



O DNA de Moro: o Projeto de Lei Anticrime sob a ótica da proteção dos dados pessoais

HELENA MARTINS DO RÊGO BARRETO (UFC)¹

Resumo

O trabalho lança um olhar crítico sobre o Projeto de Lei Anticrime proposto pelo governo federal brasileiro, particularmente no que tange à proteção de dados pessoais. A análise destaca duas medidas do pacote: a submissão de presos à identificação do perfil genético, mediante coleta de DNA, e a criação do Banco Nacional Multibiométrico e de Impressões Digitais. Situa o projeto no contexto do capitalismo de vigilância (ZUBOFF, 2015). A partir do diálogo com a criminologia crítica (BARATTA, 1999), aponta como estratégia para a naturalização dessa lógica a restrição da coleta de dados, pela proposta inicial, às pessoas presas. Depois, analisa aspectos jurídicos do projeto, tendo em vista especialmente a recém-aprovada Lei Geral de Dados Pessoais (LGDP). Neste ponto, são evidenciados os limites para a aplicação da legislação brasileira no campo da segurança pública, derivados das pressões que incidiram sobre sua formulação, ao passo que caminhos para a efetivação de uma visão garantista dos direitos são apontados.

Palavras-chave: Criminologia; Vigilância; Dados Pessoais.

1. Introdução

França, 1872. Como parte da política repressora que se seguiu à Comuna de Paris, de 1871, uma circular da administração penitenciária daquele país decretou que presos civis e, especialmente, condenados por fatos insurrecionais deveriam ser fotografados. Poucos anos depois, o criador do laboratório de identificação criminal baseada nas medidas do corpo humano, Alphonse Bertillon, revelou que “a fotografia é de pouca ajuda e não é mais que um meio de controle” (apud MATTELART, 2009). O discurso da defesa social permitiu que, entre 1913 e 1969, apenas estrangeiros e emigrantes estivessem sujeitos à determinação de catalogação de fotos e impressões digitais. Política discriminatória que foi utilizada também na África do Sul, especialmente durante o regime do apartheid, conforme registrado no livro “Um mundo vigiado”, de Armand Mattelart.

¹ Doutora em Comunicação Social pela Universidade de Brasília (UnB). É professora do curso de Comunicação Social – Publicidade Propaganda da Universidade Federal do Ceará (UFC). E-mail: helena.martins@ufc.br.

Os exemplos mostram como a construção do inimigo – o terrorista, o negro – pode ser usada como argumento para a naturalização de práticas de vigilância e controle de populações. Também são úteis para alertar sobre os objetivos de políticas que, justificadas pela demanda de segurança e ancoradas no argumento da neutralidade técnica, viabilizam a vigilância estatal sobre a população, a começar pelos setores estigmatizados. É dentro desse esquadro que se problematiza, neste artigo, o Projeto de Lei Anticrime, apresentado pelo ministro da Justiça e Segurança Pública (MJSP) do governo Jair Bolsonaro, Sérgio Moro, em 4 de fevereiro de 2019².

O texto determina a submissão de presos à identificação do perfil genético, mediante coleta de DNA, e a criação do Banco Nacional Multibiométrico e de Impressões Digitais, que teria *“como objetivo armazenar dados de registros biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais federais, estaduais ou distrital”* (BRASIL, 219). Tais medidas ampliariam os registros do Banco Nacional de Perfis Genéticos (BNPG), que atualmente contém 7.800 informações genéticas de vestígios de local de crime, 6.500 de condenados e 440 de investigados, de acordo com o IX Relatório da Rede Integrada de Bancos de Perfis Genéticos, publicado em novembro de 2018³.

Dados de condenados do BNPG são coletados quando há decisão judicial determinando isso, nos termos da Lei de Identificação Criminal, aprovada em 2012. Enfatizando a contribuição que a produção de mais dados daria à investigação e elucidação de crimes, em notícia produzida para pautar a proposta, o MJSP atribuiu a Moro a seguinte frase: *“Caso aprovado, não será mais necessário esperar todas as etapas recursais do julgamento para colher o DNA do condenado. O rol de pessoas inseridas no banco de dados será maior, bem como a celeridade na elucidação. As forças de segurança pública contarão com mais um instrumento de investigação”*⁴. A proposta traz à tona o cada vez mais difundido o uso de tecnologias informacionais para o campo da segurança, verificado, por exemplo, no uso de câmeras nas cidades.

