas para cumprimentar a todos e também registrar que, no dia de amanhã, V. Exa. estará concluindo o processo de audiências públicas com muito êxito, com dez audiências públicas e



SENADO FEDERAL
Secretaria-Geral da Mesa

80 pessoas das mais diferentes representações participando do debate sobre inteligência artificial, fora aquilo que já vem carregado pelo próprio histórico de audiências públicas da Comissão de Juristas, os debates pelos autores dos projetos que foram pensados. Portanto, cumprimos uma etapa importante e que merece, além do reconhecimento, uma solicitação e um entendimento. Já que no sistema da Comissão – estava falando, agora há pouco, com a Adriana, e ela me confirmou isso –, já que no sistema da Comissão Especial, bem como na TV Senado e nos órgãos de comunicação da Casa, estão disponíveis todas as audiências, nós gostaríamos de pedir a todos os expositores das mais diferentes representações que visitem as exposições, uns dos outros, se necessário, num debate que vai ter como consequência, Presidente, tanto mais rápido possível, a realização de uma comissão geral para que a gente possa passar diretamente a um processo não de simplificar, mas de entender qual é a legislação mínima, dinâmica.

Eu sempre brinco que a gente vai ter que fazer uma lei viva, a inteligência artificial é aquele projeto de lei que tem que ficar vivo, tem que estar vivo. E todas as vezes que eu escuto o nosso Ministro, o Astronauta Marcos Pontes, que é um especialista dedicado ao tema, nessa última passagem agora em que ele falou, eu fico com a impressão de que nós é que somos os vírus da inteligência. *(Risos.)*

Morri de medo disso. Você veja, um dispositivo só desligar a energia de 250 mil pessoas. A gente não consegue fazer com que o ser humano ligue a energia da nossa casa. Dependendo do dia, e, se tiver um jogo de futebol bom, aí é que ninguém vem mesmo.

Mas eu queria deixar claro que estou muito satisfeito de participar deste grupo, o Senador Carlos Viana também tem dado todo o apoio à Comissão, e acredito mesmo que um dos primeiros sinais da importância da lei e da importância da participação de todos vocês é que a gente consiga votar aí até o dia 15 de dezembro, e eu tenho certeza de que esta Comissão vai cumprir o seu prazo. Então, estou muito feliz que a gente possa desenvolver dessa forma. E vamos contar com a Câmara dos Deputados para a gente dar essa dinâmica, mesmo com a preocupação de que vamos ouvir tudo e nem tudo vamos ter condição de colocar no texto, até porque é o que o senhor disse, o texto é vivo ali, é aquela coisa, mas a gente não pode ficar para trás também, tem que organizar.

Então, passo por aqui para, mais uma vez, agradecer a todos pela participação. Já pedimos à TV Senado um compacto com todas essas questões, vou fazer contato também com as assembleias legislativas, o poder público como um todo, divulgando o que foi discutido aqui, porque vai que surge mais um ponto ou outro e a gente consegue ir para essa comissão geral com a situação de análise de texto mais real possível.

Quero agradecer e parabenizar V. Exa. Eu vou agora para um debate sobre tarifa de energia elétrica em que, com certeza, vão falar alguma coisa de inteligência artificial.

Obrigado.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Sem dúvida, Senador Eduardo Gomes, nosso Relator, obrigado pela presença. Sem dúvida lá também agora vão entrar os *smart meters*, medidores inteligentes, que vão utilizar essas coisas. Aliás nós estamos fazendo essa audiência hoje, realizando essa audiência graças ao requerimento do Senador Eduardo Gomes, que foi o autor desse requerimento.

Então, na sequência, eu passo a palavra ao Sr. Carlos Eduardo Miguel Sobral, Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública.

Sr. Carlos, o senhor tem dez minutos para a apresentação. Peço que controle o tempo pelo lado de lá, porque não vai conseguir ver o nosso relógio aqui. Obrigado.



SENADO FEDERAL
Secretaria-Geral da Mesa

O SR. CARLOS EDUARDO MIGUEL SOBRAL (Para expor. *Por videoconferência.*) – Obrigado, Senador Marcos Pontes.

Desejo uma boa tarde a todos nós, parabenizo o Senado pela iniciativa da Comissão Temporária, o Senador Eduardo Gomes, o Senador Carlos Viana, agradeço o convite, agradeço também a participação, e quero homenagear as intervenções do meu amigo Rony e tantas outras discussões ao longo dessa última década, o Dr. Tarcízio, o Dr. Carlos Oliveira, o Dr. Cid Silveira.

Bom, é uma oportunidade poder falar de um tema tão complexo. E ficar por último, Senador, tem uma vantagem: a gente aprende, ouve, consegue absorver muito conhecimento, e tem um problema também, que é trazer algo novo ao debate. Creio eu que todos os pontos que pensei enfrentar e trazer à reflexão foram abordados aqui pelos colegas que me antecederam. Então, eu vou tentar, ao longo da exposição, trazer alguns pontos para a reflexão.

