REVISTA BRASILEIRA DE SEGURANÇA PÚBLICA

Volume 13

Número 1

Fevereiro/Março de 2019

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA

ISSN 1981-1659

Expediente

Esta é uma publicação semestral do Fórum Brasileiro de Segurança Pública
ISSN 1981-1659

Rev. bras. segur. pública vol. 13 n.1 São Paulo fevereiro/março 2019

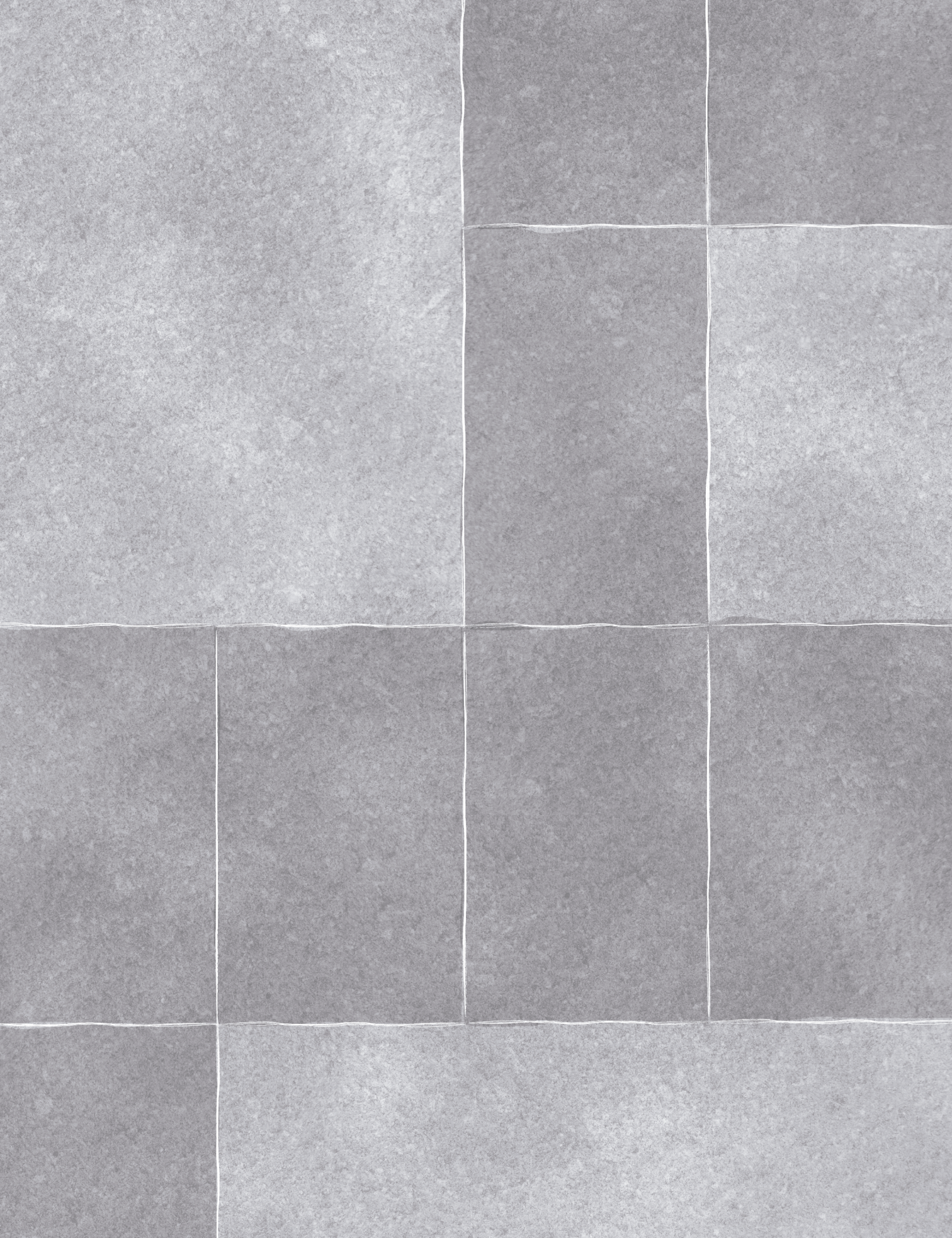
Endereço
Rua Amália de Noronha, 151, Cj. 405
Pinheiros, São Paulo - SP - Brasil - 05410-010

Telefone
(11) 3081-0925

E-mail
revista@forumseguranca.org.br

Apoio
Open Society Foundations e Ford Foundation.

Fórum Brasileiro de Segurança Pública



"Onde eles estavam na hora do crime?": Ilegalidades no tratamento de dados pessoais na monitoração eletrônica

Victor Martins Pimenta

Doutorando em Direito e mestre em Direitos Humanos e Cidadania - UnB. Pesquisador do Laboratório de Gestão de Políticas Penais e do Centro e Centro de Estudos em Desigualdade e Discriminação - UnB. Graduado em Direito - USP e em Ciência Política - UnB. Foi Coordenador-Geral de Alternativas Penais do Ministério da Justiça.

Izabella Lacerda Pimenta

Doutora e mestre em Antropologia – UFF e pesquisadora visitante do Departament of Criminology - University of Ottawa. Pesquisadora do InEAC – INCT e NUFEP. Atua como consultora do PNUD/ONU junto ao DEPEN, no tema da monitoração eletrônica de pessoas.

Danilo Cesar Maganhoto Doneda

Professor visitante na Faculdade de Direito, Doutor e mestre em Direito - UERJ. Bacharel em Direito - UFPR. Foi Coordenador-Geral de Estudos e Monitoramento de Mercado - Senacon. Foi pesquisador visitante na Università degli Studi di Camerino e na Autorità Garante per la Protezione dei Dati Personali, ambas na Itália.