Considero essencial analisar tais medidas tendo em vista tanto a crítica das tecnologias quanto o olhar da criminologia crítica sobre o sistema penal. Nesse sentido, o artigo será dividido em quatro partes, além desta introdução. Na primeira, trata do que Zuboff (2018) conceitua como capitalismo de vigilância, onde vigilância estatal e das corporações se encontram e complementam. A partir do

2A íntegra do projeto de lei está disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2192353>>. Acesso: 05 jun. 2019.

3O relatório está disponível em: <<https://www.justica.gov.br/sua-seguranca/seguranca-publica/ribpg/relatorio/ix-relatorio-da-rede-integrada-de-bancos-de-perfis-geneticos-ribpg-1.pdf/view>>. Acesso: 20 mai. 2019.

4 MJSP. Banco Nacional de Perfis Genéticos: uma ferramenta eficiente para elucidação de crimes. Brasília, 25 abr. 2019. Disponível em: <<https://www.justica.gov.br/news/collective-nitf-content-1556212211.45>>. Acesso: 20 mai. 2019.

diálogo com a criminologia crítica (BARATTA, 1999) aponta como estratégia para a naturalização dessa lógica a restrição inicial da coleta de dados às pessoas presas. A segunda parte situa a criação dos bancos de perfis genéticos. A terceira analisa aspectos jurídicos do projeto, tendo em vista especialmente a recém-aprovada Lei Geral de Dados Pessoais (LGDP), Lei nº13.709/2018. Por fim, aponta considerações para subsidiar a observação crítica das políticas de segurança desenvolvidas em associação com as novas tecnologias.

2. Uso de dados e vigilância no capitalismo hoje

Ao longo da história, diferentes formas de controle foram desenvolvidas, em geral valendo-se das tecnologias disponíveis em cada momento, de forma mais ou menos velada. No século XX, o regime de acumulação fordista baseou-se, entre outros elementos, no controle sobre os corpos das/os trabalhadoras/es, disciplinados pela rotina da fábrica. O taylorismo, chamado administração científica, introduziu tecnologias para ampliar a disciplina na administração das empresas. Simultaneamente, foram criadas ou ampliadas instituições responsáveis pela vigilância social, como polícias, prisões e manicômios.

No contexto da reestruturação produtiva do sistema capitalista dos anos 1970, houve a emergência de um novo modelo de exploração, que supera a preponderância da atividade disciplinada e hierarquizada, de cunho fordista/taylorista. Além da expropriação da força de trabalho que se expressa no corpo do/a trabalhador/a, o sistema buscou sua sujeição de forma integral, alcançando corpo e mente. Configura-se, assim, a chamada sociedade do controle, que se exerce sobre o conjunto da sociedade, de forma complementar à lógica disciplinar (SILVEIRA, 2019). A vigilância não reside em determinadas instituições que são reconhecidas como controladoras. Ela é generalizada, difusa, exercida por Estados, corporações e mesmo por outros indivíduos integrantes da sociedade.

A permanência da vigilância na história leva autores a adotar uma perspectiva neutra sobre a questão, entendendo a vigilância, conforme sintetiza Fuchs (2011: 111), “[...] *como uma qualidade ontológica de todas as sociedades ou de todas as sociedades modernas e identificam, além dos aspectos negativos, também as qualidades concretas ou em potencial da vigilância*”. Concordo com Fuchs quando critica esta abordagem e defende a adoção de uma visão negativa, nos seguintes termos:

Um conceito negativo de vigilância aponta para um aspecto negativo das estruturas de poder, das sociedades contemporâneas e das sociedades heterônomas. A maneira como se apropria da noção de vigilância denuncia e sinaliza a existência de sociedades dominantes e dominadas. Dessa forma, aponta para um caminho de emancipação e de uma sociedade sem dominantes, que é concebida como sendo uma sociedade também sem vigilância. Numa

teorização negativa, a vigilância é um conceito que está inerentemente ligado à coleta de informações para propósitos de dominação, violências e de coerção e, assim sendo, ao mesmo tempo acusa tais estados da sociedade e faz exigências políticas tendo em vista uma sociedade participativa, cooperativa e sem dominação. (FUCHS, 2111: 115)