Sou delegado da Polícia Federal e tive a oportunidade de coordenar a área de crimes cibernéticos durante oito anos, de 2007 a 2014. Participamos das discussões da lei de crimes cibernéticos, do marco civil da internet, acompanhamos, de um pouco mais distante, a Lei Geral de Proteção de Dados Pessoais, e o desafio me parece que é de tamanha envergadura, que é, de alguma forma, regulamentar ou dar um tratamento para novas tecnologias.

O uso da tecnologia e os riscos derivados das novas tecnologias não são novidade na história humana. Vários são os exemplos de tecnologias que vieram para o enriquecimento e o crescimento da sociedade humana e que eventualmente foram usadas também para causar grandes danos, como a TNT, a própria fusão nuclear. Ninguém imagina viver sem as tecnologias, mas, de uma forma ou de outra, alguém ou um conjunto de pessoas se utilizaram dessas tecnologias para causar grandes danos à humanidade. E, com a inteligência artificial, me parece que não é diferente. Não imagino que a gente consiga conter o avanço tecnológico, imagino também que seja algo positivo, mas evidentemente que o desenvolvimento dessa tecnologia implica riscos.

E eu concordo com os colegas que me antecederam que a regulamentação ou praticar um tratamento baseado na análise de riscos é o melhor caminho para a gente conseguir ter um acompanhamento da tecnologia, mitigando, reduzindo os riscos de acordo com como eles vão sendo percebidos.

E vejo a importância muito grande, Senadores, de esta Comissão trazer atores da sociedade para o debate. Nós tivemos também essa experiência, durante a lei de crimes cibernéticos, do marco civil da internet. A discussão inicia numa comunidade técnica mais estrita e, ao longo do debate, vai alcançando, vai penetrando os demais segmentos da sociedade, que vão compreendendo como é que a tecnologia pode afetar a vida das pessoas que não tenham conhecimento tão próximo da tecnologia. Então, esse debate é extremamente importante e também fazer uma ampla discussão com todos os setores envolvidos da sociedade, haja vista que todos nós seremos, de uma forma ou de outra, afetados pela tecnologia.

Cumprimento também a Dra. Roberta, acabei me esquecendo no início, porque ela trouxe uma discussão que é bastante interessante, que é a da tecnologia auxiliando-nos a termos a construção de uma sociedade mais justa, mais equilibrada, mais harmônica. Isso também nos remete a reflexões: a tecnologia como indutora de comportamento e a tecnologia como reprodutora de comportamento. Se nós pensarmos numa inteligência artificial como indutora de comportamento, fazendo algo novo, mudando a nossa ação com base em valores, com base em princípios, nos traz reflexão, numa sociedade plural, de quais valores, de quais princípios, ou seja, qual será o *framework*, qual será o *dataset*, em termos técnicos, que irá nortear essa indução, essa mudança de comportamento.



SENADO FEDERAL
Secretaria-Geral da Mesa

Se a tecnologia for reprodutora de comportamentos, numa sociedade que for discriminatória, que for racista, que for misógina, essa tecnologia, se ela usar como padrão o comportamento médio dessa sociedade misógina, racista, discriminatória, a tecnologia vai enviesar, dá para ver que vai ser um viés, vai ser um conhecimento, um ensinamento de como é o nosso padrão comportamental.

Então, tanto a tecnologia como reprodutora de comportamento ou a tecnologia como indutora de comportamento nos traz uma série de questões extremamente complexas que têm que envolver um conjunto, uma gama enorme da sociedade – se não toda a sociedade – para que a gente consiga não enviesar de um lado ou de outro, com esse debate bem profundo de como a inteligência artificial vai alterar o nosso comportamento.

Em relação aos crimes cibernéticos, a única certeza que eu tenho, Senador Marcos Pontes, Senadores da Comissão e colegas, é que o crime organizado e o crime cibernético vão usar a tecnologia da inteligência artificial. Essa é a única certeza! E, como todos os demais, há problemas relacionados à tecnologia – é um problema global. Então, se nós tentarmos dar uma solução caseira e, de alguma forma, imaginar que a gente vai conseguir coibir o uso da inteligência artificial por criminosos no Brasil regulamentando internamente, sem ter um tratamento global, não vai conseguir; a tecnologia vai ser desenvolvida fora, vai ser desenvolvida pelos brasileiros fora, vai ser desenvolvida na nuvem, em todo canto, e a gente não vai conseguir enfrentar o uso da tecnologia se não for também com o uso da tecnologia.

