Parecer 10/2024.

Rio de Janeiro, 31 de julho de 2024.

Para: **ASSOCIAÇÃO DE DOCENTES DO CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA - ADCEFET-RJ - SEÇÃO SINDICAL DO ANDES - SINDICATO NACIONAL**

Assunto: **Parecer sobre uso pela Administração do CEFET-RJ de sistema de reconhecimento facial, sem a expressa permissão dos servidores e qualquer outra condição ou informação prévia.**

A **ADCEFET-RJ** solicita parecer da Assessoria Jurídica, **Escritório Boechat e Wagner Advogados**, sobre o uso pela **Administração do CEFET-RJ** de sistema de reconhecimento facial, a ser implantado para acesso de alunos e servidores à Unidade Maracanã, sem a expressa permissão dos servidores e qualquer outra condição ou informação prévia.

Em Ofício dirigido ao Diretor Geral (09/2024/ADCEFET-RJ), em 02 de abril de 2024, os docentes representantes da Diretoria e Conselho de Representantes da **Adcefet-RJ**, questionaram sobre a implantação de reconhecimento facial na Unidade Maracanã, nos termos iniciais, transcritos abaixo:

> Nós, docentes representantes da Diretoria e do Conselho de Representantes da Adcefet-rj Seção Sindical e da Diretoria do ANDES-SN, nos dirigimos à Direção-Geral do Cefet/RJ para questionar a decisão autoritária de implantar sistema de reconhecimento facial na Unidade Maracanã para o controle de acesso e saída às dependências da instituição, com o argumento falacioso de reforço à segurança na unidade, conforme registrado em matéria publicada no site da instituição em 20 de março de 2024, disponível em: (...)

Corretíssima a postura das representações sindicais, pois na hipótese de instalação de mecanismos que importe na captação de dados sensíveis como a atribuição de identificadores relacionada à pessoa natural identificada ou identificável representa violação de direitos constitucionais e legais de proteção à privacidade que tratam do consentimento em processos de coleta de dados.

A proteção de dados pessoais é decorrente do direito constitucional à vida privada e intimidade prevista no inciso X do Art. 5º da Constituição da República transcrito a seguir:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - **são <u>invioláveis</u> a intimidade, a vida privada, a honra e <u>a imagem das pessoas</u>**, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

O sistema normativo de proteção de dados pessoais é construído a partir da interpretação conjunta da Constituição, do Código Civil (em especial o Capítulo II, que trata dos direitos da personalidade), da Lei de Acesso a Informação (em especial da seção V intitulada “Das Informações Pessoais”), do Marco Civil da Internet (Lei 12.965/2014) e da Lei do Cadastro Positivo (Lei 12.414/2011), além do Código de Defesa do Consumidor (em especial o capítulo “Dos Bancos de Dados e Cadastros de Consumidores”) para as relações consumeristas.

Neste campo de proteção, estão inseridos os resultados das pesquisas referidas no Ofício dirigido ao Diretor Geral, em 02 de abril de 2024, informada nos termos seguintes:

> (...) evocamos aqui, como agentes da construção de conhecimento, os resultados de pesquisas nos campos dos Estudos Críticos de Dados (Critical Data Studies), das relações étnico-raciais e de outros coletivos de pensamento, que vêm demonstrando os riscos da implantação desse tipo de tecnologia para populações não-brancas ou lidas como destoantes por lógicas que estabelecem alguns corpos como padrões em detrimento de outros, o que significa submeter pessoas pretas, pardas, trans, não-binárias, dentre outras, a constrangimentos por falhas de identificação, incluindo a não identificação ou erros por não diferenciação entre corpos/sujeitos distintos/as. Essas falhas, por exemplo, no âmbito do uso desse tipo de sistema na segurança pública, têm gerado prisões irregulares e danos irreversíveis a pessoas reconhecidas erroneamente como suspeitas de crimes que jamais cometeram. (...)

É fato comprovado por notícias corriqueiras do cotidiano nas diversas mídias e em pesquisas acadêmicas que o **abuso no uso de tecnologias de reconhecimento facial** é de ***enorme gravidade quando o assunto é a liberdade das pessoas***. Isso porque tais situações, especialmente de uso não autorizado de tais tecnológicas, acabam gerando resultados discriminatórios, constrangedores, racistas e injustos.

Em termos de proteção legislativa, cabe uma maior atenção às previsões contidas na Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD). Destaque especial para seu artigo 5º, inciso X, ao estabelecer que **o tratamento de dados/informação é**

> **"toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"**.

No contexto da LGPD, a proteção de dados pessoais não se resume aos parâmetros clássicos do **"direito à privacidade"** enquanto pessoa-informação-*sigilo*, mas é compreendida corretamente no quadrinômio ***pessoa-informação-circulação-controle***. Não se trata de simples mudança tópica, de nomenclatura, ou algo desprendido de sentido.