Atualmente, caminha-se na contramão dessa proposta. O uso de dados está no centro da economia, por isso tem crescido a discussão em torno da qualificação da etapa atual como capitalismo de vigilância. Formuladora deste conceito, Shoshana Zuboff aponta que “[...] *se qualifica como uma nova lógica de acumulação, com uma nova política e relações sociais que substituem os contratos, o Estado de direito e a confiança social pela soberania do Big Other*”. De acordo com Zuboff, “[...] *essa nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado*” (2018: 49). Embora o conceito abarque proposições acerca de mudanças no trabalho atual que merecem ser problematizadas, o essencial, em minha opinião, é que ajuda a explicar a dupla dimensão da utilização dos dados no tempo presente. Primeiro, como instrumento para a tentativa de redução da aleatoriedade na realização das mercadorias, com as novas formas de definir o público-alvo, obter informações sobre suas predileções e desenvolver campanhas. Segundo, como ferramenta para vigilância e controle. Conforme Mattelart (2009: 12) no que ele chama de “era tecnoglobal”, a tendência à transformação dos cidadãos em suspeitos e, simultaneamente, em alvos personalizados do mercado está relacionada às tentativas de vigilância e controle de mentes e corpos, por parte de governos ou de corporações.

Nem todos os corpos, contudo, são objetos dessas práticas da mesma forma ou com a mesma intensidade. Sobre o sistema de justiça criminal, perspectivas críticas como a de Baratta (1999) evidenciam que o nascimento da criminologia esteve ligado ao paradigma etiológico que via o crime como condição ontológica e buscava a definição do criminoso nesses termos, incorrendo em associação com a questão racial. Ao contrário, a criminologia crítica destaca os mecanismos sociais e institucionais pelos quais são construídas inclusive as condutas consideradas desviantes, bem como são selecionados os bens protegidos e os indivíduos rotulados, servindo, sobretudo, ao controle de determinados segmentos populacionais.

O quadro do sistema brasileiro evidencia tal seleção. De acordo com dados de 2016, o Brasil possui 726 mil pessoas presas, das quais 55% têm entre 18 e 29 anos e 64% da população prisional são compostos por pessoas negras. A conduta tipificada como crime que mais leva pessoas às prisões é o tráfico de drogas, representando 28% da população carcerária total. Somados, roubos e furtos chegam a 37%. Homicídios representam 11% dos crimes, conforme o Levantamento Nacional de Informações Penitenciárias (Infopen), que mostra ainda que 75% dos presos não chegaram ao ensino

médio e menos de 1% tem graduação. São pessoas jovens, negras e pobres as que, em geral, têm sido presas no país.

Apesar de o Brasil ter, hoje, a terceira maior população carcerária do mundo e de serem frequentes os casos de conflitos relacionados à superlotação, são comuns os discursos que pregam a aplicação de medidas de restrição de liberdade e negam direitos aos detentos. Trata-se de uma conduta de desumanização dos presos, estimulada por uma criminologia midiática que consiste, segundo Zaffaroni (2014), na construção de uma imagem do real na qual estão, em lados opostos, as pessoas boas, vulneráveis, e “eles”, a massa criminosa. Isso é feito por meio da fabricação do estereótipo do criminoso, de campanhas de ‘lei e ordem’, de ideias rígidas, como a suposta impunidade dos que praticam crimes.

Ao restringir a coleta de dados sensíveis, inicialmente, às pessoas presas, a proposta que consta no Pacote Anticrime vale-se da ideia naturalizada de que os detentos não têm nem merecem direitos e são, potencialmente, reincidentes. Ao fazer tal crítica, não descarto possíveis contribuições às investigações, mas considero que os impactos negativos para determinadas populações e o objetivo de utilizar tal instrumento para controlá-las devem estar no centro da discussão da proposta, pelos riscos potenciais que envolve.

Para obter detalhes sobre a aplicação da política atualmente, para fins desta pesquisa, foram solicitadas informações ao MJSP por meio da Lei de Acesso à Informação Pública. Entre as perguntas enviadas, estavam: quantas pessoas presas, atualmente, tiveram seu DNA coletado? É possível traçar um perfil dessas pessoas? Em quais casos têm sido utilizada essa informação no Brasil? O MJSP enviou três parágrafos em resposta aos questionamentos, além de textos legais e relatório do BNPG. No texto, detalhou os procedimentos adotados para a coleta e tratamento, nos seguintes termos:

Todo laboratório participante da RIBPG [Rede Integrada de Bancos de Perfis Genéticos] tem um administrador para o banco de perfis genéticos, o qual deve garantir o sigilo dos dados armazenados. Cada perfil genético inserido na RIBPG recebe um código alfanumérico, dissociado do nome do indivíduo, de acordo com os protocolos de procedimentos internos de cada laboratório de genética forense. Ou seja, o perfil genético trata-se de um dado dissociado de uma pessoa identificável. Desta forma, trata-se de dados não associados a uma pessoa identificável, por terem sido substituídas, ou dissociadas pela utilização de um código, todas as informações que permitiam identificar essa pessoa. O analista do banco de perfis genéticos, perito oficial com formação e treinamento para a realização de exames de DNA, será responsável pelos perfis genéticos por ele inseridos. O cadastramento de analistas é controlado pelo administrador. Os administradores dos bancos de perfis genéticos estadual, distrital e federal serão o ponto central de contato entre os laboratórios participantes da RIBPG e o administrador do BNPG. Na ocorrência de uma coincidência, os administradores são notificados para que busquem em sua base de controle a qual caso de local de crime se refere aquele perfil de vestígio ou a qual pessoa se refere aquele perfil de referência. (MJSP, 2019: Processo nº 0885002437201905).

O fato de se utilizar um código e não o nome da pessoa cujo DNA é armazenado reduz o caráter persecutório da política. Não obstante, não impede a possibilidade de acesso a tal informação e, com isso, sua utilização, o que a resposta do órgão não pontua. Se aprovado o Projeto de Lei Anticrime, a prática pode ser ampliada, tendo em vista que o texto fixa que qualquer autoridade policial e o Ministério Público poderão requerer ao juiz, no caso de inquérito ou ação penal instauradas, o acesso às informações.

Neste ponto, três argumentos devem ser mencionados. Primeiro, supõe-se que a utilização desses dados será estimulada, tanto pelas promessas de resolução de investigações quanto pela própria lógica dos bancos de dados, que são “[...] *em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações*” (DONEDA, 2011: 92). Segundo, sabendo-se da seletividade do sistema, pode-se supor que alguns perfis populacionais, como pessoas negras, tenham seus dados mais facilmente solicitados. Depois, são muitas as deficiências técnicas dessas instituições, sobretudo no trato com as novas tecnologias, o que poderá resultar em vazamentos e uso abusivo das informações. Ressalte-se que o DNA é uma informação única, que não pode ser alterada ao longo da vida. Com o avanço das pesquisas genéticas, outras informações têm sido produzidas a partir dele, a exemplo da identificação de possíveis doenças. De posse desses dados, investigações podem levar à produção de pesquisas que busquem identificar padrões e perfis de pessoas.

3. Bancos de perfis genéticos e a controvérsia sobre sua adoção no Brasil

Essa possibilidade faz recordar teses lombrosianas de classificação de criminosos a partir da análise de suas características corporais e psicológicas. Acreditava-se que a categorização levaria à identificação prévia daqueles que poderiam vir a ser criminosos. A aceitação desses preceitos levou ao desenvolvimento de tecnologias de identificação e administração de registros históricos de crimes, como condenações e fichas com históricos, além de medidas extremas como a tentativa de eliminação de populações inteiras pelo regime nazista (RITCHER, 2016).

Os primeiros arquivos criminais foram organizados a partir do registro dos casos e não das características dos indivíduos, o que Ritcher aponta ter sido alterado devido à dificuldade de se viabilizar o acesso às informações requeridas por juízes e policiais e de vinculá-las para viabilizar

ligação de suspeitos a crimes anteriores. Como resposta a esses problemas, foi desenvolvida e sistematizada a antropometria, a partir do trabalho de Bertillon, que dava continuidade à identificação negativa. Como mecanismo de eliminação, o método era incapaz de “[...] *atender uma das principais motivações que impulsionavam as pesquisas em torno das técnicas de identificação criminal: a capacidade de produzir prova positiva de uma identidade individual, uma marca ou uma característica do corpo que possibilitaria ligar um indivíduo a um fato, um crime ou a uma história*” (Ibidem: 70). Esse tipo de identificação só foi possível com o sistema de notação de impressões digitais e, depois, com os bancos de dados de DNA (Ibidem: 100).

Estes superaram dificuldades de se acessar e buscar correspondências nos sistemas de impressões. Isto porque o desenvolvimento dos bancos acompanhou o do *big data*, que consiste na utilização de algoritmos e de tecnologias de tratamento de grande quantidade de dados – o que permite ampliação da coleta e da verificação, tornando viável, potencialmente, o registro de toda a população. A mesma lógica orienta o banco de perfil genético, pois já que opera através do cálculo de probabilidades de combinações, “[...] *quanto mais dados armazenados estiverem disponíveis no banco de perfis maiores tornam-se as possibilidades de combinação dos dados (DNA encontrado na cena do crime x DNA armazenado nos bancos), elevando-se o grau de segurança da resposta matemática*” (VIEIRA; RODRIGUES, 2016: 201).