Então, é muito importante – e agora falo como Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública –, é fundamental que a gente use a inteligência artificial, que a gente use os recursos disponíveis, tecnológicos para combater o crime, que a gente tenha a identificação de padrão, o aprendizado de máquina, *deep learning*, identificação de algoritmos, ou seja, que a gente use o que há de mais moderno da tecnologia para a gente enfrentar o crime cibernético – não só cibernético, mas todo tipo de crime, que, de uma forma ou de outra, vai usar a tecnologia. Todo crime organizado tem necessariamente um departamento de TI – vamos chamar assim –, que escala, promove uma escalabilidade das suas atividades, seja para a prática do ilícito, seja para lavagem de dinheiro, seja para ocultação, rastreamento com criptomoeda, enfim, ele usa a tecnologia para todo tipo de... para ocultar o resultado do ilícito ou para praticar o ilícito.

Então, é importante que a gente tenha acesso, que o Estado brasileiro consiga, na sua área de segurança pública, na sua área investigativa, na sua área de inteligência de segurança pública, usar as tecnologias. Evidentemente que com muito controle, com muita transparência, e a gente persegue sempre que inteligência não é clandestinidade, inteligência não é secretismo; inteligência é sigilo, controle e transparência daquilo que já pode ser tornado público.

Então, da mesma forma que o Estado tem acesso à tecnologia de inteligência artificial...

(Soa a campanha.)

O SR. CARLOS EDUARDO MIGUEL SOBRAL *(Por videoconferência.)* – ... é importante, sim, que haja controle, que haja auditoria, que haja rastreabilidade do uso das tecnologias, mas que a gente não fique alheio ao uso, para que seja possível combater o crime cibernético, combater a criminalidade geral por meio da tecnologia.

O Dr. Rony comentou sobre a dificuldade que é na área de crimes cibernéticos quando nós temos uma enxurrada de *deepfake*. Podemos ter tecnologia para enfrentar? Com certeza. Mas será que todo mundo, toda plataforma, todos vão ter uma antivírus ou uma vacina, vamos chamar assim, que consiga detectar se algo é falso? Imaginem voz, imagem, vídeo sendo falsificados em escala, e nós sermos



SENADO FEDERAL
Secretaria-Geral da Mesa

soterrados, sobrecarregados com esse tipo de informação inverídica, que pode causar todo tipo de dano, seja moral, seja patrimonial, seja extorsão, seja político, seja eleitoral, ou seja, é uma gama de situações críticas, que nos envolvem numa reflexão bem profunda. Que a gente consiga analisar esse risco e já adotar... E talvez este seja o grande diferencial do sucesso ou insucesso: o tempo de, detectado um risco, detectado um problema, a gente conseguir adotar uma solução que seja efetiva e eficaz. Então, quanto menor o tempo do risco à solução, menor será o nosso dano e maior será a nossa segurança promovida e permitida à nossa sociedade.

Então, concluindo, eu queria agradecer de novo e me colocar à disposição para os debates.
Obrigado, Senador.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado, Sr. Carlos Eduardo Miguel Sobral, Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública.

Bom, concluídas as nossas apresentações, a gente passa agora à fase de perguntas e respostas, e, dado o tempo que nós temos disponível até às 4h, eu gostaria de fazer da seguinte forma: eu tenho aqui as perguntas que nós recebemos através do e-Cidadania. Eu vou ler essas perguntas com calma, cada uma delas, e, aqui, os nossos debatedores locais, presenciais aqui, já têm a cópia. Os que estão no remoto não têm a cópia. Então, o que eu vou fazer? Eu vou ler com muita calma, e dá tempo, então, para cada um dos nossos debatedores remotos raciocinar sobre a pergunta, anotar talvez o nome e a pergunta, para que, durante as considerações finais – eu vou passar a palavra novamente a todos os debatedores –, vocês possam, ao mesmo tempo, fazer as considerações finais e responder às perguntas que acharem conveniente responder. O.k.?

Também é possível... Se algum debatedor quiser perguntar para outro também alguma coisa durante essas considerações, também poderá fazê-lo.

Então, começando aqui pelas perguntas, a primeira pergunta, da Júlia Teresa, de Minas Gerais: "[...] [É possível citar casos em que a [...] [inteligência artificial] teve um impacto [...] na investigação e julgamento de crimes cibernéticos?]. Novamente, Júlia Teresa, de Minas Gerais: "[...] [É possível citar] casos em que a [...] [inteligência artificial] teve um impacto [...] na investigação e julgamento de crimes cibernéticos?].

Segunda pergunta, da Regiane Gama, de São Paulo: "Como serão as medidas de punição ao uso de inteligência artificial para [...] [a prática de crimes cibernéticos]?". De novo, Regiane Gama, de São Paulo: "Como serão as medidas de punição ao uso de inteligência artificial para [...] [a prática de crimes cibernéticos]?".

Terceira pergunta, do Bruno Araújo, da Bahia: "Como a inteligência artificial está sendo usada para combater o cibercrime? Quais os principais métodos e tecnologias [...] [disponíveis]?". De novo, Bruno Araújo, da Bahia, são duas perguntas: "Como a inteligência artificial está sendo usada para combater o cibercrime [ou crime cibernético]? [Segunda] quais os principais métodos e tecnologias [...] [disponíveis]?".