Data de recebimento: *05/01/2018*
Data de aprovação: *07/02/2019*

DOI: *10.31060/rbsp.2019.v13.n1.891*

Resumo

O presente artigo aborda o tema da proteção e tratamento de dados pessoais sensíveis no âmbito dos serviços de monitoração eletrônica de pessoas, indicando a existência de práticas discriminatórias ilegais, sobretudo no compartilhamento de dados com instituições policiais, que ampliam a sujeição de pessoas monitoradas eletronicamente à estigmatização e a novos processos de criminalização. São considerados dados oficiais sobre monitoração eletrônica, normativos nacionais e internacionais sobre o tema e referências sociológicas e da criminologia crítica. A análise se valeu de diálogos com especialistas, gestores, servidores e pessoas monitoradas, bem como de observação em visitas a Centrais de Monitoração Eletrônica em diversas Unidades Federativas entre 2015 e 2018.

Palavras -Chave

Monitoração eletrônica; Proteção de dados pessoais; Sistema de justiça criminal.

Abstract

"Where were they when the crime happened?": illegal practices regarding the treatment of personal data collected from electronic monitoring services

This paper addresses the issue of protection and treatment of sensitive personal data related to electronic monitoring services, indicating illegal discriminatory practices, especially in sharing data with police institutions, which increase the subjection of persons monitored electronically to stigmatization and new criminalization processes. The analysis considers official data on electronic monitoring published by the National Penitentiary Department, national and international regulations on the subject, sociological and critical criminology references, as well as data obtained from field research, including visits and observation of work routines in Electronic Monitoring Centers of several States in Brazil between the years of 2015 and 2018.

Keywords

Electronic monitoring; Personal data protection; Criminal justice system.

Referências para análise das práticas na monitoração eletrônica à luz do direito à proteção de dados pessoais

Violações aos direitos de privacidade e o tratamento inadequado de dados pessoais podem resultar em situações de maior vulnerabilidade social e criminal das pessoas monitoradas eletronicamente. O desrespeito a esses direitos amplia a sujeição dessas pessoas ao controle policial, expondo e reforçando sua condição de indivíduos condenados ou processados criminalmente. Pode, ainda, reforçar os processos de rotulação (BECKER, 2008) e de estigmatização (GOFFMAN, 1988) das pessoas monitoradas eletronicamente, substanciando-as e reduzindo-as em "criminosas", "delinquentes", "perigosas", com impacto em sua trajetória, acesso a direitos e dignidade.

Para expor essas dinâmicas, voltamos o olhar aos fluxos de informações e procedimentos estabelecidos entre as diferentes agências penais e instituições de segurança pública (centrais de monitoração eletrônica, sistema de justiça, polícias). Apontamos o *modus operandi* que amplia a possibilidade de pessoas monitoradas serem submetidas a novos processos de criminalização, ao exercer sobre elas uma força centrípeta que as atrai constantemente em direção ao sistema penal ou até mesmo à prisão (PIMENTA, 2016).

Os dados empíricos que embasam a presente análise foram construídos a partir de observação em visitas a centrais de monitoração eletrônica de diversas Unidades Federativas e de diálogos com especialistas, gestores, servidores atuantes nas centrais e pessoas monitoradas, entre o segundo semestre de 2015 e o primeiro semestre de 2018. Partindo dessa realidade empírica, analisamos como o tratamento de dados pessoais sensíveis das pessoas monitoradas no Brasil facilita ou mesmo promove práticas discriminatórias ilegais e inconstitucionais. Para tanto, consideramos, sobretudo, o compartilhamento de dados com instituições policiais, ampliando processos de estigmatização e favorecendo novos processos de criminalização.

A discussão dos achados considera o disposto na Lei de Proteção de Dados Pessoais (Lei nº 13.709/2018), bem como as alterações trazidas pela Medida Provisória nº 869, de 27 de dezembro de 2018. Se, por um lado, a MP nº 869/2018 introduz a figura da Autoridade Nacional de Proteção de Dados (ANPD), anteriormente vetada pela Presidência da República, por outro lado o órgão foi previsto sem a autonomia necessária para o desenvolvimento

adequado de suas funções, destacando-se, ainda, os limites de referida lei para a proteção dos dados de pessoas monitoradas eletronicamente.

Também são considerados repertórios e conceitos trazidos pelo Regulamento Geral sobre Proteção de Dados da União Europeia (Regulamento 2016/679), que, em vários pontos, orientam a Lei de Proteção de Dados Pessoais brasileira. Igualmente, toma-se como referência normativa a Constituição Federal de 1988, principalmente no que se refere às garantias quanto a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (Art. 5º, X), o que amplia a responsabilidade do Poder Público acerca do assunto em tela. A necessidade de dar cumprimento aos preceitos constitucionais exige o estabelecimento de protocolos, nos diferentes campos da vida social, para assegurar o respeito a garantias constitucionais e, no caso, a devida proteção dos dados pessoais sensíveis.

A proteção de dados pessoais, mais do que uma extensão de garantias referentes ao sigilo ou segredo, constitui instrumento necessário e indispensável para que a pessoa possa garantir a integridade e o livre desenvolvimento da própria personalidade. Em uma dinâmica social na qual somos cotidianamente submetidos a processos de avaliação e monitoramento e, até mesmo, somos identificados perante diversos atores a partir de nossos dados, o controle e a transparência da forma pela qual estes dados são obtidos e utilizados são cruciais (DONEDA, 2006, 2010).

A proteção desses dados importa não somente para a garantia da privacidade, mas para quase qualquer aspecto da interação social (DONEDA, 2011). Por este motivo, hoje, cerca de 121 países têm em suas legislações normas específicas sobre proteção de dados pessoais (GREENLEAF, 2017), de forma a garantir aos seus cidadãos direitos e transparência sobre a utilização de seus dados.

