DIRETRIZES PARA TRATAMENTO E PROTEÇÃO DE DADOS NA MONITORAÇÃO ELETRÔNICA DE PESSOAS

Ministério da
Justiça

Departamento
Penitenciário Nacional

PNUD

Empoderando vidas.
Fortalecendo nações.

DIRETRIZES PARA TRATAMENTO E PROTEÇÃO DE DADOS NA MONITORAÇÃO ELETRÔNICA DE PESSOAS

BRASÍLIA
2016

DEPARTAMENTO PENITENCIÁRIO NACIONAL
DIRETORIA DE POLÍTICAS PENITENCIÁRIAS
COORDENAÇÃO-GERAL DE ALTERNATIVAS PENAIS

Ficha Técnica

Título: Diretrizes para tratamento e proteção de dados na monitoração eletrônica de pessoas

Total de folhas: 85

Coordenação:
Victor Martins Pimenta – Coordenador-Geral de Alternativas Penais
Autora:
Izabella Lacerda Pimenta

Palavras-chave: Monitoração Eletrônica – Tratamento e Proteção de Dados Pessoais Sensíveis – Desencarceramento – Departamento Penitenciário Nacional.

Documento resultado do produto “Proposta de diretrizes e regras sobre tratamento e proteção de dados.” no âmbito de Consultoria Nacional Especializada para Formulação de Modelo de Gestão de Monitoração Eletrônica de Pessoas, sob supervisão de Victor Martins Pimenta, projeto BRA/011/2014 – Fortalecimento da Gestão do Sistema Prisional Brasileiro, parceria entre Departamento Penitenciário Nacional e o Programa das Nações Unidas para o Desenvolvimento.

Sumário

APRESENTAÇÃO 5

1 - POLÍTICAS PÚBLICAS NA "SOCIEDADE EM REDE" 8

1.1 - A Importância do Estabelecimento de Protocolos 10

2- CONSIDERAÇÕES INICIAIS SOBRE DADOS PESSOAIS E POLÍTICAS PÚBLICAS 13

2.1 - Proteção de dados pessoais no cenário internacional 17

2.2 - A realidade brasileira no cenário dos dados pessoais 20

2.2.1 - O Código de Proteção e Defesa do Consumidor – um caso à parte 25

3 - PARTICULARIDADES DA MONITORAÇÃO ELETRÔNICA DE PESSOAS NO BRASIL 28

3.1 - Audiências de Custódia e Monitoração Eletrônica 31

4 - CONSIDERAÇÕES SOBRE TRATAMENTO E PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO NA MONITORAÇÃO ELETRÔNICA DE PESSOAS 34

5- PRINCÍPIOS, DIRETRIZES E REGRAS SOBRE TRATAMENTO E PROTEÇÃO DE DADOS RELATIVOS À MONITORAÇÃO ELETRÔNICA DE PESSOAS 45

5. 1 – Proteção de dados pessoais sensíveis 49

5. 2 – Segurança da informação 52

5.3 - Composição dos dados pessoais sensíveis dos monitorados 53

5.4 - Regras prévias ao tratamento e proteção de dados pessoais dos monitorados 55

5.5 - Regras por espécie de tratamento e proteção dos dados pessoais dos monitorados 58

5.5.1 - Entrada dos dados 58

5.5.2 - Manipulação dos dados 64

5.5.3 - Saída dos dados 65

5.6 - Fornecimento a terceiros por comunicação, interconexão, transferência, difusão ou extração 66

5.7 - Regras de segurança física e lógica, avaliação ou controle das informações 70

6- CONSIDERAÇÕES FINAIS 76

REFERÊNCIAS BIBLIOGRÁFICAS 78

Apresentação

A monitoração eletrônica de pessoas é prática extremamente recente no país, sendo os primeiros serviços instituídos a partir de 2010. De lá pra cá, os serviços se expandiram rapidamente, estando presentes hoje em pelo menos 19 Estados, na maioria das vezes sem fluxos e procedimentos bem definidos e carentes, sobretudo, de diretrizes nacionais quanto aos diferentes aspectos que envolvem a implementação da política.

Neste curto período de implantação, a monitoração eletrônica vem assumindo um sentido marcadamente repressivo. De um lado, orienta-se pela concepção de uma política de segurança pública pautada pelo controle e vigilância sobre indivíduos considerados 'perigosos', contra os quais as agências punitivas centram sua atuação. De outro lado, os serviços estão norteados também por procedimentos oriundos da gestão prisional, de contenção e punição, sobretudo em virtude de sua alocação nas estruturas organizacionais das Administrações penitenciárias dos Estados.

Frente a este cenário, o Departamento Penitenciário Nacional (Depen) assumiu o compromisso de elaborar um modelo de gestão para os serviços de monitoração eletrônica de pessoas, valendo-se para tanto de parceria firmada com o Programa das Nações Unidas para o Desenvolvimento (PNUD/ONU). O modelo em elaboração pelo Depen tem por objetivo orientar tecnicamente os serviços, alinhando-os às diretrizes nacionais para os serviços penais.

Nesse sentido, é certo que a coleta e as diversas formas de tratamento de dados são atividades essenciais ao serviço de monitoração eletrônica. A gestão adequada das informações obtidas, inclusive quanto à geolocalização das pessoas monitoradas, é pressuposto para o bom funcionamento dos serviços, bem como para os processos de formulação, implementação, monitoramento e avaliação da política.

Não obstante, na era da informação e do controle social exercido por novas tecnologias, a construção de políticas menos excludentes nas áreas penal e de segurança pública exige um olhar cuidadoso sobre o tema da proteção e tratamento de dados pessoais. A questão é ainda mais relevante quando tratamos de procedimentos relacionados à persecução penal, pois a mera informação de que determinada pessoa responde ou foi condenada por determinado crime a expõe a reações sociais que afetam seus vínculos familiares,

comunitários e sociais, prejudicando, por exemplo, seu acesso e permanência no mercado de trabalho. Falamos então, por sua natureza, de dados pessoais sensíveis, que exigem especial proteção por parte do poder público, sob risco de expor as pessoas monitoradas eletronicamente a marcadores permanentes de estigmatização e exclusão.

Algumas práticas demonstram a urgência da produção de protocolos nesta área, seja para orientar a melhor gestão da informação, seja para evitar falhas na proteção dos dados. Tem-se observado, em alguns serviços instituídos no país, o compartilhamento dos dados das pessoas monitoradas com a Polícia Civil. Esses dados são utilizados para cruzamentos com informações sobre local e horário de crimes sem autoria identificada, de modo que 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', prática tanto criticada pela criminologia em estudos e propostas sobre segurança pública.

Da mesma forma, há movimentos para que os dados de monitoração eletrônica possam também ser compartilhados, sem restrições de acesso, com a Polícia Militar. Busca-se, assim, constituir uma variável da política de "prevenção" pela perseguição aos indivíduos monitorados, que entrariam no "radar" do policiamento ostensivo 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.

Frente a esse contexto, o documento Diretrizes para Tratamento e Proteção de Dados na Monitoração Eletrônica de Pessoas orienta os serviços na direção das melhores práticas em tratamento e proteção de dados pessoais e da garantia dos direitos fundamentos das pessoas monitoradas. Ele alinha-se, também, às diretrizes do Conselho Nacional de Justiça, emanadas pela Resolução nº 213/2015, que estabelece restrições ao compartilhamento de dados de pessoas monitoradas eletronicamente, indicando ainda a necessidade de elaboração de protocolos na área.

Ao aprofundar tecnicamente em questões pouco exploradas no país e que envolvem garantia de direitos que afetam transversalmente diversos órgãos, são oferecidos subsídios para a proteção de dados não apenas na área da monitoração eletrônica, podendo ser úteis também à construção de protocolos na política prisional e sobretudo na segurança pública.

Boa leitura a todas e a todos!

Victor Martins Pimenta
Coordenador-Geral de Alternativas Penais

1 - POLÍTICAS PÚBLICAS NA "SOCIEDADE EM REDE"

Os campos da ciência são orientados pela introdução de inovações, de paradigmas e pelo afastamento de padrões ou de verdades até então estabelecidas (Kuhn, 1978). Nos dias atuais é recorrente ouvir – independentemente de qualquer tipo de inconsistência conceitual ou conteúdo ideológico – que se vive sob um novo paradigma social/tecnológico de caráter estruturante comumente chamado de "Era da Informação", "Sociedade da Informação", "Sociedade do Conhecimento", sofrendo suas conseqüências, mudanças, possibilidades, limites e ameaças, especialmente através de inovações possibilitadas pelas tecnologias da informação. O fato de as tecnologias da informação serem o principal mobilizador dos variados fluxos comunicacionais, indica um termo provavelmente mais apropriado para se pensar as características e as questões em torno da circulação de informações em nossa sociedade, qual seja "Sociedade em Rede" [1] (Castells, 2005).

Segundo o sociólogo supracitado, conhecimento e informação sempre foram centrais nas sociedades historicamente conhecidas, a novidade é o fato de serem de base microeletrônica, através de redes tecnológicas que fornecem novas capacidades a uma velha forma de organização social: "as redes de comunicação digital são a coluna vertebral da sociedade em rede (...)" (idem, p.18) Assim, "(...) a internet é um tecido da comunicação em nossas vidas: para o trabalho, os contatos pessoais, a informação, o entretenimento, os serviços públicos, a política e a religião". (Castells, 2009, p. 100)

Os processos que permeiam esse paradigma são impulsionados pelos avanços das tecnologias de informação e comunicação, possibilitando a expansão e a circulação de diversos dados entre agentes plurais, individuais ou coletivos. A velocidade garantida na

[1] "A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes. A rede é a estrutura formal (vide Monge e Contractor, 2004). É um sistema de nós interligados. E os nós são, em linguagem formal, os pontos onde a curva se intersecta a si própria. As redes são estruturas abertas que evoluem acrescentando ou removendo nós de acordo com as mudanças necessárias dos programas que conseguem atingir os objetivos de performance para a rede. Estes programas são decididos socialmente fora da rede mas a partir do momento em que são inscritos na lógica da rede, a rede vai seguir eficientemente essas instruções, acrescentando, apagando e reconfigurando, até que um novo programa substitua ou modifique os códigos que comandam esse sistema operativo." (Castells, 2005, p.20) Em linhas gerais, a "Sociedade de Rede" introduz novas formas de sociabilidade assentadas em dimensões virtuais, promovida e facilitada pelas novas tecnologias que independem e transcendem as dimensões tempo e espaço.

comunicação, no processamento, no armazenamento e na transmissão das informações, torna possível trocas a nível global com custos cada vez menores. Inicialmente, esse último aspecto poderia sinalizar uma suposta inovação com contornos democráticos e inclusivos.

Por outro lado, a difusão das informações ocorre a partir de redes seletivas de acordo com programas específicos, conseguindo, de maneira simultânea, comunicar e não comunicar. Assim, de acordo com Castells (2009), a sociedade em rede difunde-se por todo o mundo desigualmente, não inclui todos os indivíduos e, na verdade, exclui a maior parte deles. Ele lembra, no entanto, que toda a humanidade é afetada pela sua lógica e pelas relações de poder que interagem nas redes globais da organização social. A Internet passa a ser a base dessa sociedade, uma rede que congrega diversos grupos de redes de computadores, mas, sobretudo, de pessoas e de informação.

Avançando nesta proposição, Giddens (2002) ressalta que a "alta modernidade"[2] é "(...) caracterizada pelo ceticismo generalizado juntamente à razão providencial, em conjunto com o reconhecimento de que a ciência e a tecnologia têm dois gumes, criando novos parâmetros de risco e perigo ao mesmo tempo em que oferecem possibilidades benéficas para a humanidade." (p. 32) As ambiguidades e os conflitos envolvendo interesses distintos indicam que há muito trabalho a ser desenvolvido no campo da tecnologia da informação, necessariamente envolvendo informação, conhecimento e poder, ou seja, pensar além da pura transmissão de dados, mas no compartilhamento de significados. Outrossim, cabe refletir acerca do papel do Estado nesse cenário, onde as informações passam a circular cada vez mais e com maior facilidade: "(...) as possibilidades e os limites do Estado, a partir o crescente questionamento da previsibilidade, inteligibilidade e controle de seu domínio de intervenção, incluindo o próprio domínio da informação." (Gómez, 2011, p. 186)

Para Weber (1979), o Estado Moderno caracteriza-se por dispor de dois elementos constitutivos fundamentais, a saber: o monopólio legítimo da força e a presença de um aparato administrativo para prestação de serviços públicos, ou seja, de uma burocracia. O Estado Moderno erigiu-se tendo por base "(...) os pressupostos de uma administração 'racional' e de uma justiça 'independente', que deveriam ser igualmente obrigatórias para

[2] Para Anthony Giddens (2002), a "alta modernidade" ou "modernidade tardia" consiste na presente fase de desenvolvimento das instituições modernas, marcada pela radicalização e globalização dos traços básicos da modernidade.

todos, não permitindo privilégios ou exceções, e que deveriam ser também objetivas, não podendo ser nem manipuladas, nem endereçadas a determinados indivíduos. (Miranda, 2005, p. 5)

No caso do Brasil, todavia, a lógica pessoal, própria dos ambientes da vida social íntima, perpassa também o Estado brasileiro (Holanda, 1995). Ainda que o Estado brasileiro e suas instituições sejam formalmente concebidos de acordo com o princípio da igualdade perante a lei, caracterizam-se, em geral, pelo tratamento diferenciado dos casos, pelo privilégio de certas pessoas em detrimento de outras, "pela preocupação em atender primeiramente aos interesses do Estado" (Miranda, 2005). Não é o caso de se estabelecer uma visão depreciativa da burocracia à brasileira, mas apenas salientar suas especificidades, nas quais as distinções com relação ao modelo burocrático-racional não podem ser entendidas como um "defeito" de nosso sistema. Direitos particulares subsistem e a administração é fundada mais nas situações de status e nas relações de dependência pessoal do que na competência (idem, p. 6).

Mesmo que a capacidade de vigilância esteja difundida em termos práticos ou mesmo simbólicos, o monopólio do uso da violência que Weber destacava, dentre outros elementos, para caracterizar o Estado, passa por mudanças a partir dos movimentos das redes transnacionais não vinculadas, direta ou indiretamente, a ele. Castells chama atenção para o fato de que, embora o Estado ainda tenha contornos imponentes em termos de dominação e resistência (duas faces do exercício do poder – Foucault, 2003), os fluxos de informação escapam ao controle do Estado. Tal situação impõe novos desafios às políticas públicas, sejam locais, regionais ou nacionais, sobretudo porque a informação não é mais um produto acabado, mas um processo contínuo de trabalho (Soderberg, 2008 *apud* Albagli & Maciel, 2011, p.17).

1.1 - A Importância do Estabelecimento de Protocolos

Tendo por base o contexto mencionado, observa-se, no país, despreparo ou ausência de condições estruturais para lidar com as configurações contemporâneas emergidas no âmbito da informação, do conhecimento e do poder. Ademais, do ponto de vista legislativo

ainda não há aparatos para dar conta dos atuais desafios colocados pelo paradigma da "Sociedade em Rede":

> Comércio eletrônico, privacidade e ética na Internet, ampliação e reformulação das garantias de direitos de propriedade intelectual, novas regulamentações no campo das telecomunicações, no mundo do trabalho e da educação são apenas algumas das áreas nas quais se impõe a necessidade de novas regras e normas que ordenem os processos de geração, acesso, fluxo, disseminação e uso de informações e conhecimentos, bem como que regulem as novas práticas e relações que se estabelecem em torno dessas atividades. (ALBAGLI & LASTRES, 1999, p.19)

A autora citada lembra que a estes pontos se somam a fragilidade na maioria dos arranjos produtivos de alto valor agregado e conteúdo tecnológico. Por conseguinte, chama atenção para a necessidade de definições e do exercício de um papel mais ativo e coordenado por parte do governo brasileiro que seja, de fato, capaz de orientar uma forma de inserção do país na "Era do Conhecimento". Essa investida poderia minimizar, por exemplo, o risco do país permanecer num cenário dependente e extremamente fragilizado em termos políticos e econômicos. Concomitantemente, essas práticas voltadas para a inovação trazem consigo resistência, porquanto os gestores e demais funcionários "estabelecidos" (Elias & Scotson, 2000) podem interpretá-las como uma ameaça profissional ou mesmo pessoal, principalmente porque no Brasil "(...) os interesses particulares do funcionário e os interesses públicos do cargo, freqüentemente se confundem e os cargos passam a ser uma propriedade de seus ocupantes." (Schwartz, sem data *apud* Lobão, 1997, p.46) Tudo isso se soma a um antigo entrave, qual seja, o déficit de gestão nos variados campos da política pública brasileira.