Quarta pergunta, da Laura Lourdes, de São Paulo: "Como seria a aplicação da inteligência artificial na administração do sistema de justiça criminal?". De novo, Laura Lourdes, de São Paulo: "Como seria a aplicação da inteligência artificial na administração do sistema de justiça criminal?".

Quinta pergunta, do Guilherme Marques, de São Paulo: "Como a Abin e a Polícia Federal [...] poderiam contribuir [...] [mediante a produção de conhecimento sobre o tema]?". De novo, pergunta do Guilherme Marques, de São Paulo: "Como a [...] [Agência Brasileira de Inteligência] Abin e a Polícia



SENADO FEDERAL
Secretaria-Geral da Mesa

Federal [...] poderiam contribuir [...] [mediante a produção de conhecimento para esse tema de inteligência artificial]?"

Sexta pergunta, Luiza Lins, do Rio de Janeiro: "Qual o correto procedimento que uma vítima de cibercrime deveria seguir [...]?". Boa pergunta essa aqui, é bom para as pessoas saberem também. De novo, a Luiza Lins, do Rio de Janeiro: "Qual [...] o correto procedimento que uma vítima de cibercrime deveria seguir [...] [esse tipo de crime é cada vez mais banalizado]?". Esta é uma afirmação: esse tipo de crime é cada vez mais banalizado. Então, novamente, Luiza Lins, do Rio de Janeiro: "Qual [...] o correto procedimento que uma vítima de cibercrime deveria seguir [...]?". E ela está afirmando aqui que esse tipo de crime é cada vez mais banalizado.

Dito isso, feitas as nossas perguntas, eu vou passar de novo a palavra para os nossos debatedores para as suas considerações finais e para responder as questões que acharem adequadas de serem respondidas.

Começo pelo Sr. Carlos Oliveira, Administrador Principal da Direção-Geral de Redes de Comunicação, Conteúdos e Tecnologias da Comissão Europeia. Então, Carlos...

Dá tempo de colocar cinco minutos em vez de dois? *(Pausa.)*

Vou colocar cinco minutos para as suas considerações finais e para responder as perguntas que achar adequadas para que você responda.

Obrigado.

O SR. CARLOS JOSÉ OLIVEIRA *(Para expor. Por videoconferência.)* – Senador Marcos Pontes, uma vez mais, é um prazer estar a participar nesta discussão, sobretudo tendo o privilégio de escutar intervenções muito interessantes e muito ilustrativas daquilo que são os riscos com que estamos confrontados não só com o mau uso da inteligência artificial, mas, ao mesmo tempo também, com ilustrações daquilo que são as possibilidades e o potencial que ela tem também para um uso correto. Em muitas matérias, tem a ver com a captação de crimes.

E, digamos, tentando passar em revista a longa lista de questões que eu tentei anotar.

Há muitas questões que têm a ver no fundo com comportamentos de carácter criminal em que no fundo a inteligência artificial funciona como um instrumento, mas o crime em si já é objeto de penalização no âmbito daquilo que são as legislações sobre as mais variadas matérias desde o conteúdo ilegal até a manipulação de informação. Tudo isso, digamos, em muitos casos já faz parte do edifício legislativo que previne essas práticas. Naturalmente que a inteligência artificial em alguns domínios permite, por assim dizer, dar uma amplitude a essas más práticas ou a esses comportamentos de carácter criminal, digamos, com um impacto maior sobre as pessoas, empresas e organizações.

Dito isso, outra vertente que foi também ilustrada por vários oradores sobre a utilização da inteligência artificial como um instrumento de investigação é também uma área que está sendo muito explorada porque, por exemplo... Eu vou dar aqui alguns casos em que a utilização de informação a partir, por exemplo, de fotografias por satélites tem sido muito utilizada em muitos casos para detectar situações de construções, de locais, por exemplo de má utilização de subsídios para agricultura. Há vários exemplos de trabalhos que foram feitos nessa área por parte dos organismos da União Europeia que previnem fraudes, corrupção. Isso é só para dar alguns exemplos. Portanto, as duas coisas não são necessariamente contraditórias.

Nós, pelo nosso lado, achamos que igualmente é muito importante esta colaboração com o Brasil porque é um país que tem uma posição de saliência na área dos elementos e sistemas de inteligência artificial. Para nós é muito importante também obter o ponto de vista e o sentimento daquilo que são as pessoas, digamos, de outras geografias para também enriquecer aquilo que é não só a legislação,



SENADO FEDERAL
Secretaria-Geral da Mesa

mas também a prática. Portanto, há um conjunto de aspectos que, dada a evolução tecnológica nesta área, nós temos que, por assim dizer, definir um conjunto de princípios e ir ajustando a aplicação da lei de acordo com o que são os novos desenvolvimentos nesta matéria.

