RELATÓRIO FINAL - FIB 14

a) Informações sobre a atividade

Título: **Inteligência Artificial aliada à atividade policial: entre a segurança pública e o incremento de novos riscos**

Temas:

- ➔ NTIA – INTELIGÊNCIA ARTIFICIAL
- ➔ PRIS – PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS
- ➔ QJUR – QUESTÕES LEGAIS E REGULATÓRIAS

Proponente: Guzmán, Finoto & Bougleux Advogados

Tipo: Organização (pessoa jurídica de direito privado)

Região: Sudeste

Setor: Empresarial

Moderador:

Nome: **Ana Vitória D'Assumpção Guzmán**

Organização: Guzmán, Finoto & Bougleux Advogados

Setor: Empresarial

Minibiografia: Sócia do Guzmán Finoto e Bougleux Advogados, Especialista em Direito Digital e Compliance e Pós-graduanda em Governança da Tecnologia da Informação. Integrante da Comunidade Internacional de Estudos em Direito Digital (CIED) e Presidente da Comissão de Privacidade e Proteção de Dados da OAB/Uberlândia. Autora de capítulos e artigos em direito digital e proteção de dados pessoais.

Relator:

Nome: **Ana Paula Bougleux Andrade Resende**

Organização: Tribunal de Justiça de Minas Gerais (TJMG)

Setor: governamental

Minibiografia: Mestre em Direito pela Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP), especialista em Direito Digital pela faculdade CERS e graduada em Direito pela Universidade Federal de Uberlândia (UFU). Atualmente atua como Analista de Privacidade e Proteção de Dados no Tribunal de Justiça de Minas Gerais (TJMG).

Palestrantes:

Nome: **Michele Nogueira Lima**

Organização: Universidade Federal de Minas Gerais (UFMG)

Setor: comunidade científica e tecnológica

Minibiografia: Cientista da Computação. Doutora pela Université Pierre et Marie Curie, França, 2009. Professora associada do Departamento de Ciência da Computação (DCC) da UFMG. Atuou como membro Titular do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD).

Nome: **Luiza Corrêa de Magalhães Dutra**

Organização: Instituto de Referência em Sociedade e Internet (IRIS)

Setor: terceiro setor

Minibiografia: Doutoranda e mestra pelo programa de pós graduação em Ciências Criminais da PUCRS. Especialista em Segurança Pública, Cidadania e Diversidade pela UFRGS. Pesquisadora do Instituto de Referência em Internet e Sociedade (IRIS).

Nome: **Lucas Andrade**

Organização: SEPOL/RJ

Setor: governamental

Minibiografia: Encarregado de proteção de dados pessoais na SEPOL/RJDPO pela Exin. Colaborador externo da Comissão de Proteção de Dados Pessoais da OAB-RJ/Barra da Tijuca. Master of Laws em Direito, Inovação e Tecnologia pela FGV. Coordenador do Comitê de Segurança Pública e Persecução Penal da GovDADOS.

Nome: **Humberto de Sá Garay**

Organização: Dígitro Tecnologia

Setor: empresarial

Minibiografia: Humberto de Sá Garay, destacado por sua profunda expertise em Computação Forense e Perícia Digital, brilha como consultor sênior nas fronteiras da tecnologia e inteligência para a segurança pública e corporativa. Sua jornada inclui uma notável posição executiva em Governança de TI/COBIT e uma robusta formação com pós-graduação em Inteligência Empresarial pela renomada Fundação Getúlio Vargas (FGV), especialização em Políticas e Gestão da Segurança Pública pela Universidade Federal do Rio Grande do Sul, e bacharelado em Ciências Militares pela Academia de Polícia Militar da Brigada Militar do Estado do Rio Grande do Sul. Humberto é reconhecido por sua vasta experiência no desenvolvimento de projetos educacionais e sistemas de segurança avançados, atuando em posições de liderança em importantes órgãos de inteligência policial do Brasil. Com um foco inabalável nas políticas institucionais de compliance, proteção de dados e do conhecimento, ele emprega sua expertise para desenvolver consultorias especializadas em análise de cenários, conformidade regulatória e segurança da informação. Além disso, Humberto é um ávido pesquisador em Engenharia do Conhecimento, dedicando-se ao desenvolvimento de modelos e sistemas que potencializam atividades intensivas em conhecimento. Este profissional será um dos participantes do evento sobre o fórum de internet no Brasil, trazendo sua valiosa contribuição sobre produção de conhecimento e proteção de dados.

b) Estruturação do workshop

Objetivos e resultados (propostos e atingidos):