Determinados dados pessoais ensejam proteção especial – são os dados pessoais sensíveis, como define a legislação nacional. Estes são entendidos como sensíveis porque contêm informações que oferecem potenciais riscos de uso discriminatório ou lesivo, de caráter individual ou coletivo. Ainda que as restrições relacionadas ao tratamento de dados pessoais sensíveis variem conforme o país, há significativo consenso de que são necessários cuidados especiais em sua coleta, utilização ou redistribuição, como indica o Regulamento Geral sobre Proteção de Dados da União Europeia (2016/679). Assim, dados pessoais sensíveis, como pontua a Lei nº 13.709/2018, são aqueles que contêm informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Ou seja, tais dados pessoais são sensíveis pois – a depender da forma como utilizados – podem sujeitar seus titulares a tratamentos discriminatórios e, até mesmo, em contextos específicos, a riscos contra a integridade física ou a vida.

Entre os princípios que informam a proteção de dados pessoais, interessa ao presente artigo especialmente os princípios da finalidade, adequação e não

discriminação, amplamente difundidos na legislação internacional que trata do tema e igualmente incorporados à Lei nº 13.709/2018, Art. 6º:

> 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;
> [...]
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

No tópico a seguir, apresentamos uma visão geral sobre a monitoração eletrônica no Brasil e indicamos como as práticas estabelecidas nesses serviços se relacionam com o direito à proteção de dados pessoais.

Serviços de monitoração eletrônica e tratamento de dados pessoais

A monitoração eletrônica de pessoas é um mecanismo de controle disciplinar próprio do campo penal, que utiliza meios técnicos – tornozeleira eletrônica, *softwares* e demais dispositivos – para vigilância indireta e contínua de indivíduos. Para tanto, são utilizadas tecnologias capazes de informar a geolocalização das pessoas monitoradas em "tempo real", geralmente a partir de sinais de GPS e de telefonia móvel, indicando localidades geográficas – áreas de inclusão e exclusão – nas quais um indivíduo tem ou não a permissão para entrar e permanecer de acordo com prescrição judicial. A pessoa indiciada ou condenada passa, então, a ter restrições em sua liberdade, sendo observada – "monitorada" – por uma central de monitoração eletrônica (BRASIL, 2017b, 2018c; PIMENTA, I.L., 2018).

Os serviços de monitoração eletrônica realizam, necessariamente, o tratamento de dados pessoais. Quando um juiz determina a aplicação da medida de monitoração eletrônica, com a colocação da tornozeleira eletrônica em uma pessoa em cumprimento de pena ou de medida cautelar diversa da prisão, a central de monitoração deve adotar providências para o cumprimento de procedimentos e regras descritos na decisão judicial. Entre eles, está a coleta de dados pessoais da pessoa monitorada (nome, endereço de residência e de trabalho, dados de contato telefônico e/ou eletrônico, fotografia, entre outros, além da geolocalização em tempo real). Em muitos casos, também são coletados dados pessoais de familiares ou amigos, que poderão ser contatados em casos de incidentes de violação das condições determinadas pelo juiz. Tais dados são importantes para a comunicação voltada ao reestabelecimento do regular cumprimento da medida de monitoração, impedindo que incidentes (como uma saída ocasional da área de inclusão) sejam caracterizados como descumprimento da decisão judicial, o que geralmente gera repercussão negativa para a pessoa monitorada, podendo resultar, inclusive, na sua prisão.

Assim, a coleta e demais ações de tratamento de dados pessoais decorrem do próprio instituto da monitoração eletrônica previsto em lei. Há respaldo normativo para o tratamento dos dados, desde que restrito à finalidade da coleta, conforme

explicitado no Decreto nº 7.627/2011, bem como na Resolução nº 213/2015 do Conselho Nacional de Justiça (CNJ) e na Resolução nº 5/2017 do Conselho Nacional de Política Criminal e Penitenciária (CNPCP)[1], conforme detalharemos adiante. Os dados de geolocalização, por exemplo, são utilizados para acompanhar o regular cumprimento de uma prisão domiciliar ou uma medida de proibição de aproximação com a mulher prevista na Lei nº 11.340/2006 – Lei Maria da Penha. Já os dados de contato, especialmente o número de telefone, são necessários para estabelecimento de diálogo entre a central e a pessoa monitorada, esclarecendo aspectos sobre o descarregamento de bateria, descumprimento de áreas de exclusão ou avisos para comparecimento presencial, quando necessário.

Ainda que o tratamento de dados pessoais seja imprescindível ao funcionamento dos serviços de monitoração eletrônica, é preciso ter em conta que estamos diante de dados pessoais sensíveis. A mera informação de que uma pessoa está sendo monitorada eletronicamente, em virtude de determinação judicial, apresenta forte potencial lesivo e discriminatório (BRASIL, 2016). Isso se aplica para pessoas monitoradas com ou sem condenação judicial.

A tornozeleira eletrônica imputa à pessoa monitorada o estigma (GOFFMAN, 1988), que por si só pode ser tomado como um fator de desigualação social para baixo, altamente degradante, considerando que vivemos numa sociedade majoritariamente orientada por valores e práticas que condenam moralmente e reprimem qualquer símbolo ou signo vinculado ao cárcere. Mesmo que a pessoa monitorada não esteja "trancada" numa instituição penal ou sequer tenha sido condenada, como no caso das medidas cautelares diversas da prisão, ela está igualmente sujeita a dicotomias totalizantes – "preso", "condenado", "custodiado", "monitorado" x "cidadão", "trabalhador", "homem de bem" – que são criadas e disseminadas para "colocar cada um no seu lugar e lá mantê-lo" (PIMENTA, I.L., 2014).