Eu gostaria de voltar um pouquinho ainda aos comentários que foram mencionados por vários dos oradores. Aproveito para endereçar aqui uma saudação especial com quem teve oportunidade de partilhar o cenário, em várias oportunidades, sobre este tema da inteligência artificial e também sobre proteção de dados. Nós gostaríamos muito de aproveitar para aprofundar esta nossa discussão e esta cooperação para reforçar os aspectos de proteção das pessoas nas suas várias dimensões com a mensagem de que existe inteligência artificial centrada no ser humano.

Eu não estou seguro de ter conseguido responder a todas as perguntas, mas gostava de deixar aqui uma mensagem que, aliás, foi citada por um dos palestrantes, que tinha a ver com o trabalho que tem sido desenvolvido pela Europol nestas áreas de investigação criminal e que seria bem interessante porventura discutir num âmbito mais específico, ligada também àquilo que é a problemática do cibercrime e às questões da cibersegurança.

Por isso, espero dar continuidade a este diálogo com o empenho mútuo e continuar a aprofundar estas questões.

Para nós a IA é de facto algo que tem um impacto muito importante na modernização da economia, na melhoria do bem-estar dos cidadãos e no sistema social, mas nós temos que ter sempre presente aquilo que são os efeitos indesejáveis e as patologias que qualquer tecnologia...

Uma saudação a todos, e eu continuo à disposição, caso surjam mais algumas perguntas.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado, Sr. Carlos Oliveira, Administrador Principal da Direção-Geral de Redes de Comunicação, Conteúdos e Tecnologias da Comissão Europeia.

Obrigado pela participação, Carlos, bom te ver.

Eu gostaria, então, de passar a palavra ao Sr. Tarcízio Roberto da Silva, Pesquisador de Políticas Públicas da Fundação Mozilla, para suas considerações finais e resposta a algumas das perguntas que assim desejar.

Obrigado.

O SR. TARCÍZIO ROBERTO DA SILVA (Para expor. *Por videoconferência.*) – Muito obrigado, Senador.

Queria primeiro saudar todos os participantes novamente.

Fico muito feliz de ver – ou rever – alguns colegas com quem temos participado desse debate sobre como estabelecer consensos sobre a tecnologia.

Eu anotei aqui uma questão – se eu peguei o nome certo, é Paula Milanez –, que perguntou sobre a questão dos dados, se existe uma legislação sobre como os dados para treinamento de IA são coletados e quais são os mecanismos necessários.

A depender do ponto de vista das interpretações do ordenamento jurídico com a Lei Geral de Proteção de Dados, existem, sim, muitos mecanismos que são aplicados para a inteligência artificial já, mas eu também queria lembrar algumas colaborações no sentido de transparência, como, por exemplo, uma metodologia muito interessante desenvolvida com o nome *datasheets* ou *datasets*, que seriam, em português, planilhas para bases de dados. Foram sete ou oito pesquisadoras que desenvolveram esse sistema, à época a Timnit Gebru, que estava no Google, e a Kate Crawford, pesquisadora da Microsoft – ou seja, mesmo dentro dessas empresas de *big tech* –, que fizeram uma lista de perguntas necessárias que as empresas deveriam fazer ao construir uma base de dados,



SENADO FEDERAL
Secretaria-Geral da Mesa

pesquisas relacionadas à motivação, relacionadas à composição da base de dados, relacionadas à segurança desses dados, o modo de coleta, direito autoral e assim por diante.

Perguntas como essas e metodologias como essas são muito interessantes não só para promover a transparência e permitir, por exemplo, que as possíveis entidades supervisoras possam dialogar com as organizações que desenvolvem, seja setor privado, seja universidade, sejam estados, mas a existência dessas perguntas como uma prática pelos desenvolvedores faz com que o desenvolvimento da inteligência artificial seja mais responsável.

Se uma empresa, por exemplo, que desenvolve um sistema de IA generativa consegue responder a todas aquelas perguntas, mesmo sendo algo caro – e é caro, está fazendo controle efetivo –, significa que o processo foi mais responsável.

Então, esse tipo de iniciativa é essencial, mesmo que a gente não tenha uma abordagem legislativa ou uma abordagem legalista, ou que seja necessária, como já existe no caso da LGPD, uma implementação legal da questão. Mas os mecanismos para fazer isso já existem. E enquanto diversos setores, a academia, a sociedade civil, setor privado, a gente pode chegar a esses consensos para que todas as entidades desenvolvedoras façam as melhores práticas.

Acho que é isso. As outras perguntas acho que estão mais na alçada dos colegas.

Queria reforçar o convite a consumirem a nota técnica da Coalizão Direitos na Rede sobre o PL 2.338, que apresenta algumas críticas e algumas sugestões para o avanço da matéria.