O objetivo geral proposto pelo workshop era expor de que forma a Inteligência Artificial (IA) vem sendo adotada nas atividades de policiamento no cenário brasileiro e, a partir disso, quais benefícios e malefícios são vislumbrados. Já com relação aos objetivos específicos propostos, foram elencados:

- abordar as possibilidades de uso da IA em prol da atividade policial e de segurança pública no cenário global e brasileiro, assim como os fatores que legitimam a prática;
- expor os possíveis efeitos colaterais decorrentes das ferramentas identificadas, tais como riscos aos direitos a privacidade, igualdade e não discriminação;
- explorar o cenário regulatório existente e em discussão a nível legislativo;
- refletir acerca dos mecanismos de avaliação e controle dessas ferramentas, em nível técnico e jurídico.

Quanto aos objetivos efetivamente atingidos, é possível afirmar que houve o tangenciamento de todas as questões propostas, em maior ou menor grau, sem prejuízo de maior aprofundamento, conforme será elucidado no tópico "Síntese dos debates".

Para além disso, foi possível realizar um debate plural e, principalmente, propositivo acerca da difícil tarefa de promover melhoria do desempenho da atividade policial em contraponto às problemáticas vislumbradas, de modo a colocar contrapontos a ambos os extremos (quais sejam: a defesa, de forma ampla, do abolimento da IA aplicada ao contexto jurídico-criminal *versus* a concepção de que as ferramentas técnicas são a solução dos problemas dos centros urbanos e devem ser aplicadas de forma irrestrita e sem critérios específicos).

Dentre outros resultados, tem-se a conscientização do público em geral acerca da relevância, complexidade e urgência na discussão da temática, o levantamento de questões técnicas que devem ser objeto de maior aprofundamento para o estabelecimento de requisitos rígidos, bem como a chamada de atenção para a necessidade de que haja um

debate multissetorial mais aprofundado acerca dos parâmetros a serem adotados quando da implementação dessas ferramentas.

Justificativa em relação à governança da Internet:

Já faz alguns anos que a aplicação da Inteligência Artificial é cada vez mais extensiva e difundida em nossa sociedade através das diversas formas que pode adotar (IA especialista ou generalista). Não demorou para que ela se apresentasse útil à segurança pública e, inclusive, à atividade policial.

Neste âmbito, contudo, é ainda consideravelmente prematura, tanto na perspectiva da técnica em si, quanto na perspectiva jurídica e social. Por isso, a sua utilização, quando ainda revestida de tal precocidade, implica em riscos que sequer são totalmente conhecidos.

A problemática que envolve a sua utilização parece emanar das mesmas premissas ditas para a sua validação, uma vez que, ainda que apresente potencial de melhorar a eficácia das forças policiais, também levanta preocupações sérias sobre privacidade, discriminação e governança. A vigilância constante e a análise de dados pessoais podem minar a liberdade individual e criar um ambiente de vigilância em massa, que ameaça os direitos civis.

Para enfrentar esses desafios, é preciso estabelecer uma Governança da Internet sólida, transparente e plural. E considerando que esta abrange a regulamentação e a supervisão das tecnologias digitais, é preciso aproveitá-las de modo a garantir que sejam usadas de maneira ética e equitativa. Isso demanda a colaboração entre governos, empresas, sociedade civil e especialistas em tecnologia para desenvolver políticas e normas que protejam os direitos humanos e a privacidade e, ao mesmo tempo, promovam a inovação e o uso responsável da IA.

É nesta exata medida em que discutir o tema (IA e atividade policial) com representantes dos mais diversos setores da sociedade torna-se tão relevante para o incremento qualitativo da Governança da Internet no Brasil e também no mundo.

Metodologia e formas de participação desenvolvidas durante a atividade:

O workshop teve 90 minutos de duração, cuja dinâmica seguiu o seguinte roteiro, na ordem estabelecida:

a) 10 min - introdução do workshop;
b) 65 min - perguntas e respostas formulados pela moderadora e direcionadas aos palestrantes;
c) 5 min - conclusão das ideias por parte dos palestrantes;
d) 10 min - perguntas do público.