A proteção de dados das pessoas monitoradas é condição, assim, para minimizar o tamanho e o alcance social dessa marca e desse estigma. Em qualquer tempo, durante ou após a medida de monitoração, o simples fato de ter sido monitorado é potencialmente lesivo e discriminatório. Isso já é suficiente para gerar constrangimentos injustificados, impedir ou dificultar, por exemplo, a inserção no mercado de trabalho e o acesso a serviços públicos ou espaços privados de uso coletivo, conforme indicam os relatos dos gestores das centrais e das pessoas monitoradas. Logo, dados pessoais utilizados na monitoração eletrônica são sensíveis por natureza, pois podem ensejar discriminação e tratamento degradante às pessoas monitoradas.

Em particular, a utilização de informação sobre a localização geográfica de uma pessoa é notadamente um dado sensível, podendo ser entendido como um dado cujo tratamento é sensível justamente

1 *O documento oficial do Departamento Penitenciário Nacional que orienta a política de monitoração eletrônica (BRASIL, 2017b) igualmente informa a necessidade e o dever do Poder Público na proteção e no tratamento de dados pessoais sensíveis das pessoas monitoradas, especificando esses procedimentos através de princípios, diretrizes e regras.*

por proporcionar um panorama extremamente esmiuçado sobre os deslocamentos físicos de uma pessoa, a partir do qual podem ser inferidos seus hábitos, relacionamentos, preferências e uma série de outras ilações – inclusive podendo comprometer a sua segurança física. Esses dados interessam a atores e instituições com propósitos distintos dos serviços de monitoração, podendo servir como uma "moeda de troca" altamente valorizada no mercado de banco de dados ou mesmo facilitar ações direcionadas a pessoas monitoradas. Facilitam-se, assim, perseguições motivadas por razões pessoais ou coletivas, como no caso das polícias que trabalham com metas de prisão como indicador de qualidade e produtividade (BRASIL, 2015b, 2017b).

O tratamento de dados nos serviços de monitoração eletrônica não tem implicação apenas para as pessoas monitoradas eletronicamente, mas também para seus familiares, amigos ou outras pessoas que possam ter dados pessoais coletados, como informações de contato utilizados em casos de incidentes no cumprimento das medidas. Especialmente no caso da utilização da monitoração eletrônica aplicada no cumprimento de medida protetiva de urgência de afastamento do lar ou proibição de aproximação da mulher, no âmbito da Lei Maria da Penha (Lei nº 11.340/2006, Art. 22, II e III), podem ser coletados dados pessoais de geolocalização em tempo real não apenas do homem autor, mas também da mulher em situação de violência, o que sugere amplas possibilidades de revitimização em casos de tratamento inadequado desses dados pessoais sensíveis.

Por tratar de dados pessoais sensíveis, a central de monitoração eletrônica deveria seguir protocolos rígidos, aptos a garantir a adequada proteção dos dados e a assegurar que o tratamento seja estritamente adstrito à finalidade da coleta – qual seja, assegurar o cumprimento das medidas previstas judicialmente. Contudo, os serviços se estabeleceram no país sem diretrizes nacionais e sem regras bem delimitadas. Assim, cada central define fluxos próprios, com ampla margem de discricionariedade para gestores e funcionários (BRASIL, 2017b, 2018c).

Nesse contexto, o modo de tratamento dos dados pessoais coletados nos serviços de monitoração eletrônica é condicionado, sobretudo, pela percepção a respeito das pessoas submetidas às medidas por parte de diferentes atores do Sistema de Justiça Criminal e dos trabalhadores envolvidos direta ou indiretamente com os serviços. Sendo as pessoas monitoradas entendidas como "presas" ou "criminosas", elas não são reconhecidas como sujeitos de direitos. Essa concepção facilita o estabelecimento de fluxos que desprezam aspectos como a necessidade de proteger os dados, evitar/minimizar a estigmatização ou promover a inclusão social, como prevê a Lei de Execução Penal (1984).

As crescentes demandas por controle penal, potencializadas pelo fetiche relacionado ao uso da tecnologia em ações de segurança pública, contribuem para a configuração de graves violações aos direitos de proteção e tratamento adequado de dados pessoais das pessoas monitoradas. O próximo tópico descreve como tais violações se materializam nos serviços de monitoração eletrônica.

Violações dos direitos de proteção e tratamento adequado de dados pessoais na monitoração eletrônica

Apesar dos avanços trazidos pela Lei nº 13.709/2018, seu Art. 4º, III, representa uma relevante perda de oportunidade de se promoverem regras claras de proteção de dados pessoais no âmbito da segurança pública e das políticas penais. Ao afastar sua incidência nos casos de tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, a Lei de Proteção de Dados Pessoais deixa de fora de seu escopo campos nos quais a proteção de dados pessoais se apresenta como mais necessária, diante da dimensão dos abusos verificados e das vulnerabilidades do público envolvido.

Não obstante, para além das garantias previstas na Constituição, a proteção de dados das pessoas monitoradas eletronicamente é assegurada expressamente em normas sobre a matéria. O Decreto nº 7.627/2011, que regulamenta a monitoração eletrônica de pessoas, estabelece que "o sistema de monitoramento será estruturado de modo a preservar o sigilo dos dados e das informações da pessoa monitorada" (Art. 6º). Prevê, ainda, que "o acesso aos dados e informações da pessoa monitorada ficará restrito aos servidores expressamente autorizados que tenham necessidade de conhecê-los em virtude de suas atribuições" (Art. 7º).

Também a Resolução nº 213/2015 do Conselho Nacional de Justiça, ao regulamentar as audiências de custódia no país, traz importantes referências sobre a proteção de dados na monitoração eletrônica de pessoas. O normativo estabelece que, "por abranger dados que pressupõem sigilo, a utilização de informações coletadas durante a monitoração eletrônica de pessoas dependerá de autorização judicial" (Art. 10, Parágrafo único).