Muito obrigado e saudação a todos.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado, Sr. Tarcízio Roberto da Silva, Pesquisador de Políticas Públicas da Fundação Mozilla.

Na sequência, para suas considerações finais e resposta a algumas das perguntas, eu passo a palavra à Sra. Roberta Rodrigues Correia Pimentel, Assessora-Chefe de Proteção de Dados e Privacidade do Ministério Público Militar.

A SRA. ROBERTA RODRIGUES CORREIA PIMENTEL (Para expor.) – Muito obrigada.

Algumas perguntas aqui estão relacionadas, não é? A maioria, pelo que eu li aqui, está perguntando se a inteligência artificial já teve participação nas investigações e como isso está acontecendo. De fato, na parte investigatória já existe, já é uma realidade; tanto na parte de inteligência em si se utiliza inteligência artificial como na investigação comum, tanto para cibercrime quanto para crimes comuns também, que não são crimes digitais.

Teve uma outra pergunta aqui. A Regiane Gama perguntou como serão as medidas de punição ao uso de inteligência artificial para a prática de crimes cibernéticos. Eu acredito... Não tenho conhecimento de haver alguma punição para a utilização de IA para a prática de crimes cibernéticos, não. Não sei se... Essa resposta minha não é conclusiva, porque eu realmente não tenho certeza, mas eu acredito que não. Por quê? Eu sei que existem discussões de temas como, por exemplo... Não seria um crime em si, mas poderia atenuar, poderia majorar, etc., o uso da inteligência artificial. Na verdade, eu não sei nem se seria majorar ou atenuar, depende muito do crime cometido, porque a inteligência artificial ajudaria, então também pode ser, enfim, uma forma de majorar, mas eu não tenho conhecimento.

Quanto ao restante, eu acredito que o colega Carlos Eduardo pode responder com relação à parte de crimes da parte da inteligência.

Agora eu queria fazer uma pequena observação, voltando ao tema da cibersegurança: nesse relatório do Fórum Econômico Mundial, eles sugeriram, há uma sugestão, inclusive, para que a cibersegurança esteja dentro do ESG, que é a classificação ESG das corporações de ambiental, social e



SENADO FEDERAL
Secretaria-Geral da Mesa

de governança. Pelo que eu vi lá dentro da governança, seria também a governança de segurança cibernética para nós termos noção do tanto que isso realmente está impactando fortemente.

E só um ponto com relação à educação, que eu falei anteriormente: o que eu acredito que a educação impacta está exatamente na fala do Sr. Carlos Eduardo e do Rony também, quando a gente fala do treinamento da inteligência artificial. Como a inteligência artificial, hoje em dia, impacta as nossas vidas e as nossas decisões agora, inclusive na formação do nosso senso crítico como ser humano e como a gente aprende, isso impacta diretamente na educação. Então, se você alimenta com os dados corretos baseados em valores, isso impacta na educação do país. Não tenho dúvida nenhuma disso. E que vai inclusive diminuir... Sou até entusiasta, assim.

(Soa a campainha.)

A SRA. ROBERTA RODRIGUES CORREIA PIMENTEL – Fico alegre de falar disso, porque vai diminuir o cibercrime inclusive. Eu tenho uma alegria de falar disso.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado, Sra. Roberta Rodrigues Correia Pimentel, Assessora-Chefe de Proteção de Dados e Privacidade do Ministério Público Militar.

Agora eu passo, na sequência, a palavra para as considerações finais e respostas a perguntas, para o Sr. Rony Vainzof, Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo.

O SR. RONY VAINZOF (Para expor.) – Obrigado, Senador.

Eu queria saudar o Carlos Oliveira e o querido amigo Carlos Sobral. A gente, assim como o senhor, Senador, está desde a discussão da lei de crimes informáticos, depois o Marco Civil da Internet, a Lei Geral de Proteção de Dados e agora estamos discutindo aqui o marco regulatório da IA. São queridos companheiros que contribuem bastante aqui com o Congresso Nacional sobre esses temas.

Quais serão as medidas de punição em relação ao uso da IA? Como a colega falou, não importa o meio. Tem uma decisão do STF bastante interessante de 2018, Senador, que apurava o crime de pornografia infantil, se era crime ou não, porque, na época, o tipo penal era só fotografar ou publicar, e o sujeito fez o *upload* na internet de pornografia infantil. O advogado estava defendendo que aquilo violava o princípio da legalidade, porque ele não tinha nem fotografado nem publicado. O caso aconteceu em 1996, e o que era publicar em 1996? Era numa revista física ou num jornal. O STF falou basicamente o seguinte: o crime de homicídio é matar alguém, não importa se é por meio de arma de fogo ou se é com uma facada. Então, assim, não importa o meio. Já tem tipificação penal para as mais variadas condutas e não importa o meio, se é utilizada inteligência artificial ou não, que é uma tecnologia. Claro que os perigos estão na escala que isso tem, e aí vêm todas essas nossas discussões aqui.