Quanto ao momento de perguntas e respostas dos palestrantes, foi estabelecido um momento dinâmico conduzido pela debatedora, em que a mesma pergunta pudesse ser feita a palestrantes diferentes, no intuito de apresentar pontos de vistas diferentes acerca da mesma questão. Disponibilizamos o período de 5 minutos para que cada palestrante expusesse suas reflexões e respostas, não sendo obrigatório utilizar o tempo de fala integralmente.

c) Síntese dos debates

TIPO DE MANIFESTAÇÃO	CONTEÚDO	CONSENSO OU DISSENSO	PONTOS A APROFUNDAR
Posicionamento - Luiza	Segurança pública, no Brasil, historicamente pautada na utilização ilegítima da força e da violência, gerando ações que ofendem os direitos fundamentais. Perfil da figura da "pessoa suspeita" muito bem definido, tratam-se de negros, homens e jovens. Instituições brasileiras, especialmente as responsáveis pela segurança pública, atuam com base no racismo. Já no que se refere às tecnologias digitais, elas emergem como uma forma de romper o panorama de discricionariedade da polícia, no intuito de promover maior transparência e accountability, objetivando melhorar o policiamento a partir da tecnificação. Três exemplos de aplicação: ● policiamento preditivo: aplicação da modelagem por computadores a dados passados para tentar predizer atividades futuras (muito aplicado nos EUA e no Canadá, mas também em pauta em São Paulo, por meio do Detecta); problemáticas: quais dados são utilizados no input, como são	Consenso	Estado tem atuado com tecnologias de vanguarda, mas sem estabelecer um mínimo de procedimentaliza ção.

	utilizados, quais softwares são adotados, como a IA é treinada, qual é o objetivo dessa forma de policiamento; ● hacking governamental: exploração de vulnerabilidades ou falhas em sistemas e/ou dispositivos móveis, de modo a acessar dados privados em comunicações para fins de uma investigação (ex: Pegasus); problemáticas: dúvida acerca da existência de critérios para a utilização desses mecanismos; ● câmeras corporais utilizadas nas fardas dos policiais, sobre as quais pende a discussão sobre implementação de Inteligência Artificial para fins de reconhecimento facial; problemáticas: reconhecimento facial amplamente criticado por apresentar resultados racistas (grandes falhas no reconhecimento de pessoas negras);		
Proposta - Luiza	Diversas formas de aplicar as tecnologias ao contexto da atividade policial e segurança pública, sendo necessário analisar cada uma conforme as suas particularidades: ● Defende o banimento do uso de tecnologias de reconhecimento facial no âmbito da segurança pública;	Dissenso	Técnicas adotadas devem estar amparadas em pesquisa científica; Não se deve restringir o livre

	• Defende a nulidade de ações da polícia que se pautem no acesso a comunicações privadas em dispositivos móveis sem que haja ordem judicial para tanto; • Defende o estabelecimento de parâmetros jurídicos a serem seguidos para a autorização de atividades de investigação que impliquem no acesso a comunicações privadas; • Ferramentas de hacking governamental (que permitem o acesso a comunicações passadas, futuras e até mesmo a modificação de comunicações) devem ser consideradas ilícitas e serem vedadas inteiramente, inclusive pela impossibilidade de se estabelecer uma cadeia de custódia da prova penal;		uso de criptografia forte; Necessidade de acompanhamento e controle externo das atividades policiais.
Posicionamento - Humberto	A aquisição de tecnologia pelo Estado observa critérios rígidos, aos quais as empresas privadas que pretendem comercializar suas soluções estão vinculadas; Ministério da Justiça conta com uma coordenadoria somente para verificar o tipo de tecnologia utilizada para fins de produção de provas. Além disso, já existem legislações que	Dissenso	Suficiência ou insuficiência do arcabouço regulatório brasieliro atual com relação aos riscos decorrentes da IA no Âmbito da

	estabelecem um regramento para a utilização de provas tecnicamente produzidas; há uma série de previsões legais capazes de disciplinar a adoção desse tipo de prova, a exemplo do código de processo penal, de normas ISO e de diplomas legislativos que estabelecem regramento acerca da formatação da prova e critérios para que a perícia seja realizada, ao passo que ao Ministério Público cabe o controle interno e externo da atividade judicial. Nesse sentido, a iniciativa privada deve estar atenta aos requisitos e critérios estabelecidos, assim como ao próprio mercado.		segurança pública.
Posicionamento - Lucas	A demonstração de parâmetros de adequação aos controles de proteção de dados pessoais e segurança da informação são essenciais para legitimar o uso da força no ambiente de utilização de modelos baseados em. IA. Faz-se um contraponto com relação à generalização de que a atuação policial é sempre pautada em preconceitos e lesão a direitos fundamentais, para destacar que existem servidores públicos/policiais que prezam pela transformação digital segura e atuação policial hígida. Pontua a existência de bens jurídicos informáticos (nos termos do professor	Dissenso	A utilização de tecnologia, em si mesma, não é o problema, mas sim a falta de parâmetros objetivos para o uso juridicamente seguro.