Testes de identificação genética começaram a ser efetivados pelo Federal Bureau of Investigation (FBI) em meados dos anos 1980. Para o que interessa aqui, é importante considerar que “*a possibilidade da coleta de amostras de cenas de crimes serem inseridas em um banco de dados, no qual buscas por correspondências (matches) pudessem ser realizadas, viria para fornecer suspeitos à polícia ou informar outros crimes que um suspeito já conhecido pudesse estar envolvido*” (RITCHER, 2016: 97).

No Brasil, a identificação por meio de DNA teve início em 1994, no Distrito Federal, que concentrou suas atividades nos testes de paternidade; nos estados, a genética forense foi desenvolvida em laboratórios particulares ou universidades com o mesmo fim. O uso foi ampliado nos anos 2000, com tentativas de incluir o DNA entre as técnicas de identificação nos institutos de perícia. Proposta de regulamentação foi apresentada ao Congresso em 2003, pois estavam previstas apenas técnicas de fotografia e datiloscopia, mas nunca foi aprovada (RITCHER, 2016: 107). Seis anos depois, o FBI firmou acordo com a Polícia Federal para conceder o Combined DNA Index System (CODIS), sistema

de armazenamento e cruzamento de informações genéticas adotado por todos os estados norte-americanos desde 2004. Com a parceria:

O projeto de criar uma Rede Integrada de Bancos de Perfis Genéticos composta pelos laboratórios dos estados brasileiros passou a ser alentado com maior vigor. Essa rede de bancos de dados seria a condição para que a identificação através dos perfis genéticos, pudesse ser utilizada para além dos “casos fechados”. Os bancos permitiriam, então, fornecer “suspeitos” caso a polícia não tivesse nenhuma pista sobre quem procurar e fossem encontradas correspondências no banco. (RITCHER, 2016: 109-110).

A inclusão do DNA foi legalizada pela Lei nº 12.654, que instituiu a criação de banco de dados com perfil genético a partir da extração obrigatória de DNA de criminosos condenados por crimes praticados dolosamente, com violência de natureza grave contra pessoa ou hediondos. A lei determinou que as informações “não poderão revelar traços somáticos ou comportamentais das pessoas, exceto determinação genética de gênero”, fixou que os dados “*deverão ser armazenados em banco de dados de perfis genéticos, gerenciado por unidade oficial de perícia criminal*” e que “*terão caráter sigiloso, respondendo civil, penal e administrativamente aquele que permitir ou promover sua utilização para fins diversos dos previstos nesta Lei ou em decisão judicial*”.

O banco foi regulamentado pelo Decreto nº7.950/2013, que instituiu o BNPG e a RIBPG. Sua constitucionalidade é alvo de questionamento no Supremo Tribunal Federal (STF), por haver entendimento de que consiste em produção de prova contra si mesmo, o que contraria a Constituição. Ainda assim, segundo o IX Relatório da Rede Integrada de Bancos de Perfis Genéticos (2018: 14) houve crescimento do número total de perfis genéticos no BNPG de 2.584 registros, em novembro de 2014, para 18.080, em novembro de 2018. No relatório, consta que “*a estatística para reincidência de crimes graves contra a pessoa e de crimes hediondos é superior a 50%. Além disto, o índice de homicídios esclarecidos no Brasil não ultrapassa 10% dos casos, o que sugere a necessidade urgente do implemento de outros meios para a investigação, como a utilização de bancos de perfis genéticos*” (Ibidem: 43).

Considerada subutilizada, o documento expõe expectativa de que a captura de informações leve à resolução desses problemas, o que imputa suspeição aos detentos. Diante de tal quadro, registra que o planejamento estratégico do MJSP para o quinquênio 2015-2019 “[...]previu como meta estratégica para redução de homicídios no Brasil, o aumento do número de coletas de material biológico para 50% dos condenados conforme Lei nº12.654/12” (Ibidem: 9). O texto reforça que o aumento objetiva “[...] auxiliar a resolução de crimes e evitar novos delitos, além de proteger

inocentes injustamente acusados” (Ibidem: 23). É nesse contexto que se insere o projeto apresentado por Sérgio Moro em 2019.