A introdução de novos padrões em consonância com os ditames emergidos pelo paradigma da "Sociedade em Rede" é fundamental na elaboração e na condução das políticas públicas brasileiras com métodos distintos de resolver e controlar problemas, revisando e potencializando as mesmas. Abandonar práticas orientadas pelo bom senso, pelo "aprender fazendo" e pelo saber prático informado pelos mais experientes em função do tempo de trabalho e experiência é elementar. Assumindo o valor e a importância do saber prático, deve-se reconhecer que ele abre espaço para intervenções de caráter

autoritário e pessoal quando tratamos de políticas públicas que, *a priori*, devem ser desenvolvidas para os indivíduos de maneira universal e uniforme, considerando o pressuposto da igualdade pela diferença. Pensando na primazia do Estado Democrático de Direito, os protocolos têm crucial papel na proteção e garantia dos direitos fundamentais de forma ampliada para os diferentes indivíduos independentemente de seu status:

> (...) Esses protocolos, por isso mesmo, previnem seus agentes de cometerem infrações que poderiam prejudicá-los judicialmente depois de praticadas. A obediência a tais protocolos é uma garantia não apenas daqueles usuários ou clientes das instituições, públicas ou privadas, mas também uma garantia de seus agentes de que agiram corretamente, *by the book*[3]. Não agir assim, portanto, é assumir calculadamente o risco de fazer algo moralmente reprovável, que não encontrará respaldo judicial se por acaso essa desobediência tiver efeitos públicos. A vigilância constante dos agentes visa garantir que suas práticas sigam os protocolos recomendados e deles não se afastem. As rotinas, assim, são discutidas e explicitadas, fazendo-se legítimas para a obediência dos envolvidos (KANT DE LIMA, 2013, p.572-573)

[3] *By the book* é uma expressão da língua inglesa que significa exatamente de acordo com as regras, as normas, o regulamento, a lei.

2 - CONSIDERAÇÕES INICIAIS SOBRE DADOS PESSOAIS E POLÍTICAS PÚBLICAS

As políticas públicas ainda são os instrumentos mais relevantes que o Estado dispõe para alavancar processos de mudança e aprimoramento nos campos social, econômico, político, dentre outros. Considerando as implicações ressaltadas em torno do paradigma da "Sociedade em Rede" (Castells, 2005) que atuam sobre praticamente todas as nações, formatos institucionais, mecanismos e estratégias diferentes passam a ser necessários na elaboração e condução política em qualquer campo.

Uma vez que estamos preocupados não somente com os reflexos e novos contornos políticos, econômicos e sociais a partir da chamada "Era da Informação" no âmbito do Estado, mas sobretudo na vida das pessoas, chega-se ao ponto nodal deste produto – o ser humano. Pezzi (2007) igualmente denota essa primazia:

> O pano de fundo teórico utilizado foi o deslocamento da pessoa humana para o centro das relações jurídicas tanto pública quanto privadas, isto é, o reconhecimento da primazia da pessoa humana sobre o Estado, identificando a pessoa como um fim em si mesma e o Estado apenas como um meio para a garantia e a promoção de seus direitos fundamentais. (idem, p.13)

Pululam, assim, questões que demandam esforços advindos de diferentes campos do conhecimento para serem melhor compreendidas. Até que ponto a velocidade e a facilidade em termos de acesso e de circulação de dados diversos, bem como de informações pessoais pode afetar a vida das pessoas? Qual o papel do Estado nesse cenário? É possível definir limites com vistas a conter invasões indiscriminadas, roubo de informações, comercialização de informações pessoais, no intuito de preservar a privacidade e a dignidade das pessoas? Se sim, em quais domínios da vida esses limites poderiam ser estabelecidos e aplicados? Há ferramentas para garantir confidencialidade de dados pessoais? Há instrumentos para pensar, desenvolver e aplicar a proteção de dados pessoais de maneira universal e igualitária?

Quando se trata da intervenção do Estado com vistas a proteger dados, pode-se associar o estabelecimento deste tipo de procedimento com restrição da liberdade de

expressão, apagamento da memória e da história, risco à privacidade dos cidadãos e aos direitos humanos em nome da vigilância. Seria um contra senso reivindicar o controle do Estado brasileiro nesse caso, após anos de movimento por um regime democrático (ainda que tenhamos uma democracia à brasileira que, dentre outros aspectos, não dá oportunidades iguais de acesso à educação, saúde e justiça, por exemplo)?

Há notadamente distinções entre os domínios público e privado desde o surgimento da cidade-estado na Grécia, uma vez que o homem tinha duas ordens de existência: uma que lhe era própria e outra que lhe era comum (Arendt, 2004). Inicialmente, a relação patrimônio e privacidade demarcavam esse campo. Não era, portanto, algo pretendido como universal, mas uma garantia almejada por apenas alguns segmentos sociais privilegiados. A partir da expansão do pensamento liberal e do individualismo, do surgimento dos meios de comunicação de massa, a proteção do que é privado começou a ser ganhar distintos contornos, se aproximando da privacidade tal qual se conhece (Pezzi, 2007).

Há que se reconhecer as especificidades envolvendo "público" e "privado", no sentido de considerar a liberdade individual, assim como igualdade e justiça coletivas, nem sempre em oposição, mas de forma complementar. A ideia não é conter em setores estanques os direitos humanos e as situações jurídicas de direito privado: "A pessoa, à luz do sistema constitucional, requer proteção integrada, que supere a dicotomia direito público e direito privado e atenda à cláusula geral fixada no texto maior, de promoção da dignidade humana. (Tepedino, 2001, p. 50 *apud* Pezzi, 2007, p.38) Destarte, tal complexidade é ampliada porque

> (...) pode-se provavelmente determinar os campos do direito público ou do direito privado pela prevalência do interesse público ou do interesse privado, não já pela inexistência de intervenção pública nas atividades de direito privado ou pela exclusão da participação do cidadão nas esferas da administração pública. A alteração tem enorme significado hermenêutico, e é preciso que venha a ser absorvida pelos operadores. (TEPEDINO, 2001d, p.19 apud PEZZI, 2007, p.38)

As imprecisões e os imbróglios surgidos a partir das noções de público e privado permeiam a doutrina e a jurisprudência, identifica Doneda (2010, p.101):

> "Doutrina e jurisprudência estão acordes quanto à inexistência de direito absoluto à privacidade, porque pode ser afastada a proteção deste direito quando razões plausíveis superarem o direito individual" (STJ, 2a. T., ROMS 9887, Rel. Min. Eliana Calmon, j. 14.08.2001, DJ 01.10.2001); "O direito à privacidade é constitucionalmente garantido. Todavia, não é absoluto, devendo ceder em face do interesse público" (STJ, 1a. T., ROMS 15771, Rel. Min. José Delgado, j. 27.05.2003, DJ 30.06.2003).

O *habeas data*, uma ação constitucional prevista no Art 5º, que posteriormente ensejou a promulgação da Lei de *habeas data* (Lei 9.507/97). A referida Lei em seu Art 1º reivindica a tutela apenas aos bancos de dados considerados de caráter público: "considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros (…)". A lei é tida como um instrumento originário nos debates e nas proposições acerca da proteção de dados pessoais e da privacidade no Brasil, porquanto é uma

> (...) ação constitucional diretamente vinculada à necessidade de proteção dos dados pessoais, isto é, se refere ao direito do cidadão em ter controle sobre as informações que dizem respeito a sua pessoa, permitindo-lhe decidir o que virá a público ou não, guardando sua privacidade. (...) *Mesmo não tendo o grau de eficácia pretendido, o habeas data despertou o debate acerca do controle de informações pessoais armazenados em inúmeros bancos de dados, cadastros e registros públicos e, por estar garantido e regulamentado, é um instrumento que pode ser utilizado para tutelar os direitos de personalidade, mais precisamente, a tutela da privacidade.* (PEZZI, 2007, p.117, grifo da autora)

Para Doneda (2010), é possível atingir um equilíbrio nesse campo através da aplicação do princípio da proporcionalidade, ou seja, avaliando-se os interesses em jogo, procurando tutelar o conteúdo essencial do direito à privacidade, ao mesmo tempo em que se leva em conta a necessidade da utilização dos dados pessoais no caso concreto. Com isso, os rumos legislativos baseiam-se na proteção do indivíduo e da sua privacidade, bem como na necessidade de definir um patamar de licitude para que os vários serviços que fazem uso de dados pessoais possam operar com maior eficácia, respeitados os direitos individuais

(idem, 2010). Dessa forma, não há soluções prontas, mas a serem construídas caso a caso, corroborando a complexidade da questão, especialmente quando se considera grupos ou segmentos em condições de desigualdade estrutural, por exemplo.

A privacidade é recorrentemente reconhecida por oposição àquilo que é público e que supostamente requer transparência[4], entendida como componente democrático essencial. De acordo com Serra (2002), o debate não é recente. Na obra de Kafka – Processo – há uma denúncia da sobrevivência das sociedades punitivas dos séculos XVII e XVIII, nas quais a administração da justiça era feita à revelia do público e do acusado, uma máquina já "fascista". O autor chama atenção para a importância da transparência como princípio fundamental na organização do Estado e da sua relação com o cidadão. Ademais, a afirmação da transparência como condição necessária da democracia é comum a autores como Rousseau e repetida por diversos teóricos da democracia que pensavam-na de forma indissociável do direito à informação (um dever ativo). Serra (2002) destaca, todavia, três perigos relacionados à transparência, importantes para a construção do presente documento:

1 - a confusão entre o público e o privado – traduzido na pretensão de que tudo, desde o mais íntimo e privado, seja tornado público, publicado. No limite, esta confusão transforma a transparência em panóptico, sociedade democrática em "sociedade de vigilância" já denunciada por Foucault, uma vez que a vigilância tem sido tendência em novas modalidades como "vigilância eletrônica" e "vigilância digital" (a monitoração eletrônica de pessoas se encaixa perfeitamente nesse quadro);

2 - a fabricação de acontecimento pela mídia – redundando na construção de uma falsa transparência;

3 - a onipresença da informação – ameaçando transformar a mídia em agente de controle social, do poder da sociedade sobre o indivíduo. Deleuze utiliza o termo "sociedades de controle", mas podemos denominá-las também de "sociedades da informação", onde os

[4] A Lei de Acesso à Informação nº 12.527/2011 é o principal marco brasileiro em torno do tema.

mecanismos de vigilância assumem novas formas mais eficazes, dando lugar ao controle social que se efetua mediante a informação.

O pesquisador supracitado sublinha uma espécie de mercado de informações que vem se firmando cada vez mais e em ampla escala: "o primeiro imperativo categórico da vida social é que o indivíduo se transforme num consumidor e, acessoriamente, num produtor de informação, que consuma informação, sempre mais informação, independentemente da forma e do conteúdo de tal informação – sob pena de se transformar num verdadeiro pária, num verdadeiro excluído do sistema social (...). (idem, p.208) Por conseguinte, de acordo com sua visão:

> A "sociedade-prisão" de Bentham e Foucault dá, assim, lugar à "sociedade-rede". Imerso num verdadeiro mar de informação em que o essencial e o supérfluo, o verdadeiro e o falso, o genuíno e o fabricado se misturam, se entrelaçam, se confundem, (...) o sujeito tem a sensação de que a realidade e a história se tornaram, enfim, um enorme *écran* ao alcance da mão, do olhar e do ouvido, e de que jorra uma transparência total e permanente – tendendo a esquecer-se de perguntar acerca das razões pelas quais transparece *tanta* transparência. Aqui, e por paradoxal que pareça, *a liberdade de não ser informado* ameaça tornando-se o direito fundamental. (SERRA, 2002, p.208)

2.1 - Proteção de dados pessoais no cenário internacional

A Declaração Universal dos Direitos do Homem[5] (1948) destaca no artigo 3º que "todo o indivíduo tem direito à vida, à liberdade e à *segurança pessoal*". Já no artigo 12º pontua: "*ninguém sofrerá intromissões arbitrárias na sua vida privada*, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei" (grifos da autora).

[5] O Brasil é um dos países signatários da Declaração Universal dos Direitos do Homem, apesar de ser notadamente reconhecido como um país que diariamente viola inúmeros direitos humanos, apresentando frentes políticas e sociais ainda frágeis para a mudança desse cenário, principalmente porque os próprios representantes do Estado são, muitas das vezes, os principais propulsores de tais violações. Para mais referências sobre esse tópico, ver Misse (2011).

Podemos compreender que a Declaração já sinalizava, de algum modo, a necessidade da segurança pessoal e, consequentemente, da segurança no âmbito das informações pessoais, pois a livre circulação destas pode violar direitos fundamentais, tais como a privacidade, a intimidade e a dignidade, que pressupõe a não discriminação.

No mesmo ano da Declaração referida acima, a Declaração Americana dos Direitos e Deveres do Homem no seu artigo 5º indicava semelhante preocupação: “Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar.” As duas Declarações e suas respectivas repercussões ensejaram a privacidade como um direito autônomo no contexto internacional. A Convenção Europeia dos Direitos do Homem, em 1950, firmou o direito à privacidade e, a partir daí, foram editadas diversas diretivas no tema.

No cenário internacional o debate ocorre desde o final da década de 1940, sendo fortemente impulsionado a partir da década de 1990 em diversas frentes. Os diversos documentos e normativos resultantes dessas discussões servem como base para a discussão do presente documento, sobre regras e diretrizes para tratamento e proteção de dados da monitoração eletrônica.

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, refere-se à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, harmoniza as leis nacionais que exigem práticas de gestão de dados de alta qualidade por parte dos “responsáveis pelo tratamento de dados” e as garantias de diversos direitos para os cidadãos. Os dados pessoais são concebidos como qualquer informação relativa a uma pessoa singular identificada ou identificável; é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social. O documento prevê regras específicas sobre a transferência de dados pessoais para fora da União Européia (UE) com o objetivo de assegurar a melhor proteção possível dos dados pessoais quando são exportados para outras Nações.

Outros normativos também trataram do tema e foram considerados no presente documento:

- Regulamento 45/2001 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados;

- Diretiva 58/2002 do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas;

- Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal;

- Decisão 2009/426/JAI do Conselho de 16 de Dezembro de 2008 relativa ao reforço da *Eurojust* e que altera a Decisão 2002/187/JAI relativa à criação da *Eurojust* a fim de reforçar a luta contra as formas graves de criminalidade.

Ainda, desde 2012, a Comissão Europeia tem se dedicado a uma reforma geral das regras de proteção dos dados pessoais em vigor na União Européia, com vistas a restituir aos cidadãos o controle sobre os seus dados pessoais e simplificar o quadro regulamentar para as empresas, o que é encarado como algo essencial para a realização do mercado único digital. A Comissão sublinha que todos têm o direito à proteção dos dados pessoais, apresentando garantia no sentido de que os cidadãos têm o direito de apresentar queixa e recorrer à justiça se os seus dados forem usados de forma abusiva no interior da UE.

O humanismo que transparece à primeira vista na legislação comunitária europeia é analisado por Doneda (2010). A livre circulação dos dados pessoais foi basilar para a consolidação do mercado comum europeu, um dos propósitos maiores do direito comunitário. Por outro lado, ele destaca que a legislação ao mesmo tempo em que assinala a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, assim como dos dados pessoais, não deixa de lado a proteção dos direitos fundamentais das pessoas, denotando um equilíbrio propositivo.