	Spencer Sydow), o que implica em valores imprescindíveis à convivência em sociedade que estão em formato digitalizado. Logo, o mundo do crime também tem as suas atividades desenvolvidas em ambiente digital, a partir de onde vê-se com preocupação o total banimento de uma tecnologia específica. O que parece problemático não é o uso da tecnologia em si, mas a falta de parâmetros para utilizá-la. A transparência na tomada de decisão atrelada à garantia, especialmente na cadeia de custódia, de confidencialidade, disponibilidade, integridade e autenticidade dos vestígios digitais são capazes de legitimar a persecução penal, de modo a entregar mais ferramentas à investigação. Ferramentas de policeware/spyware já utilizadas da União Europeia com respectiva regulamentação (Espanha, Estônia, Finlândia e França). A utilização de tecnologia, em si mesma, não é o problema, mas sim a falta de parâmetros objetivos para o uso juridicamente seguro. Iniciativas que podem inspirar/incentivar o estabelecimento desse regramento mencionado: ● AI act (normativa europeia recém aprovada), que estabelece parâmetros de adoção da IA, a exemplo das		

	proibições expressas e da imposição de obrigações específicas, quando da adoção; ● Sandbox regulatório adotado pelo Ministério Público do Rio de Janeiro, no qual, de maneira colaborativa, se estudam maneiras de instrumentalizar a IA e modelos tecnológicos para dar suporte à atuação institucional do Ministério Público; Segurança pública como a base de entrega de inúmeros direitos fundamentais, sem a qual não é possível ter esse tipo de debate.		
Posicionamento - Lucas	Inexistência de troca de boas práticas e diálogo interinstitucional entre os órgãos de segurança pública, o que se torna uma problemática. Assim, os parâmetros para contratação de uma tecnologia segura acabam sendo pouco disseminados nos órgãos de segurança. A observância das normas ISO, de um framework previamente estabelecido e medidas de accountability, associada a análise de riscos, implica em fugir do tecno-solucionismo. Por outro lado, é cultural entender que a última tecnologia do mercado vai resolver os problemas da sociedade, não se trata de uma questão exclusiva da polícia.	Consenso	Inexistência de troca de boas práticas e diálogo interinstitucional entre os órgãos de segurança pública a respeito do objeto de discussão.

	Assim, a reflexão e análise a respeito do exposto abre margem para que seja possível tecer críticas às tecnologias adotadas de forma pontual, por parte da sociedade civil, autoridades públicas, dentre outros, inclusive a respeito do processo de tomada de decisão no sentido de contratar e/ou adotar determinada tecnologia, de modo a criar de um espiral virtuoso no âmbito do serviço público.		
Posicionamento - Michele	Imprescindibilidade de que a segurança cibernética esteja inserida no debate, uma vez que os nossos dispositivos se encontram todos conectados. No âmbito da polícia, os algoritmos podem trazer a automatização de tarefas que podem beneficiar as atividades desenvolvidas, inclusive quando se leva em consideração a escassez de recursos. Atenção aos riscos e problemáticas: 1) Equívoco em afirmar que a IA é extremamente inteligente, até mesmo em nível superior à inteligência humana; isso porque os algoritmos, de forma bastante simplificada, trabalham meramente com a classificação de dados em grupos; 2) Problemática da explicabilidade e transparência: dificuldade de explicar os algoritmos, uma vez que necessitam da entrada de dados (*input*) para definir qual a	Consenso	Limitações expostas (especialmente dificuldade de explicabilidade e vulnerabilidades inerentes aos sistemas de IA) apontam para a necessidade de adotar as ferramentas de IA com precaução.

	melhor delimitação do modelo que será criado, delimitação essa que passará por um treinamento pelos dados de entrada, de modo que eventualmente serão observados vieses e/ou teor de aleatoriedade relacionados às saídas (*output*), o que dificulta a explicabilidade das ferramentas; Limitações expostas apontam para a necessidade de adotar as ferramentas de IA com precaução. Para além disso, destaca-se a problemática de adquirir uma ferramenta decorrente de tecnologia estrangeira, uma vez que é necessário analisar o nosso contexto, ter os nossos próprios parâmetros e definir a implementação disso, até mesmo porque são questões que interferem na explicabilidade. Por fim, mencionou-se que ataques podem ser direcionados aos próprios modelos, por meio da manipulação dos dados de entrada e/ou manipulação do treinamento dos algoritmos (denominados ataques adversariais), situações que podem enviesar os modelos em questão. Todo o exposto deve ser levado em consideração para se alcançar em um certo nível de transparência, especialmente porque as vulnerabilidades são intrínsecas aos sistemas.		