A mesma resolução traz desdobramentos específicos a esse respeito, ao apresentar orientações para os serviços de alternativas penais e de monitoração eletrônica, e prevê que as centrais de monitoração eletrônica deverão:

> Primar pela adoção de padrões adequados de segurança, sigilo, proteção e uso dos dados das pessoas em monitoração, respeitado o tratamento dos dados em conformidade com a finalidade das coletas. Nesse sentido, deve-se considerar que os dados coletados durante a execução das medidas de monitoração eletrônica possuem finalidade específica, relacionada com o acompanhamento das condições estabelecidas judicialmente. As informações das pessoas monitoradas não poderão ser compartilhadas com terceiros estranhos ao processo de investigação ou de instrução criminal que justificou a aplicação da medida. O acesso aos dados, inclusive por instituições de segurança pública, somente poderá ser requisitado no âmbito de inquérito policial específico no qual a pessoa monitorada devidamente identificada já figure como suspeita, sendo submetido a autoridade judicial, que analisará o caso concreto e deferirá ou não o pedido. (BRASIL, 2015a, Protocolo I, Item 3.3, III).

No mesmo sentido, o Conselho Nacional de Política Criminal e Penitenciária publicou a Resolução nº 5/2017, que dispõe sobre a política de implantação de monitoração eletrônica, bem como orienta

os serviços quanto a proteção e tratamento de dados pessoais, incorporando o assunto nos princípios que regem a aplicação e o acompanhamento da monitoração eletrônica. É reservado um capítulo exclusivo para tratar do tema, indicando a matéria como indispensável para a implementação e qualificação dos serviços de monitoração eletrônica. A natureza sensível dos dados pessoais da monitoração eletrônica é explicitada, reconhecendo-se seu potencial lesivo e discriminatório.

Contudo, diversas formas de violações a esses normativos são observadas nos serviços instituídos no país. Por si só, a não adoção de protocolos para os diversos fluxos e procedimentos relacionados aos serviços de monitoração eletrônica propicia um contexto favorável ao mau uso dos dados pessoais coletados. Isso pode representar, em diversos casos, violação ao direito de proteção e tratamento adequado aos dados pessoais, sujeitando os titulares dos dados (especialmente as pessoas monitoradas) a situações que vão desde a possibilidade de exposição pública de sua condição de pessoa condenada ou processada, chegando até a sua (re)criminalização a partir de práticas seletivas e discriminatórias. Também, os profissionais envolvidos com o tratamento dos dados e com o acompanhamento das medidas de monitoração eletrônica determinadas judicialmente são afetados por esse cenário, uma vez que a ausência de procedimentos claros de conduta amplia a incerteza da adequação à legalidade de suas práticas cotidianas e os coloca em posição frágil para se opor a pressões indevidas de acesso aos dados mantidos pela central (BRASIL, 2016).

Assim, a omissão do Poder Público em estabelecer fluxos específicos e adequados para a garantia da proteção de dados pessoais repercute em uma maior vulnerabilidade das pessoas monitoradas a ter expostos seus dados pessoais sensíveis e, ainda, em um maior risco de que trabalhadores dos serviços possam incorrer em ilegalidades, sujeitando-os potencialmente a responsabilidade civil, administrativa ou criminal em virtude dos atos praticados, como expresso nas Diretrizes para Tratamento e Proteção de Dados na Monitoração Eletrônica de Pessoas (BRASIL, 2016).

É possível indicar, ao menos, duas rotinas de tratamento de dados em que o Estado age ativamente na violação dos direitos das pessoas monitoradas, ignorando os normativos citados. Apesar de as centrais de monitoração eletrônica estarem instituídas, na maior parte dos casos, como serviços vinculados à administração penitenciária dos estados, elas muitas vezes estabelecem – formal ou informalmente – fluxos mais ou menos constantes de envio de informações para a polícia civil.

O principal dado coletado pelos serviços de monitoração eletrônica que desperta interesse nas polícias judiciárias é a geolocalização das pessoas monitoradas. Essas informações podem ser solicitadas por um delegado de polícia no âmbito de uma investigação em curso – por exemplo, quando há suspeita de que alguma pessoa com tornozeleira eletrônica teria envolvimento com um delito que está sendo apurado. Nesse caso, a central repassa à polícia – por e-mail, telefone, *whatsapp*, pessoalmente, etc. – informações de geolocalização sobre determinada pessoa monitorada ou mesmo sobre todo o conjunto de pessoas monitoradas, buscando indicar

se estavam ou não presentes em determinado local na hora aproximada em que o delito ocorreu. Não obstante a previsão da Resolução nº 213/2015, do Conselho Nacional de Justiça, da Resolução nº 5/2017, do Conselho Nacional de Política Criminal e Penitenciária, e dos documentos oficiais publicados pelo Departamento Penitenciário Nacional (BRASIL, 2015b, 2016, 2017b, 2018c), sobre a necessidade de decisão judicial para autorizar a utilização dos dados, que devem se referir a pessoa específica já identificada como suspeita em inquérito policial, a praxe em algumas centrais é o compartilhamento administrativo das informações, sem autorização judicial e sem respeito às condicionantes estabelecidas.

No limite, essa relação entre central de monitoração eletrônica e polícia civil se institucionaliza e ganha contornos ainda mais perversos, notadamente em políticas estaduais de segurança pública que assumem a identificação de autorias como um dos indicadores para a mensuração da "eficácia" do enfrentamento à criminalidade. Nesses casos, já é possível identificar o compartilhamento sistemático e periódico dos dados de todas as pessoas monitoradas com a polícia judiciária, tendo por finalidade o cruzamento com bases de dados policiais a respeito de crimes sem autoria identificada. A partir da "correlação hora de crime", jargão pelo qual a prática é conhecida, emergem os potenciais suspeitos – que combinados com alguma informação policial, irão compor o arcabouço probatório necessário para processar, punir e prender por novos delitos as pessoas que já se encontravam sob o controle punitivo estatal a partir do uso das tornozeleiras.