4. O Pacote Anticrime analisado sob a ótica da proteção dos dados pessoais

No Brasil, até não havia regra que tratasse detalhadamente da proteção dos dados pessoais. A tutela tinha como fundamento a Constituição Federal, que determina a proteção da personalidade e reconhece o direito à privacidade, considerando invioláveis a vida privada e a intimidade e também o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, para fins de investigação criminal ou instrução processual penal (artigo 5º, XII). Na legislação infraconstitucional, o Código de Defesa do Consumidor estabelece direitos e garantias para o consumidor em relação às suas informações pessoais presentes em bancos de dados e cadastros.

Nova referência à proteção de dados foi feita no Marco Civil da Internet (Lei nº12.965/2014), que dispõe que a disciplina do uso da internet no Brasil tem com um dos princípios a “proteção dos dados pessoais, na forma da lei”. A inclusão desse dispositivo ampliou a pressão para a criação de norma específica, a qual vinha sendo discutida pelo Ministério da Justiça desde 2007. Em 2011 e em 2015, a pasta efetivou consultas públicas sobre o sobre o Anteprojeto de Lei de Proteção de Dados Pessoais. No Congresso Nacional, diversas audiências públicas versaram sobre o tema, que também foi objeto da campanha “Seus dados são você”, iniciada em 2017 por um conjunto de organizações da sociedade civil organizadas em torno da Coalizão Direitos na Rede.

Ao longo dos anos de debate sobre a Lei Geral de Proteção de Dados Pessoais, finalmente aprovada em agosto de 2018, amadureceu-se como central a necessidade de consentimento da pessoa detentora do dado para o tratamento dele, o que significa que o titular deverá manifestar de forma livre, informada e inequívoca que concorda com o tratamento de seus dados pessoais – e apenas para uma finalidade determinada. Houve, pois, a consolidação da visão garantista presente em outras normas, como na General Data Protection Regulation (GDPR) na União Europeia, que influenciou as discussões no Brasil.

No caso da Lei Geral de Proteção de Dados Pessoais brasileira, ela está fundamentada, conforme o artigo 2º, no respeito à privacidade; na autodeterminação informativa; na liberdade de expressão, de informação, de comunicação e de opinião; na inviolabilidade da intimidade, da honra e da imagem; no desenvolvimento econômico e tecnológico e a inovação; na livre iniciativa, a livre concorrência e a

defesa do consumidor; e nos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. De acordo com o artigo 6º, as atividades de tratamento de dados pessoais deverão observar a boa-fé e dez princípios explicitados no texto, entre os quais merecem ser destacados, para fins deste trabalho: finalidade do tratamento dos dados para propósitos legítimos, específicos, explícitos e informados ao titular; necessidade, que consiste na limitação do tratamento ao mínimo necessário; livre acesso, que é a garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; e segurança, definida como a 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.

A regra, que entrará em vigor em agosto de 2020, após término de dois anos para adaptação e implementação de suas medidas, dispõe que o cidadão tem o direito a obter, a qualquer momento, informação das entidades públicas e privadas com as quais o controlador dos dados, como uma plataforma de rede social, realizou uso compartilhado de dados. Motivada pela preocupação com a segurança deles, detalha ainda, em um capítulo específico, regras para a transferência internacional de informações pessoais, ação que é limitada a poucas situações e cuja concretização só pode ocorrer para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais, medida que deverá ser avaliada pela autoridade nacional de proteção de dados.

A lei, contudo, não se aplica ao tratamento de dados para fins exclusivo segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais (artigo 4º). Não obstante pressões terem levado à fixação dessas exceções, o parágrafo primeiro do mesmo artigo que as apresenta dispõe que o tratamento de dados pessoais em tais casos “[...] *será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei*”. Há, assim, a orientação para a utilização parcimoniosa mesmo em relação à segurança, que também fica submetida aos princípios gerais mencionados anteriormente e aos direitos do titular, entre eles o acesso facilitado às informações sobre o tratamento de seus dados (artigo 9º).

A lei aprovada em agosto previa que a Autoridade Nacional deveria emitir opiniões técnicas ou recomendações referentes às exceções e que solicitaria aos responsáveis relatórios de impacto à proteção de dados pessoais, ponto vetado pelo então presidente Michel Temer. O texto original

também estabelecia que “em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado”, no que foi alterado pela Medida Provisória (MP) 869, de dezembro de 2018. A redação dada pela MP é mais flexível. Diz o texto já convertido em lei: *“os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do caput não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público”* (artigo 4º, § 3º).