Proposta - Michele	Equipamentos decorrentes de tecnologia estrangeira, seja de comunicação, armazenamento (como serviços de cloud) ou formação de data centers, que eventualmente sejam adquiridos pelo poder público brasileiro implica em que não se tenha certeza sobre a implementação da ferramenta, haja vista que não é possível acessar o seu código fonte. É possível exemplificar os riscos existentes pelo *data exfiltration*, que ocorre quando um malware e/ou um agente mal-intencionado realiza uma transferência de dados não autorizada de um computador. Por outro lado, torna-se extremamente dificultoso desenvolver essas ferramentas no Brasil (capacidade não explorada e indústria não desenvolvida nesse sentido), panorama que resulta em uma grande problemática de soberania digital. Voltando a problemática especificamente para a IA, é preciso destacar que os dados utilizados via de regra serão replicados por uma questão de redundância/segurança da informação; assim, nada impede que terceiros (a exemplo de governos estrangeiros) tenham acesso aos dados, inclusive quando envolverem informações estratégicas nacionais, como ocorre nos dados que versam sobre segurança pública. A solução para a problemática seria a	Consenso	Adoção de ferramentas de IA pelo Poder Público implica em preocupações a nível de soberania digital.

	criação de data centers no Brasil, que não poderiam depender de equipamentos estrangeiros ou pelo menos ter a certeza de que não detém nenhuma abertura (*trapdoor*) que eventualmente seja explorada de forma virtual por pessoas mal intencionadas.		
Proposta - Michele	Produção e coleta de dados pessoais, associada à maior capacidade de processamento de dados em ambientes e à evolução do processamento de dados, implicaram na evolução dos algoritmos, de modo que a IA, atualmente, seja dependente dos dados. Apesar disso, vieses são inerentes aos dados, de modo que decisões pautadas em algoritmos, mas sem reflexão, sejam capazes de gerar grandes riscos (problemática de considerar IA mais inteligente que os humanos). Aponta-se, portanto, para os seguintes caminhos: ● necessidade da supervisão humana; ● análise crítica dos resultados decorrentes de algoritmos; ● questionamento se os dados de entrada têm vieses; ● técnicas de correlação que podem ser aplicadas para amenizar as situações mencionadas. Por fim, pontua-se que os algoritmos vão evoluir à medida que tenhamos mais dados	Consenso	Supervisão humana da IA; capacidade de análise dos resultados; identificação de vieses inerentes ao funcionamento da IA.

	e consigamos ter um equilíbrio maior e equidade com relação a disponibilidade dos dados.		
Proposta - Luiza	É inevitável que a formulação de bancos de dados para utilização na segurança pública envolve dados imbuídos de preconceitos, haja vista o contexto brasileiro de racismo estrutural; aponta-se, portanto, para a necessidade de transparência quanto à finalidade das ferramentas, ao objetivo da tecnologia e aos resultados da adoção/implementação à toda a sociedade, não apenas à polícia; apenas assim seria possível promover um debate multissetorial. Outro ponto relevante refere-se à profissionalização dos policiais e da ação das polícias nesse campo (necessidade de investimento nesse sentido). Além disso, aponta-se a necessidade de promover uma discussão plural que envolva a própria sociedade, sem ignorar que a adoção de tecnologias estrangeiras pode estar atrelada a um contexto diverso da realidade brasileira. Necessidade de promover estudos científicos na área, com dois objetivos: (1) incremento da educação da sociedade a respeito do uso das tecnologias no âmbito da segurança pública; e (2) desenvolvimento de estruturas	Consenso	Necessidade de promover estudos científicos na área, com dois objetivos: (1) incremento da educação da sociedade a respeito do uso das tecnologias no âmbito da segurança pública; e (2) desenvolvimento de estruturas regulatórias, considerando princípios da finalidade, necessidade e proporcionalidade.

	regulatórias, considerando princípios da finalidade, necessidade e proporcionalidade.		
Posicionamento - Lucas	Maiores desafios na implementação das tecnologias discutidas: ● Contratação de tecnologias, que deveria ser antecedida de uma análise de riscos robusta; ● Capacitação profissional dos servidores que operam essas tecnologias e dos tomadores de decisão; ● Implementação da tecnologia sem prejudicar a eficiência do serviço público pelos atores da segurança pública e persecução penal.	Consenso	Desafios expostos devem ser aprofundados.