2.2 - A realidade brasileira no cenário dos dados pessoais

Inúmeros Estados, inclusive o Brasil, ainda não têm respostas para todas as questões suscitadas pela proteção e tratamento de dados pessoais na sua intrínseca complexidade. Sem projetar no outro o nosso "atraso" ou "deficiência" nesse campo, percebendo o papel do contexto histórico na transformação tecnológica, política, social e econômica tal qual um processo, deve-se sublinhar que a consolidação do direito à privacidade foi vagarosa e inconstante até mesmo no seu berço doutrinário - os Estados Unidos. Sendo um tema que nunca se esgota, até o momento os dados pessoais e sua necessária proteção são objeto de convenções, tratados, leis e normativas, promovendo constante interlocução entre Estados, organizações e pesquisadores interessados em dar conta de seus dilemas.

Ainda não existe aprovada uma lei exclusiva para a proteção de dados pessoais no país. Mesmo que a Constituição Federal Brasileira no Art. 5º apresente garantias quanto a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas[6], tomando tais elementos como direitos fundamentais e auto-aplicáveis, é imprescindível, conforme já foi destacado, a elaboração de lei específica capaz de garantir a proteção de dados pessoais, sobretudo no caso de dados pessoais sensíveis. Ademais, é preciso constituir uma autoridade nacional de proteção de dados, agências e instrumentos fiscalizadores, ainda inexistentes.

A ausência de uma legislação específica a respeito da proteção de dados pessoais não exime o poder público de oferecer tratamento adequado a esses dados. Pelo contrário, a necessidade de dar cumprimento aos preceitos constitucionais mencionados exige o estabelecimento de protocolos específicos, nos diferentes campos, para assegurar a devida proteção dos dados pessoais.

---

[6] Doneda (2009) ressalta que tais termos e demais profusões na doutrina brasileira para representar a privacidade é considerável, sinalizando a complexidade da questão que se estende também no campo semântico. Além de "privacidade" temos vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos usados, como "privatividade" e "privaticidade", etc. Ele lembra que a falta de uma definição "âncora", que reflita uma consolidação do seu tratamento semântico, não é um problema exclusivo da doutrina brasileira. Assim, "o repúdio à violação da vida privada, apesar da sua ressonância como mandamento e regra geral, não é algo que se pode qualificar concretamente com facilidade, o acaba amenizando o caráter absoluto - e, portanto, algo retórico - que aparentemente possui a norma." (2009, p.1) No documento que se segue, vamos fazer referência aos variados termos usados na Constituição, mas adotaremos o termo privacidade como opção mais razoável e eficaz, por – por unificar os valores expressos pelos termos intimidade e vida privada (idem).

Além das proposições gerais destacadas na Constituição há algumas normas setoriais e decretos que, em temas específicos, oferecem tratamento sobre a proteção de dados. O Código Civil, por exemplo, trata do direito à privacidade no rol de direitos da personalidade em seu Artigo 21, o que ainda se mostra insuficiente no reconhecimento desta como direito autônomo com regramentos próprios:

> A chamada positivação dos direitos de personalidade pelo Código Civil não é o elemento fundador destes direitos, sendo sua função a de orientar a interpretação e facilitar a aplicação e a tutela nas hipóteses em que a experiência e a natureza dos interesses possam ter inspirado o legislador a tratá-las com maior detalhe. (DONEDA, 2006, p.96)

O Marco Civil da Internet (Lei nº 12.965/2014), ao estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil, trata da proteção aos registros, aos dados pessoais e às comunicações privadas passando pela noção de dados pessoais e preservação da intimidade:

> Art. 10. *A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
>
> (...)
>
> Art. 11. *Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais* ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra *em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.* (Lei nº 12.965, de 23 de abril de 2014)

Como não há uma lei específica sobre proteção de dados pessoais, bem como não existe autoridade nacional para controle e fiscalização do cumprimento de disposições legais e regulamentares, movimentos nessa direção acontecem ainda de maneira ainda paulatina,

especialmente em contraste com a realidade de outros países como Argentina e Uruguai[7]. No caso brasileiro, a proteção de dados pessoais ainda permanece notadamente atrelada ao consumo, ao consumidor, numa perspectiva reducionista de direitos e conseqüente limite no exercício da cidadania, um direito constitucional. Há, todavia, projetos e anteprojetos de lei voltados para a proteção de dados pessoais, que serviram também como subsídios conceituais para este documento.

A Lei de Acesso à Informação nº 12.527/2011 indica que informação pessoal[8] é aquela relacionada à pessoa natural identificada ou identificável. O decreto nº 7.724/2012, que regulamenta a referida lei, define informação pessoal como informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem. Conforme já pontuado, a Lei de Acesso à Informação pode ser compreendida como o principal instrumento legal que visa garantir amplo acesso da população às informações de caráter público, ou seja, aquelas que não apresentam elementos capazes de identificar uma pessoa que deve, neste caso, ter seus dados pessoais protegidos:

> Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

A Seção V da Lei nº 12.527/2011, intitulada "Das Informações Pessoais", sublinha, de acordo com o fragmento selecionado, a forma de tratamento das informações pessoais, indicando preocupação acerca da noção de privacidade, intimidade, honra, bem como define acessibilidade, prazo de acesso, punição mediante uso indevido, etc:

> *Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.*

---

[7] Na Argentina existe a Lei 25.326/2000, no Chile a Lei 19.628/1999 e no Uruguai a Lei 18.331/2008.

[8] Dado e informação são elementos distintos. "Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular a ser levado em conta (...). O dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar ao seu receptor. (DONEDA, 2006, p. 152)

> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I - *terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem*; e
>
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
>
> § 2º *Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido*.
>
> § 3º *O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:*
>
> *II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; (...)* (grifos da autora)

A Lei de Acesso à Informação pode ser um instrumento com vistas a ampliar a transparência e a participação social orientada. Vivemos num ambiente onde "a carência de informações não prejudica apenas o acompanhamento social do impacto das ações estatais, mas também a formulação, pelos órgãos públicos, de políticas públicas baseadas em evidências, que possam ser aprimoradas a partir de monitoramento e avaliações" (Pimenta & Moura, 2015). A lei supracitada avança na direção de viabilizar a realização de pesquisas, o que impulsiona inovações no campo científico brasileiro, mas igualmente fomenta a construção de políticas públicas e demais ações correlatas baseadas em evidência e análises empíricas. A privacidade das pessoas a que as informações se referem é resguardada, uma vez que a lei veda tal identificação, ou seja, indica a necessidade de proteção dos dados pessoais. O decreto nº 7.724/ 2012 também define a forma de acesso às informações pessoais por terceiros. O requerente deve comprovar sua identidade, justificar a necessidade e a finalidade de acesso aos dados pessoais, juntamente com a assinatura de um termo de responsabilidade que disponha sobre a finalidade e a destinação que fundamentaram sua autorização, assim como as obrigações a que estará submetido nos termos da lei.

A lei supracitada, por outro lado, não é suficiente para garantir a autodeterminação da pessoa em relação às próprias informações pessoais[9] e a sua privacidade, mesmo porque seu objeto não é a proteção de dados pessoais. Essa situação se agrava no caso dos indivíduos monitorados eletronicamente, pois seus dados pessoais são sensíveis. Isto posto, diante da particularidade da nossa proposta, considera-se algumas definições e proposições do Anteprojeto de Lei que dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural.

O documento, atualmente em debate público organizado pelo Ministério da Justiça[10], pode ser encarado como um esforço legislativo democrático e participativo. O texto base disponibilizado na internet abre espaço virtual para a realização de debates entre sujeitos interessados pelo tema, objetivando complementar, ou até mesmo substituir, formas tradicionais de elaboração pautadas na formação de comissões de juristas.

Na página onde se encontra o anteprojeto de lei referido, além dos comentários de cada pessoa acerca de numerosos pontos, a interlocução é viabilizada. De modo simples e claro, a importância e os objetivos da lei são definidos, tomando dado pessoal como aquele dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos:

> Uma lei sobre proteção de dados permite que o cidadão tenha controle sobre como suas informações são utilizadas por organizações, empresas e pelo governo. Ela tem por objetivo estabelecer padrões mínimos a serem seguidos quando ocorrer o uso de um dado pessoal, como a limitação a uma finalidade específica, a criação de um ambiente seguro e controlado para seu uso e outros, sempre garantindo ao cidadão protagonismo nas decisões fundamentais a este respeito. O impacto maior de uma lei sobre proteção de dados pessoais é o equilíbrio das assimetrias de poder sobre a informação pessoal existente entre o titular dos dados pessoais e aqueles que os usam e compartilham[11].

---

[9] As sucessivas Diretivas da Comunidade Europeia e legislações nacionais criaram apropriados instrumentos de manejo em tema de proteção de dados pessoais, com o que passou o direito à autodeterminação informativa a se identificar com o direito à proteção de dados pessoais. (Navarro, 2011)

[10] Dentre os vários anteprojetos que tratam do assunto vamos considerar o que se encontra disponível no seguinte endereço: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ Acesso em Nov de 2015.

[11] http://pensando.mj.gov.br/dadospessoais/importancia-de-uma-lei-sobre-protecao-de-dados/ Acesso em jan 2015.

2.2.1 - O Código de Proteção e Defesa do Consumidor – um caso à parte

A inexistência de protocolos é algo grave quando pensamos em políticas públicas de qualquer natureza. Doneda (2010) nota, a partir de Carvalho (2003), que a única norma brasileira que lida especificamente com a proteção de dados, exceto o *habeas data*, é o Código de Proteção e Defesa do Consumidor. Ele regula a manutenção de bancos de dados e cadastros de consumidores, determinando para estes diversas garantias. O referido Código, além de ter sido influenciado pelas normas mais modernas relacionadas à proteção de dados pessoais, pauta-se em alguns dos princípios de proteção de dados que serão descritos mais adiante.

Pensar, priorizar e implementar a política de dados pessoais e de informações no Brasil é fundamental, sobretudo de forma a desvencilhá-la da arena do consumo, expandindo-a para situações onde tal proteção tem a capacidade de auxiliar na garantia e na promoção, igual e universal, de direitos fundamentais expressos na Constituição, como já sublinhado.

O Código de Defesa do Consumidor – Lei 8078/1990 – trata na seção VI "Dos Bancos de Dados e Cadastro de Consumidores" o direito do consumidor ao acesso às informações pessoais e de consumo sobre ele e suas fontes respectivas

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° *Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.*
>
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. (grifo da autora)

A partir do fragmento, constata-se que legislação visa proteger o consumidor através de regras precisas, não deixando em segundo plano o tratamento e a proteção de seus dados pessoais. Cadastros e dados, além de serem objetivos, devem eliminar informações negativas após o período de cinco anos. Não há uma essencialização permanente de uma situação ou de uma identidade socialmente negativa como a de “devedor”. Assim, mesmo que os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres sejam considerados entidades de caráter público, após a prescrição de débitos, os Sistemas de Proteção ao Crédito não podem fornecer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. Isso não deixa de ser um aparato de proteção para os consumidores e, numa visão macro, uma forma mais justa de perceber os indivíduos enquanto plurais, produzidos e produtores das relações sociais, não apenas numa dicotomia totalizante como “nome limpo” x “nome sujo”, “consumidor” x “devedor”, dentre outras.

O mesmo Código, no Título II - “Das Infrações Penais”, estipula penas de detenção e multas em casos diversos. Os Arts. 72 e 73 perpassam a proteção de dados diretamente, delimitando penalidades e multas:

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
>
> Pena Detenção de seis meses a um ano ou multa.
>
> Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
>
> Pena Detenção de um a seis meses ou multa.

Buscando assegurar a implementação do Código, o Procon (Proteção ao Consumidor) visa realizar a defesa do consumidor e promover a prática justa no mercado de consumo. Ao Procon cabe, por exemplo, combater irregularidades no mercado que caracterizem infração às disposições do Código de Defesa do Consumidor. Há, portanto, para os consumidores brasileiros uma legislação específica e detalhada, assim como uma agência, instrumentos e órgãos fiscalizadores.

Enquanto há apenas projetos de lei relativos à proteção de dados pessoais, que permitiriam resguardar a cidadania em uma perspectiva mais ampla, no território do consumo há limites bem estabelecidos para o tratamento e a proteção de dados dos consumidores através de um código específico - o consumidor assume, por esse olhar, um status diferenciado. A proteção dos dados pessoais no nosso país, por ínfima que seja, está vinculada ao mundo do consumo. A proteção dos dados pessoais deve ser expandida para outros domínios da vida social, conferindo qualidade na gestão das políticas públicas e maior aplicabilidade aos preceitos constitucionais. Essa expansão deve necessariamente abarcar os dados pessoais sensíveis que, intrinsecamente, apresentam enorme potencial discriminatório e lesivo aos seus titulares, como os dados pessoais da monitoração eletrônica de pessoas.

3 - PARTICULARIDADES DA MONITORAÇÃO ELETRÔNICA DE PESSOAS NO BRASIL

Como revelado no primeiro diagnóstico nacional da política de monitoração eletrônica de pessoas (Brasil, 2015h)[12], os serviços de monitoração foram implementados no país a partir de 2010, abarcando atualmente 19 Unidades da Federação, com inúmeros projetos de expansão. Esses serviços estão organizados, todavia, sem normas ou diretrizes de fluxos capazes de orientá-los a partir de uma perspectiva nacional. Desde julho de 2015, além de investimentos em bibliografia nacional e internacional, diálogos com pesquisadores e profissionais, inúmeras visitas vêm sendo realizadas de modo a amparar a construção dos produtos da presente consultoria, bem como orientar a política por meio de contextos específicos e evidências empíricas, subsidiando o modelo de gestão dos serviços de monitoração eletrônica.

Os serviços de monitoração eletrônica são pouco eficazes no desencarceramento[13]. As medidas cautelares ou protetivas juntas somam apenas 12,63% dos serviços em todo o país, sendo a execução penal responsável por 82,86% dos serviços oferecidos para 18.172 pessoas (número que cresce em consideráveis proporções).

A ausência de informações integradas entre Poder Executivo e Poder Judiciário impedem, atualmente, a aferição de indicadores capazes de mensurar o impacto da monitoração eletrônica na redução do encarceramento, inclusive no caso de sua utilização no âmbito das medidas cautelares diversas da prisão. Além disso, são poucas as pesquisas realizadas para aferir o efeito do uso das "tornozeleiras" nas pessoas monitoradas, quanto aos aspectos de dessocialização, estigmatização e danos físicos e psicológicos. O diagnóstico supracitado apresenta, contudo, indicativos de uma série de violações aos direitos

[12] O documento que consiste no primeiro diagnóstico dos serviços de monitoração eletrônica no Brasil – primeiro produto da presente consultoria – foi lançado e publicado pelo Departamento Penitenciário Nacional (DEPEN) em parceria com o Programa das Nações Unidas para o Desenvolvimento (PNUD) no dia 08 de dezembro de 2015 sob o título "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". Acesso em janeiro de 2016. Disponível em https://www.justica.gov.br/noticias/mj-divulga-primeiro-diagnostico-nacional-sobre-monitoracao-eletronica-de-pessoas

[13] 86,18% das pessoas monitoradas estão na fase de execução penal (Brasil, 2015). Esse indicador revela a utilização precária da monitoração como alternativa à prisão e, de forma mais abrangente, a potencialidade punitiva ainda dominante no imaginário social quando o assunto perpassa a arena penal.

fundamentais dos indivíduos monitorados. A monitoração, por si só, pode ser considerada uma medida constrangedora e altamente capaz de degradar a vida social do indivíduo nos âmbitos da família, do trabalho e demais relações sociais. Nesse sentido, foi apontada a necessidade de desenvolvimento de fluxos e práticas locais voltadas ao encaminhamento do público a programas e políticas de proteção e inclusão social já instituídos e disponibilizados pelo poder público Nas centrais, há investimentos pouco significativos em serviços psicossociais. A exemplo, apenas 06 centrais contam com esses profissionais e em alguns casos o acompanhamento psicossocial é considerado secundário pela ausência de infra estrutura adequada e mesmo pela predominância do "controle e vigilância" como fundamentos de um serviço que visa oferecer resposta e tratamento rápido a qualquer tipo de incidente.