Em relação à outra pergunta que foi feita sobre a utilização da IA para investigação, as investigações – depois acho que o Dr. Sobral pode comentar – já utilizam e têm que utilizar mesmo. A eficiência precisa estar nas novas tecnologias sejam elas quais forem. O CNJ está com mais de 150 projetos em 29 tribunais diferentes. O Ministro Presidente do STF, o Ministro Barroso, recentemente fez uma reunião com as *big techs* em relação a estudos de IA generativa, e assim é com as investigações. Imagine a quantidade de informações em buscas e apreensões em nuvem, em buscas e apreensões em dispositivos, em dados estruturados, em dados não estruturados. Se você não utilizar ferramentas como a inteligência artificial para as investigações, o crime sempre vai estar na frente das investigações. Então, esse é um ponto super-relevante.



SENADO FEDERAL
Secretaria-Geral da Mesa

E para finalizar aqui algumas considerações finais, Senador, primeiro, acho que a gente não pode nem supervalorizar os benefícios da tecnologia e nem subestimar seus desafios. E o Senado aqui está fazendo um papel crucial com essa Comissão Temporária, justamente não subestimando os desafios da tecnologia.

Eu quero reiterar aqui a importância do plano de nação para inteligência artificial, Senador: investimento e capacitação. A gente tem que refletir sobre se queremos ser eternamente consumidores de tecnologia ou ter um plano a médio e longo prazo, para a gente poder efetivamente desenvolver tecnologia e ter gente capacitada para isso. É importantíssimo inovação criteriosa e responsável, ou seja, eficiência precisa caminhar ao lado de princípios. A gente passou da fase do *digital first*, porque hoje tudo é *digital*; aliás, é *phygital*, porque não tem mais essa distinção entre físico e digital; estamos na fase do *digital trust*, da confiança no ambiente digital, e, para isso, nós precisamos de segurança cibernética, proteção de dados e inteligência artificial ética e responsável.

Crucial da efetividade é a lei já existente da política nacional de educação digital, ou seja, um letramento digital e de inovação, e tem alguns relatórios que mostram os perigos sobre a substituição dos profissionais pela inteligência artificial. Inclusive, eu sou advogado, Senador. A segunda maior posição de exposição de profissionais é do Legal. E será que nós seremos substituídos? Somente aqueles que não usarem a tecnologia a seu favor. Então, não é uma questão de substituição, é uma questão de complementariedade, é uma questão de simbiose entre homem e máquina. A gente precisa ressaltar a importância dessa complementariedade e não da substituição.

(*Soa a campainha.*)

O SR. RONY VAINZOF – Então, parabéns pelo trabalho e muito obrigado, Senador.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado ao Sr. Rony Vainzof, Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo.

Eu gostaria também aqui de registrar a presença do Deputado Federal Pedro Aihara, de Minas Gerais – obrigado aqui pela presença –, ressaltando o *background* de ser um bombeiro militar, ou seja, uma das pessoas, um dos heróis que nos ajudam, no dia a dia, a salvar vidas. Parabéns pela carreira. Obrigado pela presença aqui também.

Eu gostaria de passar a palavra agora, para suas considerações finais, ao Sr. Carlos Eduardo Miguel Sobral, Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública. E certamente muitas das perguntas estão dentro aí, exatamente, do escopo do seu trabalho. Parabéns pelo trabalho e obrigado, já antecipadamente, pela participação.

O SR. CARLOS EDUARDO MIGUEL SOBRAL (Para expor. *Por videoconferência.*) – Obrigado, Senador.

Ao tempo que me despeço e parabenizo de novo o Senado pela realização não só dessa audiência, mas de todo o trabalho da Comissão Temporária, primeiro, digo que concordo com todos os colegas que me antecederam, em especial o Dr. Rony, que disse que a inteligência artificial não vai substituir a atividade humana, ela vem para complementar, ela vem para auxiliar, e todo uso da inteligência e tecnologia na atividade de investigação tem sempre, ao final do processo, uma pessoa, um ser humano que avalia, valida e decide, auxiliado pela tecnologia.

O uso da inteligência artificial, da tecnologia no combate ao crime não é recente. Nós temos uma larga experiência de uso no combate à pornografia infantil, na detecção de imagem de criança em situação de exploração sexual, através de tonalidade de pele, quantidade de pele envolvida numa



SENADO FEDERAL
Secretaria-Geral da Mesa

imagem. Essas imagens são nas casas de milhões, e o tratamento da inteligência artificial nos permite ter um primeiro filtro, que depois é validado pela atividade humana, o que nos proporciona um combate à pornografia infantil. Então, é bem comum o uso da inteligência artificial.