É assim que, a partir do compartilhamento de dados das pessoas monitoradas com a polícia civil e o cruzamento com informações sobre local e horário de crimes sem autoria identificada,

> a mera presença de pessoas monitoradas "no lugar errado e na hora errada" faz delas potenciais suspeitas de práticas delitivas. Estamos diante, assim, do uso da tecnologia aplicada contra seres humanos na atualização tecnológica da já conhecida "investigação por suspeição" (BRASIL, 2016, p. 6).

Essas práticas atentam contra os princípios da finalidade, adequação e não discriminação, relativos à proteção de dados pessoais. Os dados de geolocalização são dados pessoais sensíveis que expõem profundamente a intimidade das pessoas monitoradas e, considerando as dinâmicas próprias das agências punitivas brasileiras, colocam essas pessoas em situação de extrema vulnerabilidade social e penal. O tratamento dessas informações deve, por princípio, se ater estritamente à finalidade da coleta, qual seja, permitir o monitoramento de condições fixadas judicialmente, como medida cautelar ou como condição para acesso a direitos (usualmente referidos como "benefícios") durante a execução da pena (como saídas temporárias ou exercício de trabalho externo).

A cessão de dados das pessoas monitoradas para a realização de cruzamentos com bases de dados da polícia civil constitui um tratamento com objetivo diverso do da coleta, violando os princípios da finalidade e adequação. Ao mesmo tempo, a utilização desses dados para a identificação de potenciais responsáveis por crimes sem

autoria identificada, revela-se altamente lesiva e discriminatória, sujeitando os titulares dos dados a filtros que tomam como pressuposto seu potencial delitivo, ao qual não estão submetidos os demais indivíduos da sociedade – os "não-monitorados".

A situação é ainda mais alarmante quando consideramos que muitos órgãos policiais estabelecem metas para seus agentes, as quais podem incluir a maior produtividade na identificação de autoria de crimes. A depender da política estadual de segurança pública, tais metas influenciam na remuneração (bonificação) dos policiais ou nos processos de avaliação para progressão na carreira. Estabelece-se, nesses casos, uma lógica de incentivos perversos para que sejam atribuídas autorias a crimes a qualquer custo, em uma cena bastante propícia à imputação da responsabilidade por delitos a pessoas monitoradas eletronicamente que não os cometeram, como observado em várias ocasiões.

A segunda rotina de tratamento de dados pessoais pela qual o Estado brasileiro viola direitos das pessoas monitoradas eletronicamente é mais difusa, operando de formas variadas em diferentes serviços espalhados pelo país. Além dos fluxos de envio de dados para a polícia civil, conforme indicado anteriormente, também pode ocorrer, em determinados casos, de a central de monitoração eletrônica fornecer informações sobre as pessoas monitoradas para a polícia militar.

A tornozeleira eletrônica é uma marca visível de desigualação social para baixo e de submissão ao sistema penal. Ela nos remete a práticas punitivas medievais, nas quais a estigmatização tinha um sentido assertivo, de marcar corpos como uma forma de tatuagem, permitindo a todos identificar quem eram os delinquentes quando transitassem pelos espaços coletivos (ANITUA, 2008). Da mesma forma, a pessoa monitorada eletronicamente nos dias de hoje será, vez ou outra, reconhecida nas ruas e demais espaços sociais por sua condição – despertando a atenção, inclusive, de agentes responsáveis pelo policiamento ostensivo.

O interesse da polícia militar pelas pessoas monitoradas eletronicamente se dá, assim, pela pretensão de acompanhar, em sua atividade de rua, o comportamento desses sujeitos. Saber em tempo real por onde transitam os "delinquentes estigmatizados" poderá ajudar, por esta lógica, a prevenir que eles cometam outros crimes, conforme relatos de gestores e policiais. Observamos neste cálculo uma dimensão moral, mobilizando valores disponíveis em um sistema de crenças socialmente legitimado, orientado por esquemas classificatórios que rotulam por oposição: "preso monitorado", "bandido" x "cidadão de bem", "trabalhador" (PIMENTA, I.L., 2014). Tal "método" poderá também servir (supostamente) para "tranquilizar" a população, que saberá que aquelas "pessoas de tornozeleira" – e por isso "perigosas" – estão sob controle próximo da polícia, mesmo que não estejam descumprindo qualquer restrição judicial ao transitarem em áreas e horários permitidos. Há caso de pessoa monitorada presa pela polícia em *shopping center* simplesmente por ter sido identificada a tornozeleira, ainda que nenhuma condição determinada pela justiça estivesse sendo desrespeitada – a liberdade viria no dia seguinte, desfeito o "mal-entendido".

Foucault (1999, p. 234) já advertia que "a vigilância policial fornece à prisão os infratores que esta transforma em delinquentes, alvo e auxiliares dos controles policiais que regularmente mandam alguns deles de volta à prisão". O que a monitoração eletrônica produz é uma nova roupagem para antigas práticas, agregando tecnologias que expandem a capacidade de produzir, delimitar e controlar a delinquência estigmatizada.

Em alguns estados, todas as pessoas presas em regime semiaberto com direito a saída temporária são submetidas, durante o período fora da prisão, ao uso de tornozeleiras eletrônicas. Em uma das centrais circulam informes para policiais militares com dados sobre as pessoas presas que estão temporariamente nas ruas e sob monitoramento eletrônico, para reforço das ações de policiamento ostensivo. A partir dessas rotinas de compartilhamento de dados entre central e polícia militar, busca-se:

> constituir uma variável da política de "prevenção" pela perseguição aos indivíduos monitorados, que entrariam no "radar" do policiamento para inibir seu potencial comportamento delitivo. Esta proposta afasta qualquer perspectiva de emancipação dos sujeitos submetidos às medidas de monitoração, aproximando-os sempre do sistema penal ao invés de construir caminhos para trajetórias que os tornem menos vulneráveis a novos processos de criminalização (BRASIL, 2016, p. 6)