O estigma é um dos principais problemas associados aos serviços de monitoração. Os indivíduos monitorados necessariamente estão sob a tutela do Estado, tanto no caso de cumpridores de medidas cautelares diversas da prisão e de medidas protetivas de urgência ou apenados em diferentes estágios da execução penal. Condenado, ou não, tanto faz. Um elemento fundamental que o equipamento de monitoração lhe imputa é 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. Lembrando que "o normal e o estigmatizado não são pessoas, e sim perspectivas que são geradas em situações sociais durante contatos mistos, em virtude de normas *[valores e significados]*[14] não cumpridas que provavelmente atuam sobre o encontro". (idem, p.148-149) O autor, ao discorrer sobre desvio social, enfatiza que os "delinqüentes e criminosos", por exemplo, são pessoas consideradas engajadas numa espécie de negação coletiva da ordem social, faltando-lhes moralidade, representando "defeitos nos esquemas motivacionais da sociedade". A monitoração, segundo essa perspectiva, compromete engajamentos sociais dentro do princípio da normalidade, ignorando a promoção da igual dignidade e dos direitos humanos.

Atualizando a perspectiva goffmaniana, incluem-se os processos vividos pelas pessoas monitoradas no rol das situações estigmatizantes. Do ponto de vista simbólico, o

[14] Grifo da autora.

monitorado é um indivíduo que está na liminaridade entre a prisão – a “tornozeleira” é um símbolo associado ao cárcere – e a liberdade, uma vez que esta última é limitada no tempo e no espaço, vigiada e ameaçada por incidentes de ordem técnica ou mesmo tratamentos e respostas fundamentadas no “bom senso” de cada funcionário que pode levá-lo ao cárcere. No entanto, do ponto de vista prático, o monitorado não está numa instituição penal e no caso dos cumpridores de medidas, muitos sequer passaram em algum momento de suas vidas pelo ambiente prisional, não tendo qualquer familiaridade com esse tipo de socialização. Com isso, as pessoas monitoradas eletronicamente, independentemente de estarem na fase de instrução ou execução penal, devem ter seus direitos fundamentais garantidos. Ao estarem sob a tutela do Estado, seus direitos não podem ser transformados em benefício, como se os sujeitos monitorados eletronicamente fossem "beneficiados com uma medida alternativa", quando o que lhes caberia, na verdade, seria a prisão - narrativa recorrente identificada em discursos de gestores e servidores atuantes nos serviços.

As respostas dadas pelas centrais diante de incidentes diversos, como aqueles relacionados à descarga de bateria e áreas de inclusão e de exclusão (limites definidos pelos juízes ou pelas Centrais e traçados no mapa do sistema de monitoramento das Centrais)[15] causam enormes danos ao cumpridor. Além disso, a gestão dos serviços de monitoração eletrônica, em muitos casos, promove o compartilhamento de dados pessoais com instituições de segurança pública de forma indiscriminada, não protocolar e ilegal, por não respeitar propriamente a privacidade do monitorado:

> O sistema de monitoramento será estruturado de modo a preservar o sigilo dos dados e das informações da pessoa monitorada. (Decreto-Lei nº 7.627/2011, Art. 6º)

Os serviços de monitoração são encarados pela maioria dos operadores como ferramenta de segurança pública e, portanto, plenamente acessíveis por instituições

[15] No primeiro caso, a definição da área no sistema de monitoramento prevê limites territoriais dentro dos quais o monitorado é autorizado a circular em horários previamente estabelecidos. No segundo caso é definida uma área no território onde o monitorado não está autorizado a entrar ou circular. Os limites estabelecidos pelos juízes costumam variar muito. O raio da área de exclusão pode variar de 250 a 5000 metros, o que implica violações constantes no sistema de monitoramento, sugerindo a própria mudança de endereço do monitorado para outros bairros ou cidades e restrições no desenvolvimento de atividades laborais e educativas, impactando no processo de integração social. (Brasil, 2015h)

policiais, por exemplo. Torna-se uma prática naturalizada o compartilhamento de dados das pessoas monitoradas com a polícia, o que indica um fraco alinhamento das políticas penais de cada Unidade da Federação, representada neste caso pelas Centrais de Monitoração Eletrônica, com a atual política penitenciária nacional (Brasil, 2015h).

Deve ser objeto de atenção específica, sobretudo, o fato de a realização dos serviços não estar atrelada – formal ou informalmente – aos princípios de proteção de dados e de segurança da informação nas Centrais e empresas contratadas para executar os serviços, alguns desenvolvidos com fundos do próprio DEPEN por meio de convênios. Investigações de campo realizadas ao longo da presente consultoria revelam que diretores e servidores das Centrais, que, em tese, teriam um entendimento mais abrangente sobre o assunto, muitas vezes ignoram o tema, indicando que "isso tudo está no contrato". Daí a necessidade de construção de protocolos para orientar a atuação das Centrais no tema, uma vez que "(...) o indivíduo que confia seus dados deve contar com a tutela jurídica para que estes sejam utilizados corretamente, que se trate de um organismo público ou privado." (Limberger, 2007, p.60 apud Pezzi, 2007, p.76)

3.1 - Audiências de Custódia e Monitoração Eletrônica

As Audiências de Custódia surgem como um dos pontos centrais no avanço da política penal brasileira numa promessa desencarceradora, visando conter a enorme massa de presos provisórios, isto é, 41% da população carcerária segundo os dados do Infopen 2014 (Brasil, 2015g). O indicador, além de revelar um modo sistemático, abusivo e desproporcional de aprisionamento, sinaliza a urgência das mudanças já em andamento.

Os Acordos de Cooperação nº 05, nº 06 e nº 07, de 09 de abril de 2015, firmados entre o Conselho Nacional de Justiça e o Ministério da Justiça, sublinham que as medidas cautelares diversas da prisão aplicadas no âmbito das audiências de custódia serão encaminhadas para acompanhamento em serviços instituídos preferencialmente no âmbito do Poder Executivo estadual, denominados Centrais Integradas de Alternativas Penais ou com outra nomenclatura, bem como às Centrais de Monitoração Eletrônica, em casos estritos.

Os referidos acordos prevêem que a adoção das medidas tenha como finalidade, além da redução da população prisional, a promoção da autonomia e da cidadania da pessoa submetida à medida; o incentivo à participação da comunidade e da mulher em situação de violência doméstica e familiar na resolução dos conflitos; a auto responsabilização e a manutenção do vínculo da pessoa submetida à medida com a comunidade, com a garantia de seus direitos individuais e sociais; e a restauração das relações sociais. Destarte, conforme nosso entendimento e a Resolução 213, de 15 de dezembro de 2015, do Conselho Nacional de Justiça[16], a aplicação da monitoração eletrônica deve ser residual, impedindo seu crescimento exponencial[17]:

> A aplicação da monitoração eletrônica será excepcional, devendo ser utilizada como alternativa à prisão provisória e não como elemento adicional de controle para autuados que, pelas circunstâncias apuradas em juízo, já responderiam ao processo em liberdade. Assim, a monitoração eletrônica, enquanto medida cautelar diversa da prisão, deverá ser aplicada exclusivamente a pessoas acusadas por crimes dolosos puníveis com pena privativa de liberdade máxima superior a 04 (quatro) anos ou condenadas por outro crime doloso, em sentença transitada em julgado, ressalvado o disposto no inciso I do caput do art. 64 do Código Penal Brasileiro, bem como a pessoas em cumprimento de medidas protetivas de urgência acusadas por crime que envolva violência doméstica e familiar contra a mulher, criança, adolescente, idoso, enfermo ou pessoa com deficiência, sempre de forma excepcional, quando não couber outra medida cautelar menos gravosa. (Conselho Nacional de Justiça, Resolução 213, 2015, Protocolo I)[18]

O Departamento Penitenciário Nacional, em parceria com o Conselho Nacional de Justiça, deve indicar procedimentos com vistas a minimizar os impactos negativos causados durante e, igualmente, após o término da medida. O estabelecimento de diretrizes e regras envolvendo os dados pessoais (informações pessoais, a localização do monitorado, as áreas

16 A Resolução 213, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, dispõe sobre a apresentação de toda pessoa presa à autoridade judicial no prazo de 24 horas.

17 A partir de constatações em campo notamos que muitos juízes não costumam se sentir seguros com a aplicação de medidas sem o uso monitoração, evidenciando um exagero pelo controle e vigilância disciplinar, assim como desconhecimento dos magistrados em torno dos serviços.

18 O Protocolo I da Resolução 213, de 15 de dezembro de 2015, do Conselho Nacional de Justiça descreve procedimentos para a aplicação e o acompanhamento de medidas cautelares diversas da prisão para custodiados apresentados nas audiências de custódia.

de inclusão e de exclusão, as restrições de horários, etc.) passa a ser uma das prioridades dentro dos atuais contornos da política penitenciária nacional. Os conceitos e bases estão assentados em paradigmas pautados pelos direitos humanos, prevendo garantias básicas na autodeterminação das pessoas em relação às suas informações pessoais e na manutenção da privacidade e dignidade.

4 - CONSIDERAÇÕES SOBRE TRATAMENTO E PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO NA MONITORAÇÃO ELETRÔNICA DE PESSOAS

Quando dicotomias totalizantes – “preso”, “monitorado”, “custodiado” x “cidadão”, “trabalhador”, “homem de bem” – são criadas para “colocar cada um no seu lugar e lá mantê-lo”, desconsidera-se as mudanças inerentes a qualquer indivíduo e sociedade, como se vivêssemos sob uma estrutura estanque, o que constitui uma completa ilusão. Nesse ponto, o presente documento, como parte integrante do modelo de gestão para os serviços de monitoração eletrônica de pessoas, tem um caráter inovador, plural e inclusivo, sobretudo porque não considera o indivíduo monitorado eletronicamente meramente como um sujeito do direito penal, mas como um sujeito de direitos que, estando em liberdade – ainda que vigiada – deve ter não somente obrigações, mas direitos e garantias. Diante de sua capacidade de mudança, inerente à condição humana, e de aderência às normas, os serviços de monitoração devem contemplar, conforme já foi dito e apontado no primeiro diagnóstico da política (Brasil, 2015h), atividades de acompanhamento psicossocial, visando redução de danos ao cumpridor que deve ter uma vida mais próxima possível da normalidade e promoção da igual dignidade humana, o que inclui o direito fundamental à privacidade. Isto posto,

> Não obstante sejam salutares as medidas que evitem o cárcere, também é necessário atentar para que as medidas restritivas de direitos estejam em consonância com o anseio de um Direito Penal mínimo, o que não significa tão só a cautela na tipificação de condutas essencialmente necessárias de repressão penal, mas ainda, e principalmente, que sejam elencadas penalidades alternativas que visem somente ao seu cumprimento, e que, para tanto, não extrapolem os limites da dignidade da pessoa do apenado, tampouco o conduza a constrangimentos injustificados. (ESTORILIO, 2012, p.16)

O Código de Processo Penal é claro nesse assunto quando trata da reabilitação no capítulo II nos artigos elencados abaixo:

> Art. 743. A reabilitação será requerida ao juiz da condenação, após o decurso de quatro ou oito anos, pelo menos, conforme se trate de condenado ou reincidente, contados do dia em que houver terminado a execução da pena principal ou da medida de segurança detentiva, devendo o requerente indicar as comarcas em que haja residido durante aquele tempo.
>
> Art. 748. A condenação ou condenações anteriores não serão mencionadas na folha de antecedentes do reabilitado, nem em certidão extraída dos livros do juízo, salvo quando requisitadas por juiz criminal.

Presumimos assim, sobretudo pelo conteúdo do Art. 748, o direito voltado para garantir que nenhuma identidade ou representação social degradante seja essencializada e reduzida de forma permanente. O status de "monitorado", quando não de "preso"[19], é fundamentalmente transitório, até mesmo pelo fato de não haver previsões legais de condenação à prisão perpétua, sendo um dos objetivos do sistema prisional, a despeito de sua ineficácia neste ponto específico, promover "ressocialização" para o retorno do indivíduo à sociedade. O Código indica sigilo acerca da passagem pelo cárcere após determinado período de tempo ao final da execução da pena ou da medida de segurança detentiva, imprimindo o apagamento de rótulos identitários que têm como fonte experiências pessoais no universo prisional, ou seja, que fogem ao modelo social reificado que, via de regra, desiguala e exclui os "ex-presos". Se isso é possível e tem previsão legal no caso da prisão, o mesmo deve ser considerado no caso da monitoração eletrônica, sobretudo por ser uma medida intermediária, que não é propriamente o encarceramento.

Se, no entendimento do juiz, a prisão não foi necessária, a medida aplicada (cautelar ou protetiva de urgência) é suficiente para a tutela pretendida. A liberdade deve ser, portanto, uma precípua para o cumpridor aderir às normas por meio do encaminhamento aos serviços psicossociais. A construção de uma política de monitoração eletrônica pautada pela dignidade da pessoa humana deve necessariamente garantir que a pessoa monitorada -

[19] Em muitas Centrais de Monitoração Eletrônica é recorrente ouvir o termo "preso" para designar qualquer pessoa monitorada, tanto na fase de execução quanto de instrução penal. As formas de tratamento pessoal seguem o fluxo ditado pelo sistema prisional que perpetua rótulos e estigmas, prática que não condiz com a nossa Constituição que prevê no Art 5º, LVII - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória. Daí, o termo "preso" ser altamente impróprio nesse contexto. Temos como "pessoa monitorada", "pessoa em monitoração", "cumpridor de medida" são considerados menos degradantes.

antes e depois da medida - tenha uma vida mais próxima possível da normalidade, num esforço de minimizar qualquer tipo de dano (físico, moral, psicológico, etc.), bem como o acesso a direitos fundamentais que possam promover e assegurar uma rotina pautada pelo princípio da normalidade[20].

Consequentemente, proteger e tratar os dados pessoais dos monitorados por meio de protocolos adequados e em sintonia com a igual dignidade humana, de maneira a garantir direitos constitucionais voltados para proteção da honra, imagem e vida privada, ou mais precisamente, sua privacidade, durante o cumprimento das medidas é fundamental, assim como ao término destas. O Decreto 7.627/2011 já tece exigências neste sentido:

> Art. 5º O equipamento de monitoração eletrônica deverá ser utilizado de modo a respeitar a integridade física, moral e social da pessoa monitorada.

A integridade moral e social está estritamente vinculada à proteção da honra, imagem, privacidade, dignidade e, por conseguinte, dos dados pessoais dos monitorados, sobretudo pelo risco que sua má utilização apresenta.

As legislações internacionais, mais especificamente, as diretivas da União Europeia seguem rumos que reforçam o paradigma da segurança em nome do Estado. Destarte, não se aplicam tratamento de dados pessoais quando o assunto permeia a arena penal, conforme especificado:

> Artigo 1º
> Âmbito e objetivos
> 3. A presente directiva não é aplicável a actividades fora do âmbito do Tratado que institui a Comunidade Europeia, tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, *e em caso algum é aplicável às actividades relacionadas com a segurança pública, a defesa, a segurança do Estado* (incluindo o bem-estar económico do Estado quando as actividades se relacionem com matérias de segurança do Estado) *e as actividades do Estado em matéria de direito penal.*

[20] Ter uma vida pautada pela normalidade significa a real possibilidade de desenvolver atividades sob os padrões sociais impostos para a sociedade como um todo. Estorilio (2012) nos ajuda a clarear esse princípio, ao afirmar que o "(...) trabalho lícito em busca da subsistência não deve ser impedido sob pena de romper com qualquer um dos 'elementos vitais' trazidos pelo constituinte no inc. IV". (p.23) Acrescentamos igualmente a educação, a saúde, o lazer, a família, etc.