Outro uso também que é comum é a identificação de símbolos de natureza criminosa em imagens e vídeos, e a identificação de locais através de imagem. Então, em uma imagem que é um retrato de uma situação criminosa, tanto de sequestro como também de exploração sexual, é comum, com o tratamento da imagem, se buscar o local retratado ou parte do local retratado – em uma quantidade imensa de imagens. Então, é comum o uso da tecnologia para o combate a pornografia infantil, crimes de ódio e exploração sexual.

Está em andamento a evolução desses usos para outras tantas atividades, de investigação, de inteligência. Nós temos um tema a ser enfrentado, que é a autenticação via biometria, o reconhecimento facial. Ainda não há um histórico grande de utilidade, mas é uma pauta que está na agenda e é um debate também que é público – dos alcances, dos limites e das repercussões. E neste particular, eu vejo muito salutar a participação dos órgãos públicos, como Abin, PF, não só, mas de todos os órgãos públicos que tenham pertinência, aderência ao tema, que tragam ao debate suas reflexões sobre os potenciais usos positivos e potenciais riscos de uso negativo da tecnologia. É importante que tragam suas visões, para que a gente possa ter uma reflexão bem madura, bem abrangente da tecnologia e de suas repercussões.

Por fim, Senador, o uso da tecnologia para a prática de crime, como o Dr. Rony comentou. Mas o instrumento... O autor do delito vai responder pelo crime praticado, independentemente do instrumento que ele use, que seja uma inteligência artificial, seja um dispositivo informático, seja uma faca, seja uma arma de fogo. Enfim, independentemente do instrumento que ele utilize, vai responder pelo crime praticado.

Na Lei de Crimes Cibernéticos nós temos um dispositivo que trata daquele que produz um dispositivo informático, um código malicioso para a prática de crime. Ele não é usuário do instrumento, por isso que ele não responde pelo crime praticado. Mas ele produz aquele instrumento com o intuito de permitir a prática do crime. Então, pode ser que, eventualmente num debate, se nós tivermos inteligência artificial sendo produzida, customizada, ensinada para a prática de delitos, não sendo ele o autor do delito, pode ser que haja, sim, uma oportunidade para dar o mesmo tratamento – nós temos o art.154-A do Código Penal – de criminalizar aquele que desenvolve tecnologia com dolo específico de utilizá-la para a prática de delito. Ou seja, ele tem que saber, tem que querer e desenvolver aquela ferramenta, aquela inteligência artificial para a prática de crime, e talvez tenha aí uma oportunidade, sim, de se prever uma criminalização.

Então, despoço-me e agradeço a oportunidade.

O SR. PRESIDENTE (Astronauta Marcos Pontes. Bloco Parlamentar Vanguarda/PL - SP) – Obrigado, Sr. Carlos Eduardo Miguel Sobral, Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública.

Eu também gostaria de registrar a presença do Dr. Helio Kimelblat, Diretor Executivo da Rede Amazônica, aqui conosco, lembrando que esta manhã, nós tivemos aqui um debate nesse local sobre a utilização de inteligência artificial no jornalismo e em outras áreas, como nas eleições também. Então, obrigado pela presença.

Antes de encerrar esta presente reunião, eu gostaria de colocar em votação a aprovação da Ata da 11ª Reunião.



SENADO FEDERAL
Secretaria-Geral da Mesa

Então, de forma protocolar, as Sras. e os Srs. Senadores que aprovam permaneçam como estão.
(Pausa.)

A ata está aprovada e será publicada no *Diário do Senado Federal*.

Antes de terminar, também eu gostaria de novamente agradecer a todos os nossos apresentadores, debatedores: o Sr. Carlos Oliveira, Administrador Principal da Direção-Geral de Comunicações, Redes, Conteúdos e Tecnologia da Comissão Europeia, que esteve conosco nesse debate; o Sr. Tarcízio Roberto da Silva, Pesquisador de Políticas Públicas da Fundação Mozilla; a Sra. Roberta Rodrigues Correia Pimentel, Assessora-Chefe de Proteção de Dados e Privacidade do Ministério Público Militar; Rony Vainzof, Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo – obrigado –; e o Sr. Carlos Eduardo Miguel Sobral, Coordenador-Geral de Inteligência da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública.

Gostaria também de agradecer a todos aqueles que nos acompanharam através da TV Senado e das redes do Senado Federal, e em especial aqueles que participaram com perguntas, através do Portal e-Cidadania: Julia Teresa, de Minas Gerais; Regiane Gama, de São Paulo; Bruno Araújo, da Bahia; Laura Lourdes, de São Paulo; Guilherme Marques, de São Paulo; e Luíza Lins, do Rio de Janeiro.

Não havendo mais nada a se tratar, eu declaro encerrada esta reunião e desejo uma ótima noite para todos.

Obrigado.

(Iniciada às 14 horas e 14 minutos, a reunião é encerrada às 16 horas e 10 minutos.)