A mesma permissividade para a ampla utilização de dados pessoais que guiou as alterações propostas pelo governo Temer podem ser verificadas no Pacote Anticrime. Embora a coleta de DNA ainda seja objeto de discussão no STF, ele previu a aplicação da medida a todos os condenados por crimes dolosos, inclusive aqueles cometidos sem violência. Na prática, uma pessoa acusada da prática de furto, condenada por um juiz de primeira instância, terá seu DNA coletado e armazenado pelo Estado. A medida será aplicada também em casos em sem trânsito em julgado da sentença condenatória, o que significa que presos provisórios terão que conceder ao Estado dados pessoais extremamente sensíveis para viabilizar seu tratamento como potenciais suspeitas de quaisquer novos crimes que a polícia esteja investigando.

O disposto contraria o princípio da presunção de inocência, expressamente afirmado na Constituição Federal, em seu artigo 5º, inciso LVII, onde está proclamado que “ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória”. A Carta Magna ressaltou o direito de não autoincriminação, o que permite, por exemplo, o direito ao silêncio. No inciso LVIII, determina que “o civilmente identificado não será submetido a identificação criminal, salvo nas hipóteses previstas em lei” - no que foi regulamentada pela Lei Nº 12.037, que passou a fazer referência à coleta de DNA após a aprovação da Lei nº12.654 de 2012. Ainda assim, a coleta de material biológico fica restrita, nos termos do inciso IV do art. 3º, em casos em que “[...] *for essencial às investigações policiais, segundo despacho da autoridade judiciária competente, que decidirá de ofício ou mediante representação da autoridade policial, do Ministério Público ou da defesa*”.

A norma deixa claro, ainda no artigo 5º-A, § 1º, que *“as informações genéticas contidas nos bancos de dados de perfis genéticos não poderão revelar traços somáticos ou comportamentais das pessoas, exceto determinação genética de gênero, consoante as normas constitucionais e internacionais sobre direitos humanos, genoma humano e dados genéticos”*. Tendo em vista que o projeto propõe que “o

Banco Nacional Multibiométrico e de Impressões Digitais será integrado pelos registros biométricos, de impressões digitais, íris, face e voz colhidos em investigações criminais ou por ocasião da identificação criminal”, nos termos do no artigo 7º-A, § 2º, vê-se que ele vai além do que permite a lei, já que dados como íris podem revelar dados somáticos. Associados e manipulados, também comportamentais.

O texto do projeto determina que a exclusão só ocorrerá em caso de absolvição do acusado ou decorridos vinte anos após o cumprimento da pena. Não há informações sobre como esses dados serão, de fato, armazenados e tratados, sendo prevista apenas posterior regulamentação do Banco Nacional Multibiométrico por parte do Executivo. Outro problema é o fato de o Brasil não ter, hoje, uma política de guarda soberana dos dados de DNA coletados. Ao buscar informações acerca deste ponto junto ao MJSP, questionei: *“Informações veiculadas pela imprensa apontam que os perfis genéticos são, hoje, armazenados no exterior, em um banco de dados criado pelo FBI. Há acordo de cooperação entre Brasil e Estados Unidos para regular esse processo? Se sim, onde pode ser visualizado?”*. Em resposta, o órgão confirmou que a RIBPG utiliza o CODIS e detalhou que o programa é cedido gratuitamente pelos Estados Unidos. Não fez referência, contudo, a acordo, limitando-se a apontar que *“este programa é utilizado por mais de 34 países, sendo a principal ferramenta a nível mundial de banco de perfis genéticos. Apesar do uso disseminado em outros países, as informações entre os países não são compartilhadas por meio do CODIS”*.

Outro ponto importante do Pacote Anticrime é a forma como trata da proteção dos dados. De acordo com Doneda (2011: 93), com os bancos de dados *“aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo”*, daí porque o autor reforça a observância dos princípios referidos anteriormente na efetivação dos bancos. O texto em análise, embora apresentado após a aprovação da Lei Geral de Dados Pessoais e, nesse processo, da ampliação da discussão no âmbito da sociedade brasileira acerca da necessidade de uma abordagem garantista dos direitos no tratamento dos dados, não aponta mecanismos que garantam transparência nos procedimentos de tratamento e proteção dos dados sensíveis a serem coletados e abre espaço para o uso indiscriminado e pouco seguro deles, pois, conforme citado, permite que autoridade policial e Ministério Público solicitem tais informações.