> (Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002) (grifos da autora)

O que se propõe no presente documento é inovador tanto para a proteção de dados pessoais como para o campo penal, porquanto a pessoa – apenado, monitorado ou egresso – é encarada como figura central da política penal. As construções políticas ainda encontram entraves segundo os preceitos punitivistas predominantes, porém "(...) não se pretende mais nenhuma teoria que aplique o direito penal justificando o direito de punir, mas sim que se saiba construir limites aos poderes desta punitividade."(Estorilio, 2012, p.20) Vislumbra-se o poder não na sua dimensão restritiva, mas especialmente produtiva e positiva (Foucault (2003). Logo,

> Este tipo de debate tem repercussões no campo da política (*politics)* como esfera de disputa de poder, mas igualmente no campo das políticas (*policies)* como estratégias de ação. Isso faz emergir implicações diferentes a possíveis estratégias de fortalecimento e afirmação de segmentos sociais marginalizados, de projeção de países e regiões periféricos no sistema internacional, assim como de construção democrática, do exercício da cidadania e do desenvolvimento em termos mais abrangentes. (ALBAGLI & MACIEL, 2011, p.34)

Trata-se aqui de uma política pública, uma política penal, ou seja, distinta a política de segurança pública em função de seus distintos sujeitos e objetos. O principal sujeito da política penal – isso se estende à monitoração eletrônica – é o indivíduo, a pessoa custodiada, a pessoa monitorada. Em conseqüência disso, os dados pessoais do monitorado, incluindo sua geolocalização[21], são dados sensíveis que podem afetar direta e indiretamente sua vida:

[21] Geolocalização ou localização georreferenciada é um recurso capaz de revelar a localização geográfica por meio de endereço IP, conexão de rede sem fio, torre de celular com a qual o telefone está conectado, hardware GPS dedicado que calcula latitude e longitude da informação enviada por satélites no céu. No caso da monitoração eletrônica, essa informação é compartilhada com as empresas que prestam serviços às Centrais ou as próprias Centrais de Monitoração Eletrônica. Um dos métodos de geolocalização triangula a posição do indivíduo baseando-se na sua localização relativa das diferentes torres da sua operadora de celular (daí, por exemplo os equipamentos de monitoração geralmente adotarem dois chips de operadoras distintas). Este método é rápido e não necessita de qualquer hardware de GPS dedicado, mas ele só pega uma ideia aproximada de onde o indivíduo está. Outro método usa algum hardware de GPS dedicado no aparelho para se comunicar com algum satélite de GPS dedicado que está orbitando no planeta. O GPS normalmente pode identificar a localização a poucos metros. O lado negativo de um chip de GPS dedicado no aparelho é o alto

> O desequilíbrio de forças causado pelo uso de dados sensíveis armazenados em banco de dados é causa suficiente para que essa categoria tenha um atendimento especial. Como duas pessoas poderão concorrer a uma vaga de emprego, nas mesmas condições, considerando que o empregador tem disponível o acesso a um banco de dados em que consta que um deles pertenceu ao sistema carcerário em razão de cumprimento de pena?[22] (Trecho extraído do Jornal Folha de São Paulo de 4 de junho de 2006 *apud* PEZZI, 2007, p.92)

De modo geral, os dados dos indivíduos monitorados eletronicamente são mantidos em bancos informatizados de dados pessoais desenvolvidos e geridos por empresas que atuam no ramo. A alimentação dos bancos é realizada por funcionários da empresa contratada; variados servidores públicos do estado, como agentes penitenciários; terceirizados, etc. Eles são criados e mantidos sem critérios de proteção e tratamento estabelecidos nacionalmente, comprometendo a boa gestão dos serviços.

É um não dito ou pouco se fala sobre os perigos embutidos no tratamento de dados pessoais na área penal, provavelmente porque o "preso" ou o "monitorado" não são tidos como sujeito de direitos. A monitoração é um sistema institucionalizado de risco. Aliás, risco e perigo sempre existiram, todavia o "fatalismo é a recusa da modernidade – o repúdio a uma orientação de controle em relação ao futuro em favor de uma atitude que deixa que os eventos venham como vierem" (Giddens, 105). Daí, o a necessidade de mudanças por meio de protocolos com vistas a resguardar os direitos fundamentais das pessoas monitoradas, pois entende-se que

> O descontrole e a incerteza sobre quem dispõe ou possui acesso a dados pessoais ultrapassa o poder de escolha que delimita e define a esfera pessoal de cada ser humano, desnudando o mais íntimo de forma avassaladora. A necessidade de tutela jurídica para aqueles que confiam seus dados pessoais a entidades públicas

consumo de energia. O *Google Maps* usa os dois métodos: primeiro surge um grande círculo que aproxima sua posição (procurando uma torre de celular próxima), então um círculo menor (triangulando com outras torres de celulares), então um único ponto com sua posição exata (pego por um satélite de GPS).

[22] A reportagem destaca: "Governo quer vender dados dos paulistas". De acordo com a autora supracitada, tratava-se de um projeto de lei apresentado pelo secretário de segurança pública, Saulo de Castro Abreu Filho, autorizando empresas particulares a administrarem e comercializarem bases de dados com ficha pessoal de todos os indivíduos do estado.

> ou privadas se torna evidente na medida que esses dados possuem um valor econômico em razão da sua utilização para fins comerciais. (PEZZI, 2007, p.10)

Acrescenta-se, dentre outros, o valor político no caso da monitoração eletrônica. A potencialidade de dano existe para o indivíduo que tem seus dados pessoais armazenado em um banco de dados. Tais bancos são ferramentas que permitem o avanço de limites na esfera da privacidade, por conta de sua potencialização geométrica no armazenamento de praticamente qualquer tipo de dado e com qualidade. Assim, "(...) se é perceptível o valor de se ter um banco de dados organizado individualmente, o que se dirá quando os mesmos são cruzados. O poder que emana dessa fusão se consagra em uma informação mais precisa, porém mais invasiva (...). Esse poder toma uma dimensão ainda maior em virtude da facilidade de transmissão e circulação dos dados." (idem, p.10 e 11)

É necessário prever, cobrar de modo instrumental e protocolar a responsabilidade do gestor de um arquivo de monitoração eletrônica para que se mantenha diligente e atento à manipulação desses dados, bem como dos demais funcionários que lidam com tais dados. Aliás:

> A pessoa monitorada deverá receber documento no qual constem, de forma clara e expressa, seus direitos e os deveres a que estará sujeita, o período de vigilância e os procedimentos a serem observados durante a monitoração. (Decreto nº 7.627, de 24 de Novembro de 2011, Art. 3º)

Com isso, entendemos que os direitos, os deveres e os procedimentos durante a medida devem ser informados por escrito à pessoa monitorada. Uma vez que a privacidade é um direito e os procedimentos decorrentes da monitoração incluem, necessariamente, o tratamento dos dados pessoais dos monitorados, este tipo de protocolo é imprescindível. Além disso, a não positivação de um direito fundamental não implica na sua inexistência, pois há direitos humanos fundamentais não inscritos no texto constitucional possíveis de concretização e desenvolvimento plural. Daí, a norma com *fattispecie aberta* (Baldassare) ou, melhor dizendo, o princípio da não tipicidade dos direitos fundamentais. (Canotilho, 2003)

O termo de confidencialidade assinado entre a empresa e a contratante dos serviços é a forma mais utilizada no campo da segurança da informação. No caso da monitoração, esse procedimento, embora necessário, não é suficiente se não for estendido para todos os indivíduos que lidam com os dados pessoais. Ou seja, qualquer um que recolha, registre, organize, conserve, adapte, altere, recupere, consulte, transmita ou realize qualquer tipo de operação que envolva dados pessoais, independentemente de serem servidores públicos ou funcionários contratados atuando nas centrais, empresas e secretarias devem assinar, neste caso, um termo de tratamento e proteção de dados pessoais dos monitorados, das mulheres em situação de violência doméstica, bem como dos familiares, amigos, vizinhos e conhecidos tanto dos monitorados quanto das mulheres em situação de violência doméstica e familiar.

Há, com certeza, potencial lesivo na publicização de tais bancos de dados, uma vez que não lidam com pessoas indeterminadas ou anônimas, como é o caso dos bancos de dados de pesquisas de opinião e do censo. Ele é construído e alimentado a partir dos dados pessoais do monitorado e da mulher em situação de violência doméstica e familiar, isto é, dados relacionados à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos.

Os dados gerados pela monitoração eletrônica, por si só, são caracterizados como dados pessoais sensíveis, conforme já salientado na introdução do presente documento. São dados pessoais sensíveis, não são dados abertos e, diante dos riscos potenciais que carregam, não é qualquer pessoa que pode livremente usá-los, reutilizá-los e redistribuí-los.[23]

Existe nos dados sensíveis uma potencialidade para o uso discriminatório ou particularmente lesivo não somente a um indivíduo como a uma coletividade (os monitorados em saída temporária podem ser um bom exemplo, assim como parentes e amigos dos monitorados). Descuidos e mau uso destes dados pode incitar perseguições de vítimas[24] e prisões injustificadas, alimentadas por metas de prisão estipuladas na área de

[23] Para mais informações sobre dados abertos, ver o Portal Brasileiro de Dados abertos. Disponível em http://dados.gov.br/dados-abertos/ Acesso em janeiro de 2016.

[24] Não é o caso de desconsiderar ou colocar em segundo plano os direitos e papeis da vítima no sistema de justiça criminal. O ideal é promover práticas que dêem conta de tratar com respeito aos direitos da vítima e do autor da infração penal. Aliás, segundo os fundamentos da Política de Alternativas Penais é primordial responsabilizar com *autonomia e liberdade*; promover o envolvimento, a reparação e a proteção da *vítima* e da

segurança pública, por exemplo. Tratamento e proteção adequados, em consonância com os princípios de segurança da informação são ainda mais urgentes e necessários na medida em que também são armazenados dados de familiares, amigos, vizinhos e conhecidos das pessoas monitoradas. Esse procedimento, de acordo com as centrais, ocorre para facilitar a localização da pessoa monitorada em caso de algum incidente quando esta não possuir um telefone ou não atender seu próprio telefone.

Não somente a privacidade pode ser comprometida, mas a segurança da pessoa monitorada a partir do mau uso do banco de dados. Não raro,

> cultiva-se a ideia de que o compartilhamento de tais dados com a polícia é uma prática adequada à monitoração que protege o próprio monitorado, enquanto se constrói uma sociedade mais segura, atentando-se àqueles que por "suspeição sistemática" já "costumam dar mais problemas". Segundo observações feitas em campo, informações da CGPMA e do GT de monitoração, os indivíduos que portam a "tornozeleira" são facilmente identificados e sistematicamente suspeitos no caso de "eventos crime", o que evidencia violação constitucional quanto à presunção de inocência. (BRASIL, 2015h, p.47)

O tratamento e a proteção dos dados sensíveis auxiliam o combate de formas de tratamento degradantes para as pessoas monitoradas, as mulheres em situação de violência doméstica familiar e, igualmente, para seus familiares, amigos, vizinhos e conhecidos, o que encontra respaldo no Art. 5º da Constituição:

> 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:
> III - *ninguém será submetido à tortura nem a tratamento desumano ou degradante*.
> LVII - *ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória.* (grifos da autora)

---

comunidade; atuar *de ponta a ponta* no sistema de justiça e investir na *mediação* e nas *práticas restaurativa,* o que está consolidado na "Diretriz n.4: Às diversas práticas de alternativas penais em curso no Brasil, deve-se buscar agregar o fortalecimento das potencialidades e afirmação das trajetórias das pessoas, o protagonismo das partes, a participação da vítima, a reparação de danos e a restauração das relações, sempre que possível." (Brasil, 2015e, p.49)

Ademais, do ponto de vista do dano moral, o tratamento degradante, conforme o Art.186 do Código Civil é um ato ilícito:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Complementando, almeja-se "uma nova leitura do princípio da igualdade, e sua intenção é a de que os dados armazenados não sirvam para prejudicar as pessoas. (...) buscando-se uma maior proteção tanto na sua coleta como na guarda ou na utilização para os fins aos quais foram captados, evitando-se, assim, situações de desigualdade". (Limberger *apud* Pezzi, 2007, p.92)

Informação e conhecimento sempre constituíram importantes pilares da humanidade. A Internet ainda não teve suas repercussões e aplicações devidamente dimensionadas. Uma vez que os dados das pessoas monitoradas geralmente são mantidos em bancos de dados com acesso local ou mesmo *web*, o rigor no tratamento e proteção deve ser maior porque ao longo desse dimensionamento e aprendizado os equívocos e os erros podem surgir com mais facilidade. O eventual "vazamento de banco de dados" contendo informações pessoais sobre indivíduos monitorados eletronicamente, por culpa ou dolo, tem um enorme potencial discriminatório. Estes dados podem ser compartilhados indiscriminadamente através da Internet, promovendo e intensificando a criminalização destes indivíduos em diversas esferas da vida social, durante e após o cumprimento da medida. Isso pode afetar negativamente sua socialização e acesso a direitos fundamentais como trabalho, saúde, educação, dentre outros.

A privacidade e a intimidade são direitos fundamentais que podem ser facilmente violados no caso das pessoas monitoradas eletronicamente. Os dados pessoais de geolocalização merecem especial proteção e tratamento porque apresentam elevado potencial lesivo, possibilitando excessivas exposições da intimidade não estipuladas na medida judicial, o que consiste em abuso de poder. Além de estes dados serem intrinsecamente sensíveis, a disponibilidade de *softwares* de cruzamento de dados capazes de mapear perfis individuais de personalidade amplia a necessidade de proteção.

A complexidade inerente ao direito à privacidade foi fortalecida com a expansão da informática porque "sua lógica não costuma ser a do indivíduo, visto que os custos e os meios de produção envolvidos requerem a quantidade para que sejam viáveis; e, portanto, podemos dizer que este sistema funciona tendo em vista basicamente os grandes números – dentro dos quais se diluem os indivíduos e também o humanismo clássico com saldos suportes em sua conotação ética" (Doneda, 2006, p.30)

Considerando que a tecnologia não determina os processos sociais, "a sociedade é que dá forma à tecnologia de acordo com as necessidades, valores e interesses das pessoas que utilizam as tecnologias" (Castells, 2005, p.17), o esforço aqui é altamente propositivo. Objetiva-se contornar uma série de problemas envolvendo a proteção e o tratamento de dados da monitoração eletrônica nas centrais e fora delas, para os sujeitos envolvidos – em qualquer nível – direta ou indiretamente nos serviços. O real interesse contido na tutela da privacidade e da autodeterminação da pessoa em relação às próprias informações pessoais é, sem dúvida, o da dignidade da pessoa humana:

> (i) ela pode compreender tanto a tutela da informação fornecida quanto daquela recebida (em terminologia conhecida, o controle dos inputs e outputs da informação) por uma pessoa; (ii) ela pode ser utilizada igualmente em situações nas quais a privacidade esteja no âmago do problema, bem como em outras nas quais a privacidade seja um aspecto secundário, mas que depende igualmente de uma tutela. Estaria inserida, portanto, tanto em situações patrimoniais quanto não-patrimoniais, aumentando o espectro da efetividade da tutela. (DONEDA, 2006, p.146-147)

Em algumas centrais, além dos bancos de dados armazenados de forma eletrônica (centralizada ou não), os dados são mantidos em meio físico (*hard disk* externo, *pendrive*, fitas magnéticas, ou seja, unidades móveis e portáteis de armazenamento de arquivos), pastas contendo documentos em geral do monitorado, notificações, ofícios e demais comunicações impressas geradas ao longo dos serviços, gerando duplicidade de informações e um risco maior de inconsistências referentes ao mesmo individuo. Do ponto de vista da segurança da informação, esse tipo de procedimento tende a duplicar a nossa preocupação, pois os dados materializados em papel implicam tratamentos variados e, com certeza, mais

onerosos. Quando a pessoa monitorada sai do sistema por conta de morte ou fim da medida, os documentos, em alguns estados, seguem para o arquivo morto da Secretaria de Administração Prisional ou Secretaria de Justiça. No entanto, não há protocolos para nortear qualquer fase do tratamento de dados pessoais da monitoração eletrônica.

Finalmente, ressalta-se mais uma vez que a privacidade e o sigilo dos dados pessoais do monitorado está prevista no Decreto 7.627/2011, justificando a urgência da proposta e sua efetiva aplicação, que também encontra respaldo legal no Código de Processo Penal, como analisamos em páginas anteriores:

> Art. 6º O sistema de monitoramento será estruturado de modo a preservar o sigilo dos dados e das informações da pessoa monitorada.