Considerando o alto número de mortes cometidas por agentes policiais (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2017), o compartilhamento com a polícia militar da informação sobre a localização em tempo real das pessoas monitoradas pode representar, inclusive, risco à vida desses indivíduos. Uma das hipóteses de aplicação da monitoração eletrônica é como medida cautelar diversa da prisão – que pode vir a ser aplicada logo no dia seguinte à pessoa ter sido presa em flagrante por policiais militares e apresentada em juízo nas audiências de custódia. Diálogos estabelecidos em campo revelam a insatisfação de agentes policiais com relação à liberdade imediata concedida para a pessoa presa em flagrante. Essa insatisfação, somada ao acesso a dados sobre sua geolocalização, é receita pronta para diversas espécies de abusos, que podem incluir desde imputações artificiais de novas condutas delitivas (garantindo, assim, a manutenção da prisão) até mesmo o extermínio, em práticas do "sistema penal subterrâneo" (CASTRO, 2005).

Assim como ocorre no compartilhamento de dados das pessoas monitoradas com a polícia civil, os fluxos de informações entre central e polícia militar constituem práticas colidentes com os princípios da finalidade, adequação e não discriminação, que deveriam pautar as ações de tratamento de dados pessoais. Ainda, tais situações ferem garantias previstas constitucionalmente quanto a inviolabilidade da intimidade, da vida privada, da honra e da imagem dessas pessoas (Art. 5º, X), elementos também entoados pelo Decreto nº 7.627/2011 e pelas Resoluções do CNJ nº 213/2015 e do CNPCP nº 5/2017.

Conclusão

Os debates sobre monitoração eletrônica estão geralmente centrados na dualidade "monitoração" *versus* "não monitoração", ou seja, no reconhecimento ou

na negativa de sua "eficácia" em termos de controle e vigilância disciplinar e, por um viés mais crítico, na potencialidade, ou não, do instrumento para a promoção do desencarceramento. Esse debate importa e deve ser aprofundado, havendo pouco acúmulo a respeito, o que tem favorecido a adoção acrítica de discursos favoráveis à expansão da monitoração eletrônica – por se enxergar nela uma suposta alternativa ao hiperencarceramento. Nesse sentido, é preciso questionar:

> se uma medida própria de contenção e controle penal como a monitoração eletrônica tem aptidão de fazer frente aos pressupostos do paradigma punitivo, promovendo uma transformação na forma como lidamos com conflitos e violências na sociedade e como tratamos as pessoas assujeitadas pelo sistema penal. Meu entendimento, a princípio, é que não: um instrumento concebido para controle de corpos não permite, por sua natureza, as mudanças conceituais para uma política penal alternativa emancipadora. (PIMENTA, V.M., 2017, p.30)

A forma como são tratados os dados pessoais está no centro da disputa do sentido político e social da monitoração eletrônica. Em geral, os serviços de monitoração eletrônica são enxergados como extensões da atividade policial do Estado, garantindo o controle sobre uma "delinquência monitorada" – as tornozeleiras são vistas como "benefícios" concedidos a indivíduos que deveriam, a rigor, estar presos. A partir do uso da tecnologia, entende-se ser possível a vigilância constante sobre esses indivíduos, mantendo-os sob estrito controle e sob a constante ameaça de serem enviados (de volta) à prisão.

A monitoração eletrônica é concebida, assim, como uma política de "prevenção" baseada no controle de corpos das pessoas já submetidas aos processos de criminalização. Essa concepção e as práticas a ela relacionadas produzem significativo impacto para as pessoas submetidas às medidas de monitoração eletrônica, implicando uma maior dificuldade de construção de novas trajetórias de vida, ao impedir que elas se afastem do sistema penal, ao qual acabam constantemente atraídas – seja pelos procedimentos adotados pela Central, seja pelas abordagens realizadas pela polícia, de forma autônoma ou a partir de acionamentos pelos próprios serviços de monitoração eletrônica.

A reflexão aqui proposta importa não apenas à monitoração eletrônica, pois serve para pensar também as formas de tratamento de dados no sistema punitivo como um todo, indicando como a violação sistemática do direito à proteção adequada de dados pessoais é uma das estratégias de reprodução de um sistema penal seletivo e excludente. No horizonte de uma agenda de enfrentamento a essas violações, destacamos a insuficiência da Lei nº 13.709/2018 para a proteção de dados pessoais das pessoas monitoradas, uma vez que afasta expressamente a aplicação da lei para o tratamento de dados pessoais realizado para fins de segurança pública ou para atividades de investigação ou repressão de infrações penais (Art. 4º, III), remetendo o regramento da matéria a legislação específica (Art. 4º, § 1º), que não existe e para a qual não há perspectiva real de vir a existir.

No caso da monitoração eletrônica de pessoas, as práticas indicadas ao longo

deste artigo violam não apenas princípios gerais de proteção de dados pessoais, mas desconsideram, também, outras diretrizes e normas nacionais já existentes acerca do tema, emanadas pelo Conselho Nacional de Justiça (BRASIL, 2015a), Conselho Nacional de Política Criminal e Penitenciária (BRASIL, 2017a) e Departamento Penitenciário Nacional (BRASIL, 2016, 2017b). Sua disseminação indica a necessidade de medidas para assegurar o tratamento e a proteção de dados pessoais nas políticas de segurança pública e no sistema penal, justamente por lidarem com público que menos tem seus direitos reconhecidos e que está mais sujeito a profundas violações e comportamentos discriminatórios por parte do Estado.

Referências Bibliográficas

ANITUA, Gabriel Ignacio. **Histórias dos pensamentos criminológicos**. Rio de Janeiro: Revan, 2008.

BECKER, Howard S. **Outsiders – Estudos de sociologia do desvio**. Rio de Janeiro: Zahar, 2008.

BRASIL. **Lei nº 13.709, 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). Brasília, DF, 2018a.