Por meio da Lei de Acesso à Informação, também questionei o MJSP se as pessoas que têm os dados coletados para o BNPG têm ou podem ter acesso às informações sobre o tratamento dessas

informações e se as informações obtidas podem ser utilizadas por agentes privados, por exemplo empresas de segurança. Nas respostas enviadas pelo órgão, contudo, não foram feitas referências a isso. Quanto ao uso por agentes privados, caso ocorra, essa prática pode ser lida como uma postura que, ainda que permissiva, encontra respaldo legal, pois a LGPD veda o compartilhamento de dados sensíveis, com exceção de “[...] *dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos*” (artigo 11, II, “b”).

Apesar de não falar abertamente sobre tais procedimentos, o governo federal está propondo que a submissão das informações seja obrigatória. Caso o condenado se negue a fazer a conceder a identificação do perfil genético, terá, pelo texto do projeto, cometido “falta grave”, o que pode acarretar a regressão do regime prisional e alterar a data-base para a concessão de novos benefícios.

Considerações finais

Pelo exposto até aqui, é possível apontar que a ampliação da coleta e da utilização de dados biométricos para fins de segurança pública pode significar reforço à lógica vigilantista que marca o momento atual do capitalismo, a nível mundial, bem como à seletividade característica do sistema penal. Esses processos se encontram porque a proposta de submeter obrigatoriamente pessoas presas à coleta ajuda a naturalizar a adoção dessas medidas, tendo em vista o que o país tem tratado, em geral, pessoas privadas de liberdade de forma desumanizada e, na esteira disso, desprovidas de qualquer direito.

Em relação à análise da proposta à luz da Lei Geral de Proteção de Dados Pessoais, vê-se que há relativização do direito à proteção de dados em matéria de segurança pública, já que a regra internalizou dispositivos que fragilizam a abordagem restritiva do uso de dados e garantista em relação aos direitos no caso de sua aplicação para ações na área da segurança pública, o que evidencia limites à contenção do vigilantismo citado anteriormente, ainda que em um setor já tão suscetível a práticas discriminatórias e pouco transparentes.

Não obstante, apesar dessas fragilidades, é importante ter em vista que os princípios gerais da lei devem ser observados e que há parâmetros, estabelecidos pelo artigo 23 da norma, para o tratamento de dados pessoais pelo poder público, como a submissão à finalidade pública, norteadas pelo interesse público e com o objetivo de executar competências legais ou atribuições legais do serviço público. Essas observações devem ser especialmente consideradas no caso dos registros biométricos, por serem dados sensíveis. Por fim, a autorização genérica para o uso de dados pessoais

na segurança pública pode ser contida por lei específica, conforme consta na lei geral em relação à segurança, o que pode contribuir para superar os limites da LGPD no que tange à área e democratizar as discussões e práticas relacionadas a ela.

Referências

BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal: introdução à sociologia do direito penal**. Rio de Janeiro: Revan, 1999.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988.

._____**Lei nº 12.96 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil .

._____**Lei nº13.709 de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº ,12.965 de 23 de abril de 2014 (Marco Civil da Internet).

._____**Medida Provisória nº 869 de 27 de dezembro de 2018**. Altera a Lei nº ,13.709 de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados.

DONEDA, Danil. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FUCHS, Christian. **Como podemos definir vigilância?** MATRIZES,1,109-135. São Paulo, 2011.

MATTELART, Armand. **Um mundo vigilado**. Madri: Paidós, 2009.

RICHTER, Vitor Simonis. **Identificação Genética e Crime: a introdução dos bancos de DNA no Brasil**. Tese de Doutorado apresentada no Programa de Pós-graduação em Antropologia Social da Universidade Federal do Rio Grande do Sul, 200páginas, Porto Alegre,2016.

SILVEIRA, Sérgio Amadeu. **A noção de modulação e os sistemas algorítmicos**. In: Souza, Joyce et al (orgs). A sociedade de controle: manipulação e modulação nas redes digitais (31 – 46). São Paulo: Hedra, 2018.

VIEIRA, Caroline; RODRIGUES, Celso. **Práticas de controle social na era do pós-panoptismo: análise do Banco de Dados Genéticos**. Justiça & sociedade. Revista do Curso de Direito do Centro Universitário Metodista – IPA. São Paulo: Metodista.V.1, n.1, 2016.

ZAFFARONI, Eugenio Raúl; BIANCHINI, Alice; GOMES, Luiz Flávio (Coord.). **A palavra dos mortos: conferências de criminologia cautelar**. (Saberes críticos). São Paulo: Saraiva, 2014.

ZUBOFF, Shoshana (2015). **Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação**. In: Bruno, Fernanda et al (orgs.). Tecnopóliticas da vigilância: perspectivas da margem (p. 17 – 68). São Paulo: Boitempo, 2018.