5 - PRINCÍPIOS, DIRETRIZES E REGRAS SOBRE TRATAMENTO E PROTEÇÃO DE DADOS RELATIVOS À MONITORAÇÃO ELETRÔNICA DE PESSOAS

A partir dos elementos apresentados e discutidos até o momento, o presente protocolo apresenta princípios, diretrizes e regras voltados para o tratamento e proteção dos dados pessoais da monitoração eletrônica. São assumidos princípios gerais[25] de ordem teórica e conceitual e diretrizes com objetivo de organizar o presente protocolo, assim como possibilitar o desenvolvimento e a reestruturação de práticas dos atores envolvidos direta ou indiretamente aos serviços de monitoração eletrônica, sublinhando a pessoa monitorada enquanto sujeito de direitos e que, portanto, deve ter iguais condições de acesso às políticas públicas e sociais e à igual dignidade[26]. Após a indicação das direções conceituais que os serviços devem tomar em termos de seus fluxos e estruturas, chega-se às regras. As regras estipulam, de forma clara e precisa, o *modus operandi* dos diferentes atores da monitoração eletrônica, de forma que os repertórios apresentados sejam capazes de ganhar concretude na gestão e operação dos serviços.

Os bancos de dados da monitoração eletrônica são fundamentalmente constituídos por dados pessoais sensíveis dos indivíduos monitorados. Tais dados apresentam, de forma inerente, riscos potenciais para o uso discriminatório ou lesivo para as pessoas monitoradas, individual ou coletivamente, expondo os sujeitos, durante e após os serviços, a diversas formas de tratamento degradante como práticas de justiçamento e prisões injustificadas. A potencialidade discriminatória ou lesiva se estende aos dados pessoais sensíveis das mulheres em situação de violência doméstica e de familiares, amigos, vizinhos ou conhecidos dos monitorados e das mulheres porquanto podem igualmente mobilizar

[25] Os princípios e as definições utilizadas, em que pese a reapropriação para os dados da monitoração eletrônica, foram formulados a partir de reuniões com Antonio Ianelli e André Girotto, responsáveis pela elaboração do Sistema de Informações do DEPEN (SISDEPEN); livro e artigos de Doneda (2006, 2009, 2010); documentos como as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança Da Informação e Comunicações 07/IN01/DSIC/GSIPR de 15 de jul de 2014, disponível em http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf, acesso em dez de 2015; Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações – versão 2.0, acesso em dez de 2015, disponível em http://dsic.planalto.gov.br; a Lei da Protecção de Dados Pessoais de Portugal 67/98; o anteprojeto de lei de proteção de dados pessoais, acesso em Nov de 2015, disponível em: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/

[26] Documentos elaborados respectivamente por Felipe Athayde e Fabiana Leite (Brasil, 2015f; Brasil, 2015e) igualmente indicam postulados, princípios e diretrizes para a gestão dos estabelecimentos prisionais e para as alternativas penais, tomando o indivíduo como o centro das políticas prisionais.

controles de caráter vexatório, punitivo ou mesmo penal. Os dados pessoais sensíveis construídos a partir dos serviços de monitoração eletrônica devem, então, receber tratamento e proteção adequados, com vistas a garantir que não sejam usados para promover qualquer tipo de discriminação contra as pessoas monitoradas e as mulheres em situação de violência doméstica, assim como seus familiares, amigos, vizinhos e conhecidos.

É fundamental considerar que o uso indiscriminado e indevido do banco de dados contendo informações pessoais sobre os indivíduos monitorados eletronicamente, as mulheres em situação de violência doméstica, assim como seus familiares, amigos, vizinhos e conhecidos, por culpa ou dolo, tem um potencial discriminatório enorme. A circulação de tais informações na Internet pode promover não somente a discriminação, mas igualmente a criminalização destas pessoas, mantendo-as afastadas de uma vida social dentro da normalidade, com acesso ao trabalho, saúde, educação, etc. A privacidade dos indivíduos monitorados é ainda mais sensível porque os dados pessoais de geolocalização apresentam maior potencialidade lesiva no que se refere à exposição excessiva da intimidade, não estipulada na medida judicial, ou seja, uma forma abusiva de poder.

Diante do exposto, é importante sublinhar a relevância do presente protocolo no dia a dia dos operadores das Centrais, empresas, qualquer entidade pública ou privada que lidam com os dados pessoais sensíveis da monitoração eletrônica. A pessoa física, a entidade pública ou privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso aos dados pessoais da monitoração eletrônica, submetendo-os a tratamento indevido ou divulgação não autorizada deverão ser responsabilizadas por tais condutas ilícitas:

> Art. 32 - Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:
> IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;
>
> Art. 34 - Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso. (Lei de Acesso à Informação nº 12.527/2011)

O Código Penal prevê de maneira mais assertiva a responsabilização e a aplicação de pena no caso de violação de sigilo funcional:

> Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1o Nas mesmas penas deste artigo incorre quem: (Incluído pela Lei nº 9.983, de 2000) I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; (Incluído pela Lei nº 9.983, de 2000) II – se utiliza, indevidamente, do acesso restrito. (Incluído pela Lei nº 9.983, de 2000) (Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Art.325)

Segundo o anteprojeto de lei de proteção de dados pessoais utilizado como uma das referências[27], tratamento de dados refere-se ao:

> conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração.

Os dados sensíveis que compõem os bancos de dados de cada uma das centrais, Secretarias de Administração Prisional – ou afins – e/ou empresas prestadoras dos serviços de monitoração eletrônica podem incluir dados das pessoas monitoradas: nome; foto; número de telefone; números de documentos de identificação pessoal; endereços residencial, de trabalho, de estudo, de hospitais ou afins (em caso de trabalho, estudo e de tratamentos continuados de saúde); e-mail; data de nascimento; estado civil; gravação de chamadas telefônicas originadas a partir da comunicação da Central com o monitorado; informação relativa à localização pessoal através de sistemas de geolocalização;

[27] Como já pontuado anteriormente, considera-se o anteprojeto de lei sobre tratamento e proteção de dados disponível no seguinte endereço: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ Acesso em Nov de 2015.

identificadores eletrônicos; origem racial ou étnica. No caso das mulheres em situação de violência doméstica e familiar, os dados pessoais sensíveis podem incluir: nome; número de telefone; endereços para delimitação da(s) área(s) de exclusão; informação relativa à localização pessoal através de sistemas de geolocalização. Os dados pessoais sensíveis de familiares, amigos, vizinhos ou conhecidos dos cumpridores e das mulheres em situação de violência doméstica - considerados titulares indiretos – podem incluir: nome, endereço e telefone, com o intuito de, por exemplo, possibilitar o contato indireto com o monitorado no tratamento de incidentes, após esgotadas todas as modalidades de tratamento destes através da Central.

O protocolo tem por objetivo promover a proteção para os integrantes da rede de monitoração eletrônica – não somente as pessoas monitoradas eletronicamente, mas igualmente empresas, instituições públicas, corporações, funcionários e servidores que trabalham direta ou indiretamente em alguma etapa dos serviços de monitoração eletrônica. Desde o segundo semestre de 2015, visitas *in loco* foram realizadas para o conhecimento dos serviços. Nota-se que funcionários privados e servidores públicos em qualquer nível hierárquico, aqui denominados operadores[28], ou seja, a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável, costumam atuar, na maioria dos casos, sem procedimentos estabelecidos formalmente. Os operadores, portanto, estão mais suscetíveis a erros em qualquer fase do tratamento e proteção de dados pessoais, assim como correm maior risco de penalização diante da tomada de decisões aleatórias norteadas pelo “bom senso”, prática que deve dar lugar aos almejados fundamentos da segurança da informação:

> A Instrução Normativa nº. 1, de 13 de junho de 2008, expedida pelo Gabinete de Segurança Institucional da Presidência da República (IN 01 GSIPR, 2008), com a finalidade de disciplinar a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, estabelece o seguinte conceito de segurança da informação e comunicações: “ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.”

[28] Os operadores também podem incluir diretores e coordenadores dos serviços de monitoração eletrônica, uma vez que estes também lidam com os dados pessoais dos monitorados. Ou seja, qualquer funcionário privado ou público no exercício de sua função.

Os princípios de segurança da informação são considerados neste documento porque a monitoração eletrônica é um sistema institucionalizado de risco, como já pontuado, e qualquer sistema apresenta vulnerabilidade por conta de ausência ou ineficiência das medidas de proteção. Em termos gerais, toda informação tem valor (econômico, político, cultural, etc.) e precisa ser protegida contra acidentes ou ataques, independente de estar armazenada em bancos de dados eletrônicos ou físicos. São consideradas, portanto, a segurança física que visa proteger equipamentos e informações contra usuários não autorizados e prevenção de danos por causas naturais, assim como a segurança lógica aplicada em casos onde um usuário ou processo da rede tenta obter acesso a um objeto que pode ser um arquivo ou outro recurso de rede, ou seja, objetiva proteger os dados, programas e sistemas contra tentativas de acessos não autorizados feitas por usuários ou outros programas.

A primeira parte do protocolo está estruturada em dois grupos: proteção de dados pessoais e segurança da informação. Estabelecidos os horizontes conceituais, passa-se às regras, ou seja, os caminhos adequados a serem seguidos para a proteção e tratamento de dados da monitoração eletrônica. As regras estão divididas em dois grupos: regras por espécie de tratamento e proteção durante a entrada, a manipulação e a saída de dados pessoais; e, regras de segurança física e lógica.

5. 1 – Proteção de dados pessoais sensíveis

1 - Privacidade

Os serviços de monitoração eletrônica devem oferecer meios efetivos de tutela da privacidade, garantindo-a como um direito fundamental a todas pessoas monitoradas e as mulheres em situação de violência doméstica, bem como de seus familiares, amigos, vizinhos e conhecidos – a pessoa natural a quem se referem os dados pessoais sensíveis objeto de tratamento. Todos os dados pessoais construídos a partir dos serviços de monitoração eletrônica são sensíveis. Os dados pessoais de geolocalização merecem especial proteção e tratamento porque apresentam maior potencialidade lesiva em relação

à privacidade da pessoa monitorada, possibilitando excessivas exposições da intimidade não estipuladas na medida judicial.

2 - Limitação da finalidade

O tratamento e a proteção dos dados pessoais devem ser realizados com finalidades lícitas, legais, legítimas, específicas, explícitas e conhecidas pelos envolvidos direta e indiretamente neste processo, considerando que os dados pessoais da monitoração eletrônica são altamente sensíveis. Os dados das pessoas monitoradas devem ser tratados para o desenvolvimento dos serviços de monitoração eletrônica dentro do escopo da política penal, visando exclusivamente o atendimento da finalidade legalmente estabelecida: o acompanhamento do cumprimento das condições determinadas judicialmente para medidas cautelares diversas da prisão ou medidas protetivas de urgência ou, ainda, das saídas temporárias e prisão domiciliar. Dados pessoais, inclusive de geolocalização, não podem ser utilizados para fins políticos criminais preventivos.

3 - Mínimo informacional

Somente devem ser coletadas e tratadas as informações pessoais essenciais e necessárias para os serviços de monitoração eletrônica, considerando o potencial lesivo e discriminatório associados a esses dados. Os dados pessoais coletados referentes aos indivíduos monitorados, às mulheres em situação de violência doméstica e familiar, bem como de seus familiares, amigos, vizinhos e conhecidos deverão, portanto, se ater ao mínimo indispensável, recebendo tratamento e proteção adequados. Os bancos de dados pessoais da monitoração eletrônica devem ser construídos com base no mínimo informacional, não excessivo em relação às finalidades do tratamento, de acordo com os princípios de adequação, necessidade e proporcionalidade.

4 - Imputação pessoal

A monitoração eletrônica não pode ultrapassar a pessoa em cumprimento da medida. Não pode ser imputado tratamento discriminatório e lesivo aos indivíduos relacionados direta ou indiretamente ao cumpridor e à mulher em situação de violência doméstica e familiar. Os serviços de monitoração eletrônica não podem implicar qualquer tipo de medida de caráter

penal ou vexatório aos familiares, amigos, vizinhos e conhecidos das pessoas monitoradas, bem como às mulheres em situação de violência doméstica, seus familiares, amigos, vizinhos e conhecidos.

5 - Tratamento não discriminatório

A monitoração eletrônica é uma medida que deve ser adotada em casos excepcionais, evitando excessivo crescimento, diante de outras possibilidades legais. O tratamento e a proteção dos dados dos indivíduos monitorados, dados pessoais sensíveis a priori, devem evitar a reprodução de processos punitivos, uma vez que estes são extremamente capazes de mobilizar estigmas; disseminar tratamentos discriminatórios nas relações de trabalho, consumo; limitar ou restringir o acesso a serviços e direitos básicos como educação, saúde, assistência social, etc. Formas adequadas de tratamento e de proteção destes dados podem impedir que o estereótipo de "monitorado" seja disseminado e perpetuado, devendo ser encarado como uma condição transitória. Os dados pessoais sensíveis não podem ser usados como ferramentas arbitrárias na invasão da vida íntima da pessoa monitorada, o que consiste em abuso de poder, ensejando discriminação e demais formas de tratamento degradantes.

6 - Transparência

A transparência deve ser um componente essencial na elaboração, no acompanhamento e na avaliação de políticas públicas. A política de monitoração eletrônica de pessoas é essencialmente de interesse coletivo, o que deve ensejar a ampla participação social. Incitar a participação social não pode significar a exposição dos indivíduos monitorados e das mulheres em situação de violência doméstica e familiar, cujos dados pessoais sensíveis merecem tratamento e proteção especiais por conta de sua potencialidade discriminatória e lesiva. Os serviços de monitoração eletrônica devem propiciar a realização de pesquisas, especialmente para orientar a elaboração, o acompanhamento e a avaliação de políticas públicas na área.

5. 2 – Segurança da informação

7 - Disponibilidade

A disponibilidade é fundamental e obrigatória nos serviços de monitoração eletrônica, garantindo a prestação continuada destes, sem interrupções no fornecimento de informações que devem ser analisadas e pré-formatadas para evitar equívocos em qualquer etapa de execução dos serviços, o que inclui o devido tratamento e proteção de dados pessoais.

8 - Integridade

É obrigatória a preservação da exatidão dos dados pessoais e demais informações, bem como dos métodos de processamento, mantendo todas as suas características originais, com objetivo de garantir que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional. A integridade da informação está relacionada à sua fidedignidade, ou seja, ao princípio da exatidão, pois os dados pessoais devem corresponder à realidade atual do indivíduo monitorado e da mulher em situação violência doméstica e familiar.

9 - Confidencialidade

A confidencialidade é um elemento obrigatório no tratamento e proteção de dados pessoais relativos à monitoração eletrônica, atuando como garantia de que a informação estará acessível apenas para funcionários privados ou servidores públicos no exercício de suas funções e identificados dentro do sistema. Deve ser impedido o acesso não autorizado, acidental ou intencional, garantindo que apenas indivíduos, sistemas, órgãos ou entidades devidamente autorizados e credenciados tenham acesso aos dados pessoais ou qualquer outro tipo de informação.

10 - Autenticidade

Os órgãos públicos ou a empresa prestadora de serviços responsável pela monitoração eletrônica deverá dispor de documentos de fácil comprovação de sua autenticidade e, nos casos de sistemas informatizados, preferencialmente seus certificados digitais para possível

interoperabilidade com sistemas externos e de órgãos distintos. O certificado digital deve consistir em documento eletrônico capaz de identificar indivíduos, empresas, sistemas e informações no mundo digital, aumentando a proteção de transações online e a troca virtual de dados. Ainda com vistas a promover a autenticidade nos serviços, a Central de monitoração deverá conferir os documentos de identificação pessoal e a decisão judicial da pessoa monitorada para garantir a autenticidade pessoal do indivíduo, evitando que a medida seja aplicada a quem não se destina.