Antes pelo contrário, os aspectos de circulação e controle são centrais para o marco regulatório da proteção de dados pessoais, em especial porque, na maior parte dos sistemas de captura e tratamento de dados, todos esses processos escapam do âmbito da atuação própria e especifica do usuário do sistema, sendo regido por algoritmos e mecanismos outros, via de regra automatizados, independentes das decisões e ações voluntárias do usurário. E, nesse contexto em que a circulação-controle ganham mais destaque que o simples sigilo, o consentimento expresso da pessoa ganha ainda maior relevo e centralidade.

Como consequência, a Lei de Dados Pessoais tem como base o conceito de consentimento como **"manifestação livre, informada e inequívoca pela qual o titular *concorda* com o tratamento de seus dados pessoais para uma finalidade determinada"** (Lei 13.709/2018, Art. 5º, XII).

Vale frisar: **uma concordância LIVRE, INFORMADA e INEQUÍVOCA**. ***Por consequência, nada que seja compulsório, não-informado ou dúbio é válido enquanto consentimento***. E, ao analisar a

situação concreta, essa parece ser a situação (obrigatória, sem consulta ou informação e sem consentimento do usuário).

Além disso, esse sistema de processo de tratamento de dados pessoal possui **dez princípios** positivados neste mesmo diploma legal, que são:

> I - **finalidade**: realização do tratamento para ***propósitos legítimos***, específicos, explícitos **e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, ***proporcionais e não excessivos*** em relação às finalidades do tratamento de dados;
>
> IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

> VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - **não discriminação**: ***impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos***;
>
> X - **responsabilização** e **prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A Lei nº 13.709/2018 também introduziu no ordenamento jurídico brasileiro a necessidade de satisfazer as condições impostas pelo inciso I do Art. 7º para que seja válido o tratamento de dados pessoais, em especial:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - **mediante o fornecimento de *consentimento* pelo titular**;

A própria Lei determina que o referido consentimento deverá **ser feito por escrito ou por outro meio que demonstre a manifestação da vontade do titular**, fortalecendo a autonomia dos indivíduos em face da coleta de seus dados pessoais. **Não há, portanto, consentimento "implícito", o que seria uma evidente afronta legal**.

O princípio da **"autodeterminação informativa"** e da importância do consentimento livre e informado é de notório reconhecimento doutrinário e encontra na Lei do Cadastro Positivo (Lei 12.414/2011) e no Marco Civil da Internet (Lei 12.965/2014) seu acolhimento e regramento no ordenamento jurídico pátrio. E de forma subsidiária para o caso em comento, no Código de Defesa do Consumidor (Lei 8.078/1990).

A regra do consentimento está prevista no art. 7º, XII e IX, do Marco Civil da Internet. Enquanto o inciso VII de tal artigo condiciona o fornecimento a terceiros dos dados pessoais ao consentimento livre, expresso e informado do usuário, salvo em caso de previsão legal, o inciso IX estabelece norma geral acerca do consentimento em caso de coleta, uso, **armazenamento e tratamento de dados pessoais, prevendo ainda que o consentimento deve constar de forma destacada**.

Sob a esfera do direito público, os bancos de dados e cadastros das pessoas naturais estão sob o abrigo do regime constitucional e legal da proteção da privacidade que tem como condição essencial de validade o princípio do consentimento para o armazenamento de dados pessoais cabendo ao Administrador, inclusive, a requerimento do interessado, adotar as providências necessárias para impedir ou fazer cessar ato contrário a inviolabilidade a vida privada, conforme expressamente previsto no artigo 21 do Código Civil.

Em consonância com o aqui exposto, *a geração de identificadores únicos por meio de algoritmos que fazem tratamento de dados biométricos*, como os que produzem o reconhecimento facial ou a reconstrução por um conjunto de dados identificáveis como o de reconhecimento de expressões faciais, *cujo uso se destinará para o aproveitamento de controle de acesso à instituição pública*, *viola o novo signo da privacidade do usuário se este não consentirem com tal prática*.

Dito de outro modo, **a utilização do sistema de reconhecimento facial implantado pela Administração do CEFET não pode dispensar, para sua regularidade e legalidade, do expresso consentimento do usuário**. Consentimento esse, vale repisar, é *sempre expresso*, *manifesto*, *nunca implícito ou tácito*. Ou seja, uma concordância **prévia, livre, informada e inequívoca**.

Caso contrário, a simples imposição de sistema de coleta e tratamento de dados biométricos, a exemplo do reconhecimento facial, sem aviso prévio, consulta e, principalmente, sem a concordância prévia e consentimento do usuário contraria a legislação vigente sobre o assunto.

Essas são as nossas observações para o momento.

Boechat e Wagner Advogados
Assessoria Jurídica da ADCEFET/RJ