BRASIL. **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. 2018b.

BRASIL. Ministério da Justiça. Departamento Penitenciário Nacional. Programa das Nações Unidas para o Desenvolvimento. **Diagnóstico Sobre a Política de Monitoração Eletrônica**. Brasília, DF: MJ; PNUD, 2018c. Disponível em: <http://depen.gov.br/DEPEN/dirpp/monitoracao-eletronica/arquivos/diagnostico-monitoracao-eletronica-2017.pdf>. Acesso em: 10 jan. 2019.

BRASIL. Ministério da Justiça. Conselho Nacional de Política Criminal e Penitenciária. **Resolução nº 5, de 10 de novembro de 2017**. Dispõe sobre a política de implantação de Monitoração Eletrônica. Brasília, DF, 2017a.

BRASIL. Ministério da Justiça. Departamento Penitenciário Nacional. Programa das Nações Unidas para o Desenvolvimento. **Manual de Gestão para a Monitoração Eletrônica de Pessoas**. Brasília: MJ; PNUD, 2017b. Disponível em <http://www.justica.gov.br/seus-direitos/politica-penal/politicas-2/monitoracao-eletronica-1/MODELODEGESTOPARAAMONITORAOELETRNICA-DEPESSOAS.pdf>. Acesso em: 2 jan. 2018.

BRASIL. Ministério da Justiça. Departamento Penitenciário Nacional. Programa das Nações Unidas para o Desenvolvimento. **Diretrizes para Tratamento e Proteção de Dados na Monitoração Eletrônica de Pessoas**. Brasília, DF: MJ; PNUD, 2016. Disponível em: <http://www.justica.gov.br/seus-direitos/politica-penal/politicas-2/monitoracao eletronica-1/arquivos/diretrizes-para-tratamento-e-protecao-de-dados-namonitoracao-eletronica-de-pessoas.pdf>. Acesso em: 2 jan. 2018.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 213, de 15 de dezembro de 2015**. Dispõe sobre a apresentação de toda pessoa presa à autoridade judicial no prazo de 24 horas. Brasília, DF: CNJ, 2015a.

BRASIL. Ministério da Justiça. Departamento Penitenciário Nacional. Programa das Nações Unidas para o Desenvolvimento. **A implementação da política de monitoração eletrônica de pessoas no Brasil**. Análise crítica do uso da monitoração eletrônica de pessoas no cumprimento da pena e na aplicação de medidas cautelares diversas da prisão e medidas protetivas de urgência. Brasília, DF: MJ; PNUD, 2015b.

BRASIL. **Decreto nº 7.627, de 24 de novembro de 2011**. Regulamenta a monitoração eletrônica de pessoas prevista no Decreto nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, e na Lei nº 7.210, de 11 de julho de 1984 – Lei de Execução Penal. Brasília, DF, 2011.

BRASIL. **Lei nº 12.258, de 15 de junho de 2010**. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e a Lei no 7.210, de 11 de julho de 1984 (Lei de Execução Penal), para prever a possibilidade de utilização de equipamento de vigilância indireta pelo condenado nos casos em que especifica. Brasília, DF, 2010.

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006**. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal. Brasília, DF, 2006.

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

BRASIL. **Lei nº 7.210, de 11 de julho de 1984**. Institui a Lei de Execução Penal. Brasília, DF, 1984.

CASTRO, Lola Aniyar de. **Criminologia da Libertação**. Rio de Janeiro: Revan, 2005.

DONEDA, Danilo. A Tutela da Privacidade no Código Civil de 2002. **Anima Revista Eletrônica**, v. 1, p. 89-100, 2009.

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

DONEDA, Danilo; VIOLA, Mario. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. **Revista Brasileira Risco e Segurança**, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. v. 1.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública – 2017**. São Paulo: Fórum Brasileiro de Segurança Pública ,2017. Disponível em: <http://www.forumseguranca.org.br/wp-content/uploads/2017/12/ANUARIO_11_2017.pdf>. Acesso em: 2 jan. 2018.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 20 ed. Petrópolis: Vozes, 1999.

GOFFMAN, Ervin. **Estigma**: notas sobre a manipulação da identidade deteriorada. São Paulo: LTC, 1988.

GREENLEAF, Graham. Global Tables of Data Privacy Laws and Bills. **Privacy Laws & Business International Report**, 5th ed., n. 145, p. 14-26, 2017. Disponível em: <https://ssrn.com/abstract=2992986>. Acesso em: 2 jan. 2018.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados (RGPD)**. Regulamento (UE) nº 2016/679. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Bruxelas: UE, 2016.

PIMENTA, Izabella Lacerda. Nem Benefício, Nem Regalia: práticas e arbitrariedades nos serviços de monitoração eletrônica de pessoas no Brasil. In: DE VITTO, Renato; DAUFEMBACK, Valdirene (Orgs.). **Para além da prisão**: reflexões e propostas para uma nova política penal no Brasil. Belo Horizonte: Letramento, 2018.

PIMENTA, Izabella Lacerda. **Dos acessos ao "mundo do trabalho"**– uma etnografia sobre os processos de construção institucional de presos e egressos no Rio de Janeiro (Brasil) e em Ottawa (Canadá). Tese (Doutorado) – Programa de Pós-Graduação em Antropologia, Universidade Federal Fluminense. Niterói, RJ, 2014.

PIMENTA, Victor Martins. Fundamentos para a Política Penal Alternativa. **Aracê – Direitos Humanos em Revista**, v. 4, n. 5, p. 14-34, 2017.

PIMENTA, Victor Martins. **Por trás das grades**: o encarceramento brasileiro em uma abordagem criminológico-crítica. 172 f. Dissertação (Mestrado em Direitos Humanos e Cidadania) – Universidade de Brasília, Brasília, 2016.

FÓRUM BRASILEIRO DE
SEGURANÇA PÚBLICA