11 - Da Segurança e da Prevenção

Os dados da monitoração eletrônica devem conter barreiras de proteção a fim de minimizar as vulnerabilidades nos sistemas, infraestrutura física e lógica. Invasões ou acessos de sujeitos não autorizados aos locais de armazenamento de informações e centrais de monitoramento devem ser evitados. Devem ser utilizadas constantemente medidas educativas, técnicas e administrativas, proporcionais à natureza das informações tratadas, ou seja, dados pessoais sensíveis. Tais medidas deverão estar minimamente entrelaçadas com os propósitos de capacitação dos operadores responsáveis pelo gerenciamento de acessos aos dados, bem como a adoção de infraestrutura adequada, evitando os acessos não autorizados, destruição, perda, alteração, comunicação ou difusão ou qualquer dano de ordem natural, acidental ou ilícita. As medidas de segurança devem incluir planos de riscos e continuidade do negócio, a fim de garantir um nível de comprometimento adequado no planejamento e tratamento destas ocorrências e um efetivo controle das informações

5.3 - Composição dos dados pessoais sensíveis dos monitorados

Os dados pessoais dos indivíduos monitorados e das mulheres em situação de violência doméstica e familiar, bem como de seus familiares, amigos, vizinhos e conhecidos são dados pessoais sensíveis por sua potencialidade discriminatória e lesiva, individual ou coletiva. As regras a seguir visam combater a discriminação e qualquer forma de tratamento degradante imputadas às pessoas monitoradas e às mulheres em situação de violência

doméstica, incluindo familiares, amigos, vizinhos e conhecidos de ambas as categorias, segundo os preceitos fundamentais do Estado Democrático de Direito.

Seja qual for o tipo de suporte – papel, eletrônico, informático, som e imagem – os dados pessoais dos monitorados são inerentemente sensíveis. É redundante dizer "dados pessoais sensíveis dos monitorados", porquanto os dados pessoais dos indivíduos monitorados são sensíveis em sua natureza[29]. Os dados pessoais devem ser coletados de acordo com o princípio do mínimo informacional e somente quando necessários para o cumprimento da medida. Eles devem ser compostos por, no máximo, as seguintes informações:

- nome;
- foto;
- números de documentos de identificação pessoal;
- endereços residencial, de trabalho, de estudo, de hospitais ou afins (em caso de trabalho, estudo e tratamentos continuados de saúde);
- número de telefone;
- e-mail;
- data de nascimento;
- estado civil;
- origem racial ou étnica;
- dados de tráfego, ou seja, informação relativa à localização pessoal (através de sistemas de geolocalização, por exemplo);
- identificadores eletrônicos.

A coleta de outros dados pessoais deve ser excepcional e realizada após cuidadosa avaliação da equipe responsável pelo procedimento, necessariamente respeitando-se a finalidade da medida e todos os riscos envolvidos no tratamento e proteção dos dados pessoais sensíveis da monitoração.

[29] Vamos sublinhar o termo "sensível" somente quando for importante demarcar novamente essa característica dos dados pessoais dos monitorados.

Os dados pessoais das mulheres em situação de violência doméstica e familiar são igualmente sensíveis em sua natureza e devem ser compostos por, no máximo, as seguintes informações:

- nome;
- endereço(s) para definição da(s) área(s) de exclusão;
- número de telefone;
- dados de tráfego, ou seja, informação relativa à localização pessoal quando a mulher em situação de violência doméstica e familiar optar pela utilização da Unidade Portátil de Rastreamento.

Os dados pessoais sensíveis de familiares, amigos, vizinhos ou conhecidos, tanto das pessoas monitoradas, quanto das mulheres em situação de violência doméstica e familiar devem ser compostos por, no máximo, as seguintes informações:

- nome;
- número de telefone;
- tipo relação mantida com a pessoa monitorada ou com a mulher em situação de violência doméstica e familiar.

5.4 - Regras prévias ao tratamento e proteção de dados pessoais das pessoas monitoradas

1 - O sistema de monitoramento será estruturado de modo a preservar o sigilo dos dados e das informações da pessoa monitorada (Decreto 7.627/2011, Art. 6º)

1.1 - Os dados pessoais dos monitorados, das mulheres em situação de violência doméstica e familiar, assim como de seus familiares, amigos, vizinhos ou conhecidos são dados pessoais sensíveis e deverão ser tratados e protegidos de modo a não lhes proporcionar qualquer tipo de discriminação ou tratamento degradante pelos operadores das Centrais de Monitoração Eletrônica e demais órgãos, instituições ou

indivíduos envolvidos direta ou indiretamente nos serviços de monitoração eletrônica, durante e após o cumprimento da medida judicial.

2- 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 (Decreto nº 7.627, de 24 de novembro de 2011, Art. 7º)[30]

2.1. Apenas operadores das Centrais de Monitoração Eletrônica capacitados e devidamente autorizados por meio de documento assinado pelo diretor/coordenador deverão tratar e ter acesso aos dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos;

2.2. É vedado o acesso aos dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos aos operadores e demais indivíduos não autorizados para o tratamento de tais dados, sendo proibida a permanência destes nos espaços designados para qualquer ação de tratamento envolvendo os dados pessoais referidos.

3 - São obrigatórios procedimentos de seleção e capacitação dos operadores que lidam com os dados pessoais dos monitorados, das mulheres em situação de violência doméstica e seus familiares, amigos, vizinhos e conhecidos, em qualquer nível de ação do tratamento e proteção dos dados.

4- A capacitação deverá ocorrer de forma inicial e continuada para todos os operadores que trabalham com os dados pessoais dos monitorados, das mulheres em situação de violência doméstica e seus familiares, amigos, vizinhos e conhecidos.

5 – Os contratos firmados entre as empresas que prestam os serviços de monitoração e as Centrais de Monitoração Eletrônica deverão prever a capacitação de todos operadores

[30] O Decreto nº 7.627, de 24 de novembro de 2011, regulamenta a monitoração eletrônica de pessoas prevista no Decreto-Lei 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

independente da área de atuação[31], visando assegurar capacidade técnica e garantir o cumprimento dos princípios, diretrizes e regras estabelecidos no presente protocolo.

6- Todos os operadores, incluindo o diretor/coordenador, em qualquer nível de acesso e segurança, deverão assinar um termo de tratamento e proteção de dados pessoais da monitoração eletrônica constando necessariamente seu comprometimento acerca da confidencialidade necessária nas ações relativas ao tratamento e proteção de dados pessoais das pessoas em monitoração eletrônica, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos, durante e após o término da medida.

7- A(s) empresa(s) que presta(m) serviços de monitoração eletrônica às centrais deverão assinar um termo de tratamento e proteção de dados pessoais da monitoração eletrônica constando necessariamente seu comprometimento profissional acerca da confidencialidade necessária nas ações relativas ao tratamento e proteção de dados pessoais das pessoas em monitoração eletrônica, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos, durante e após o término da medida.

7.2 - Todas as entidades, públicas ou privadas, ao tratar dos dados pessoais dos monitorados deverão desenvolver ações integradas para garantir ampla efetividade no tratamento e proteção de dados por meio de controles internos e externos, auditorias, entre outras.

[31] Indicamos a seguinte composição das Centrais de Monitoração Eletrônica: Direção ou coordenação; Núcleo de Monitoramento - constituído por operadores que trabalham em regime de plantão, visando identificar possíveis descumprimentos das decisões judiciais e tratar os incidentes; Núcleo de Análise e Estatística: constituído por operadores com conhecimento em Inteligência e domínio em matemática e/ou estatística; Núcleo de Apoio Administrativo: constituído por operadores com experiência na área administrativa; Núcleo de Operações: responsável pelo atendimento aos monitorados, substituição de equipamentos e manutenção em primeiro nível; Núcleo Social: responsável por receber a pessoa a ser monitorada, explicar suas obrigações, levantar informações relevantes sobre o indivíduo no que concerne aos aspectos psicossociais, realizar encaminhamentos para a rede de proteção social e realizar o acompanhamento psicossocial do cumpridor.

5.5 - Regras por espécie de tratamento e proteção dos dados pessoais dos monitorados

5.5.1 - Entrada dos dados

Coleta, Produção, Recepção, Classificação

8 - Durante a coleta de dados pessoais sensíveis do monitorado e da mulher vítima de violência doméstica e o cadastramento no sistema de monitoração eletrônica:

8.1 – A decisão do juiz deverá ser a base para a coleta de dados pessoais e o cadastramento no sistema de monitoração eletrônica, abarcando a pessoa monitorada, a mulher vítima de violência doméstica e seus familiares, amigos, vizinhos ou conhecidos para o cumprimento da medida;

8.2 – Além do juiz, apenas a própria pessoa monitorada poderá informar seus dados pessoais necessários para o cumprimento da medida, incluindo dados pessoais de seus familiares, amigos, vizinhos ou conhecidos;

8.2.1- A coleta dos dados pessoais de familiares, amigos, vizinhos ou conhecidos, se dará com intuito exclusivo de facilitar a localização da pessoa monitorada no tratamento de algum incidente, apenas quando esta não possuir ou não atender o telefone indicado ou, por outra razão, não puder ser contatada;

8.3- Os juízes, nas decisões envolvendo medidas protetivas de urgência, deverão informar os dados pessoais da mulher em situação de violência doméstica e familiar para a definição da(s) área(s) de exclusão;

8.3.1 - Além do juiz, somente a própria mulher em situação de violência doméstica e familiar poderá conceder informações pessoais de seus familiares, amigos, vizinhos ou conhecidos;

8.4 – A mulher em situação de violência doméstica e familiar não poderá ser obrigada a comparecer na Central de Monitoração Eletrônica para procedimentos relativos à coleta de dados pessoais e ao cadastramento no sistema de monitoração eletrônica;

8.5 - A mulher em situação de violência doméstica e familiar não poderá ser obrigada a utilizar a Unidade Portátil de Rastreamento (UPR), independente da Central oferecer esse tipo de serviço;

8.6– A mulher em situação de violência doméstica e familiar que optar pela utilização da Unidade Portátil de Rastreamento (UPR) deverá comparecer à Central para buscar o equipamento, receber informações sobre o seu uso e solicitar, quando necessário, reparo ou troca da UPR;

8.6.2 – A mulher em situação de violência doméstica e familiar que optar pela utilização da Unidade Portátil de Rastreamento (UPR) não poderá ser penalizada, caso opte por interromper o uso da UPR, devendo devolver o equipamento à Central;

8.6.3 – A mulher em situação de violência doméstica e familiar que interrompa a utilização da Unidade Portátil de Rastreamento (UPR) deverá ser acompanhada até o fim da medida protetiva de urgência, segundo a(s) área(s) de exclusão delimitadas e demais condições previstas na medida;

8.7 - Os procedimentos de coleta de informações e de cadastro da pessoa monitorada e da mulher em situação de violência doméstica e familiar deverão ser realizados individualmente e em local reservado, garantindo a preservação da privacidade e impedindo o acesso, a divulgação e a apropriação não autorizados de qualquer informação pessoal;

8.8- O ambiente deverá ser capaz de proporcionar privacidade, evitando constrangimentos e exposição das informações da pessoa monitorada e da mulher em situação de violência doméstica e familiar;

8.9- A equipe psicossocial deverá dispor de ambiente capaz de proporcionar maior privacidade, minimizando constrangimentos e exposição das informações, observando-se o sigilo previsto nos Conselhos Profissionais de Psicologia e de Serviço Social.

9 – A pessoa monitorada deverá obrigatoriamente ser informada acerca de seus direitos, o que inclui a privacidade, o tratamento adequado e a proteção dos dados pessoais.

10- A pessoa monitorada deverá receber documento no qual constem, de forma clara e expressa, seus direitos e os deveres a que estará sujeita, o período de vigilância e os procedimentos a serem observados durante a monitoração (Decreto nº 7.627, de 24 de novembro de 2011, Art. 3º), consubstanciado em termo de tratamento e proteção de dados pessoais da monitoração eletrônica, que deverá:

10.1- ser o instrumento adotado para informar os direitos e os deveres da pessoa monitorada e da mulher em situação de violência doméstica e familiar;

10.2- conter instruções precisas, objetivas e claras acerca de todas as fases de tratamento das informações, incluindo as formas de tratamento e proteção de seus dados pessoais sensíveis, assegurando o uso destes dados para os fins de cumprimento da medida e vedando sua utilização para fins discriminatórios e lesivos;

10.3- apresentar instruções precisas, objetivas e claras acerca de todas as fases e possibilidades de tratamento das informações de familiares, amigos, vizinhos ou conhecidos, garantindo que os dados pessoais não sejam usados para fins discriminatórios e lesivos;

10.4- ser lido em conjunto pela pessoa monitorada e pelo operador responsável pela coleta com vistas a promover entendimento integral das partes e eventuais esclarecimentos;

10.5- ser assinado e datado, de forma voluntária, pela pessoa monitorada e pelo operador responsável pela coleta;

10.6 – a pessoa monitorada deverá receber uma via do documento que informa seus direitos e deveres, incluindo os procedimentos relativos à proteção e tratamento de dados pessoais;

10.7 – a mulher em situação de violência doméstica e familiar não deverá ser obrigada a comparecer à Central para assinar e receber o termo de tratamento e proteção de dados pessoais;

10.7.1 – apenas a mulher em situação de violência doméstica e familiar que optar pela utilização da Unidade Portátil de Rastreamento (UPR) deverá, na ocasião em que receber a UPR, assinar, datar e receber uma via do termo de tratamento e proteção de dados pessoais que enfatize, além dos termos

acima sublinhados, os procedimentos relativos aos dados pessoais de tráfego, ou seja, informação relativa à localização pessoal;

10.8 - Caso a pessoa monitorada ou a mulher em situação de violência doméstica que opte pelo uso da UPR não seja capaz de ler e assinar o termo de consentimento informado, o operador deverá explicar o conteúdo verbalmente, permitindo eventuais esclarecimentos;

10.8.1- Caso a pessoa monitorada ou a mulher em situação de violência doméstica que opte pelo uso da UPR não seja capaz de assinar o termo de consentimento informado, o operador deverá confirmar verbalmente o entendimento integral do conteúdo e realizar a assinatura por testemunha de leitura no documento assinado e datado pelo operador responsável pela coleta;

10.8.2- Se a pessoa monitorada ou a mulher em situação de violência doméstica que opte pelo uso da UPR se recusar a assinar o termo de consentimento informado durante a coleta dos dados pessoais, a recusa deverá ser registrada por escrito ao final do próprio termo com data e assinatura de uma testemunha e não poderá ensejar nenhum tipo de sanção.

11- Os bancos de dados que integram os serviços de monitoração eletrônica não poderão conter informações pessoais excedentes, desnecessárias e em desconformidade com as finalidades dos serviços.

12 - O cadastramento/registro da pessoa monitorada no sistema da Central de Monitoração Eletrônica deverá conter unicamente:

12.1 - Nome, foto, número de telefone, números de documentos de identificação pessoal, número de telefone, endereço residencial, e-mail, data de nascimento, estado civil, origem racial ou étnica;

12.2 - Tipo penal relacionado ao processo criminal que justificou a aplicação da medida;

12.3 – A natureza da medida;

12.4 - Todas as condições relativas ao cumprimento da medida: prazo com data de início e término; limites das áreas de inclusão e de exclusão; horários de circulação e de recolhimento; condições; proibições diversas; autorizações de trabalho, de estudo e de tratamento de saúde; outras autorizações envolvendo inclusão social através de atividades de convivência familiar e/ou comunitária, de cunho religioso, de acesso à justiça e demais serviços públicos;

12.5 - Dados pessoais relativos à saúde e endereço de hospitais ou afins quando a pessoa monitorada estiver realizando tratamentos de saúde;

12.6- Dados pessoais relativos a trabalho e endereço do trabalho quando a pessoa monitorada estiver desenvolvendo alguma atividade laborativa;

12.7 - Dados pessoais relativos a estudo e endereço de estabelecimento educacional quando a pessoa monitorada estiver desenvolvendo alguma atividade educacional;

12.7 - No caso de familiares, amigos, vizinhos ou conhecidos da pessoa monitorada, apenas: nome, número de telefone e o tipo relação mantida com a pessoa monitorada;

12.7.1- A quantidade e a qualidade destas informações não deverão exceder a finalidade estrita da medida.

13 - O cadastramento/registro da mulher em situação de violência doméstica e familiar no sistema da Central de Monitoração Eletrônica deverá conter apenas:

13.1 – Nome e número de telefone;

13.2 – Endereço residencial e endereços do local de trabalho e de estudo para a delimitação da(s) área(s) de exclusão, conforme especificados na decisão judicial;

13.3 - no caso de familiares, amigos, vizinhos ou conhecidos da mulher em situação de violência doméstica e familiar, unicamente: nome, número de telefone e o tipo relação mantida com esta;

13.3.1- A quantidade e a qualidade destas informações não deverão exceder a finalidade estrita da medida.

14 – Além dos dados cadastrais, serão coletados dados pessoais necessários para o acompanhamento da medida judicial no sistema da Central de Monitoração Eletrônica:

14.1 - Geolocalização da pessoa monitorada através de coleta continuada ao longo do acompanhamento da medida, ou seja, dados relativos à localização pessoal do monitorado através de sistemas de geolocalização de forma contínua e permanente;

14.2 - Geolocalização da mulher em situação de violência doméstica e familiar apenas quando esta optar pela utilização da Unidade Portátil de Rastreamento (UPR), através de coleta continuada ao longo do acompanhamento da medida, isto é, dados relativos à localização pessoal da mulher em situação de violência doméstica através de sistemas de geolocalização de forma contínua e permanente, podendo tornar as áreas de exclusão dinâmicas.

15- Os dados pessoais coletados pelos profissionais da equipe psicossocial, registrados em meios físicos ou eletrônicos, serão utilizados para fins exclusivos de acompanhamento e proteção social, não podendo ser acessados por terceiros, inclusive pelos profissionais responsáveis pelos serviços de monitoração eletrônica.

16 - As alterações nos dados pessoais necessários para o acompanhamento da medida judicial no sistema da Central de Monitoração Eletrônica, além dos referidos dados de cadastro/registro devem se referir:

16.1 - número de telefone, números de documentos de identificação pessoal (no caso da aquisição de tais documentos após o cadastro), endereço residencial, estado civil da pessoa monitorada;

16.2- novas condições determinadas judicialmente para o cumprimento da medida: limites das áreas de inclusão e de exclusão, horários de circulação e de recolhimento, condições, autorizações e proibições diversas;

16.3 - início de atividade laboral, tratamento de saúde e/ou atividades educacionais. Dados pessoais atrelados ao trabalho, saúde, estudo, religião e atividades familiares e/ou comunitárias, bem como os respectivos endereços de tais estabelecimentos/instituições deverão ser coletados e registrados;

16.4 - número de telefone e endereços da pessoa mulher em situação de violência doméstica e familiar;

16.4.1- no caso de familiares, amigos, vizinhos ou conhecidos da pessoa monitorada e da mulher em situação de violência doméstica e familiar: nome, número de telefone e o tipo relação mantida com a mulher.

5.5.2 - Manipulação dos dados

Utilização e acesso

17 - 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 (Decreto nº 7.627, de 24 de novembro de 2011, Art. 7º)

17.1 - Cada operador treinado, previamente autorizado e cadastrado no sistema de monitoração eletrônica, deverá ter níveis de acesso discriminados de acordo com a finalidade da função, especificando, inclusive, quais informações ou funcionalidades serão possíveis para o seu nível de acesso;

17.2 - a autenticação de usuários deverá ser obrigatória para todos os operadores do sistema de registro de informações das pessoas monitoradas e do sistema de registro de incidentes;

17.3 - Todos os operadores, independente de lidarem direta ou indiretamente com os dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos, deverão utilizar tais dados para as finalidades dos serviços de monitoração eletrônica, de modo a impedir irregularidades ou ilegalidades vinculadas ao uso inadequado dos dados, desrespeito à privacidade e discriminação;

17.4 - Os dados pessoais de familiares, amigos, vizinhos ou conhecidos dos indivíduos monitorados e das mulheres em situação de violência doméstica e familiar deverão ser utilizados para os propósitos da monitoração eletrônica, no caso de impossibilidade de comunicação direta com a pessoa monitorada, quando tal procedimento se fizer necessário, sobretudo no tratamento de incidentes.

5.5.3 - Saída dos dados

Arquivamento e Armazenamento

18 - O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

19 - Os dados pessoais dos indivíduos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos deverão ser mantidos ativos no sistema de monitoração apenas durante o período de cumprimento da medida judicial.

20 - Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades: (...) II – pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais. (Anteprojeto de Lei de Proteção de Dados Pessoais, Art.15)

21- Após o cumprimento da medida judicial deverão ser mantidos unicamente dados estatísticos, sendo assegurado o anonimato das pessoas, observando-se finalidades como a avaliação da política de monitoração eletrônica e realização de pesquisas.

Eliminação

22 - Os dados pessoais dos indivíduos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos deverão ser eliminados ao final do cumprimento da medida judicial, observando-se os princípios do presente protocolo.

23 - As informações sobre o cumprimento regular da medida de monitoração eletrônica, bem como eventuais incidentes, deverão ser reduzidas a termo, para encaminhamento ao Poder Judiciário.

5.6 - Fornecimento a terceiros por comunicação, interconexão, transferência, difusão ou extração

24 - Por abranger dados que pressupõem sigilo, a utilização de informações coletadas durante a monitoração eletrônica de pessoas dependerá de autorização judicial, em atenção ao art. 5°, XII, da Constituição Federal (Conselho Nacional de Justiça, Resolução 213, 2015, Art.10, Parágrafo único)

25 - A atuação das Centrais de Monitoração Eletrônica de Pessoas deverá 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.

26 - Os dados coletados durante a execução das medidas de monitoração eletrônica possuem finalidade específica e deverão estar relacionadas com o acompanhamento das condições estabelecidas judicialmente.

27 - 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.

28 - 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. (Conselho Nacional de Justiça, Resolução 213, 2015, Protocolo I)[32]

28.1 - É proibido o compartilhamento de dados da pessoa monitorada ou do sistema de monitoração eletrônica com terceiros sem prévia autorização judicial, exceto

[32] O fornecimento de dados pessoais para os fins de investigação criminal, especialmente dados pessoais de geolocalização durante o período de armazenamento, dependerá de prévia autorização judicial, solicitada no âmbito de inquérito policial específico, em que a pessoa monitorada figure como suspeita ou indiciada.

quando a Central, diante do contínuo acompanhamento, precisar tratar incidente de violação da área de exclusão por cumpridor de medidas protetivas de urgência com a necessidade específica de acionamento de instituições de segurança pública;

28.2 - O tratamento de incidentes relativo à violação de área de exclusão pelo cumpridor de medidas protetivas de urgência com aproximação da mulher em situação de violência doméstica e familiar deverá obrigatoriamente ser registrado no sistema de monitoração eletrônica, de acordo com data e horário, acionando as modalidades de tratamento na seguinte ordem: 1) envio de sinal ao equipamento de monitoração eletrônica, 2) contato telefônico com o monitorado, 3) contato telefônico com familiares, amigos, vizinhos ou conhecidos, 4) contato telefônico com a mulher em situação de violência doméstica e familiar para checar a ocorrência do incidente, unicamente no caso de medidas protetivas de urgência, 5) contato telefônico com familiares, amigos, vizinhos ou conhecidos da mulher em situação de violência doméstica para checar a ocorrência do incidente, unicamente no caso da impossibilidade de contato com a mulher;

28.3 - Todos os incidentes e suas modalidades de tratamento deverão ser registradas e comprovadas pelo sistema de monitoração;

28.4 - Após esgotadas todas as modalidades de tratamento de incidentes de violação da área de exclusão no caso de cumpridores de medidas protetivas de urgência, devidamente acompanhadas e registradas no sistema, e apenas quando não for possível o tratamento dos incidentes especificados através do contato direto ou indireto com a pessoa monitorada, a mulher em situação de violência doméstica ou seus respectivos familiares, amigos, vizinhos ou conhecidos, o acionamento urgente e imediato das instituições de segurança pública deverá ser possibilitado pelo sistema de monitoração eletrônica por meio da geração de uma sub ocorrência;

28.5 - A sub ocorrência específica que viabiliza o acionamento das instituições de segurança pública pela Central de Monitoração Eletrônica deverá permitir o compartilhamento de dados pessoais dos monitorados segundo os princípios da necessidade e do mínimo informacional, limitando-se aos seguintes dados: 1) nome, 2) última geolocalização pessoal, 3) endereços, 4) foto;

28.6 - Demais dados pessoais sensíveis poderão ser repassados exclusivamente em caso de inquérito policial específico no qual a pessoa monitorada devidamente identificada já figure como suspeita com prévia autorização judicial, conforme já pontuado;

28.7 - Todos os incidentes, seus respectivos acompanhamentos e conclusões deverão ser obrigatoriamente registrados no sistema de monitoração eletrônica, sobretudo em casos excepcionais no caso de medidas protetivas de urgência que mobilizem procedimentos externos aos procedimentos de rotina da Central de Monitoração Eletrônica com o acionamento das instituições de segurança pública e fornecimento de dados pessoais dos monitorados.

29 - Qualquer imputação de responsabilidade civil ou criminal deverá ser devidamente investigada, dando andamento às penalidades cabíveis no caso de desvios de finalidade ou o não cumprimento das regras em qualquer etapa do tratamento dos dados pessoais dos monitorados, sensíveis por natureza

29.1 - Com vistas a permitir que a responsabilização sobre o uso indevido dos dados pessoais sensíveis possa ser individualizável, protegendo os atores contra formas indistintas e injustas de responsabilização, deverão ser registrados no sistema de monitoração eletrônica os dados da instituição de segurança pública com a qual foram compartilhados os dados pessoais do monitorado ou de qualquer indivíduo que tenha seus dados pessoais armazenados no sistema de monitoração eletrônica, a modalidade de fornecimento dos dados (telefone, rádio, e-mail, mensagens por telefone, etc), principalmente informações que identifiquem de forma precisa a instituição, o que pode incluir endereço do estabelecimento e identificação profissional do policial;

29.2 - É vedado o compartilhamento dos dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos informados às instituições de segurança pública para terceiros;

29.3 - A identificação do indivíduo que acessou os dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos,

vizinhos ou conhecidos deverá ser mantida no sistema de registro da instituição de segurança pública a qual está vinculado;

29.4 - Para possibilitar a responsabilização individualizável sobre o uso dos dados pessoais sensíveis, as instituições de segurança pública que tenham acesso aos dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos deverão desenvolver formas de controle interno e externo destas informações, incluindo auditorias.

30 - O compartilhamento de dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos com as instituições de segurança pública deverá ser subsidiário, excepcional e evitado através do tratamento de incidentes por operadores capacitados e treinados para assegurar a prioridade ao cumprimento, manutenção e restauração da medida em liberdade, bem como pela adoção de medidas de conscientização e atendimento psicossocial.

31- Os encaminhamentos realizados pela Central de Monitoração Eletrônica para trabalho, saúde, educação, atendimento psicossocial ou qualquer serviço voltado para o exercício dos direitos de cidadania, observando-se os princípios da necessidade, da finalidade, do mínimo informacional e da separação de competências, deverão ser realizados considerando apenas o compartilhamento dos seguintes dados das pessoas monitoradas: 1) nome, 2) endereço, 3) números de documentos de identificação pessoal, 4) dados que sejam necessários para o encaminhamento de acordo com a equipe psicossocial[33].

[33] A atuação das Centrais de Monitoração Eletrônica de Pessoas deverá: (...) IV. Buscar integrar-se em redes amplas de atendimento e assistência social para a inclusão de forma não obrigatória dos autuados a partir das indicações do juiz, das especificidades de cada caso e das demandas sociais apresentadas diretamente pelos autuados, com destaque para as seguintes áreas ou outras que se mostrarem necessárias: a) demandas emergenciais como alimentação, vestuário, moradia, transporte, dentre outras; b) trabalho, renda e qualificação profissional; c) assistência judiciária; d) desenvolvimento, produção, formação e difusão cultural principalmente para o público jovem; V. Realizar encaminhamentos necessários à Rede de Atenção à Saúde do Sistema Único de Saúde (SUS) e à rede de assistência social do Sistema Único de Assistência Social (SUAS), além de outras políticas e programas ofertadas pelo poder público, sendo os resultados do atendimento e do acompanhamento do autuado, assim indicados na decisão judicial, comunicados regularmente ao Juízo ao qual for distribuído o auto de prisão em flagrante após o encerramento da rotina da audiência de custódia. (Conselho Nacional de Justiça, Resolução 213, de 15 de dezembro de 2015, Protocolo I)

32 - A Secretaria Estadual de Justiça, o Departamento Penitenciário Nacional ou Poder Judiciário do Estado poderá autorizar o uso dos dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos para fins de pesquisa, desde que a identificação de seus titulares seja tratada por meio de recursos metodológicos para a manutenção do anonimato com rigorosa confidencialidade e mediante requerimento do pesquisador ou instituição de pesquisa junto a tais órgãos e instituições[34]

32.1 - O desenvolvimento de pesquisas devidamente autorizadas por órgãos e instituições competentes deverá adotar termo de responsabilidade para garantir finalidade e obrigações relacionadas ao acesso dos dados pessoais sensíveis, incluindo a descrição de métodos e técnicas de pesquisa para vedar a publicidade de qualquer tipo de identificação pessoal dos monitorados, seus familiares, amigos, vizinhos ou conhecidos;

32.2 - uma vez que é obrigatória a manutenção da privacidade e do anonimato com rigorosa confidencialidade dos dados pessoais dos monitorados, das mulheres em situação de violência doméstica e de seus familiares, amigos, vizinhos ou conhecidos, os resultados e análises das pesquisas deverão respeitar a privacidade e a confidencialidade dos dados, independentemente de gerar publicações em qualquer nível de divulgação e de propósito.

5.7 - Regras de segurança física e lógica, avaliação ou controle das informações[35]

33 - A Central de Monitoração Eletrônica e os espaços destinados aos serviços de monitoração deverão ser compatíveis com os modelos de estruturas de Centrais de Monitoramento de Redes (NOC - *Network Operations Center*), garantindo níveis de acesso à Central e confidencialidade na monitoração.

[34] Observar o Art.31 da Lei de Acesso à Informação nº 12.527/2011, citado na etapa de saída dos dados (arquivamento e armazenamento).

[35] Há várias normas internacionais de gestão de segurança da informação que podem ser implantadas no sistema de monitoração eletrônica, como a ISO/IEC 27001. Elas descrevem como colocar em prática um sistema de gestão de segurança da informação avaliado e certificado de forma independente, visando a proteção de dados confidenciais de maneira mais eficiente e minimizando a probabilidade de acessos ilegais ou sem permissão.

34 - O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito. (Anteprojeto de Lei de Proteção de Dados Pessoais, Art.42)

35 - As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis da monitoração eletrônica de pessoas.

36 - A infraestrutura necessária para o armazenamento do banco de dados deverá conter um servidor de aplicação e uma *storage* adequada para comportar o tipo de banco de dados da empresa contratada para executar os serviços de monitoração eletrônica.

37 - É proibido qualquer tipo de armazenamento de dados pessoais dos monitorados e de seus familiares, amigos, vizinhos ou conhecidos em *desktops, hard disk* externo, *pendrive* ou qualquer outra unidade móvel e portátil de armazenamento de arquivos.

38 - É proibida a manutenção de banco de dados fora do sistema, alterando internamente as informações nele contidas, sem a existência de um Plano de Mudanças, contendo: justificativa, plano de *backup*, plano de retorno, nome dos responsáveis pela autorização, nome dos responsáveis pela execução de tais mudanças.

39 - a infraestrutura física do local onde se encontram os servidores e *storages* deverão conter o mínimo de segurança física para o devido tratamento e proteção dos dados pessoais, preferencialmente incluindo: 1) acesso restrito, 2) portas com controle de biometria para acesso ao local, 3) câmeras de vigilância, 4) ar condicionado, 5) extintores de incêndio apropriados para equipamentos de tecnologia da informação, 6) detectores de fumaça, 7) detectores de calor, 8) detectores de umidade.

40 - Toda infraestrutura de tecnologia da informação deverá, preferencialmente, ser avaliada com relação a sua alta disponibilidade por profissionais habilitados e capacitados em Tecnologia da Informação, garantindo o funcionamento contínuo dos serviços de monitoração eletrônica no caso de falhas em algum componente.

41 - Todos os computadores utilizados pelas Centrais de Monitoração Eletrônica deverão preferencialmente possuir: 1) licenciamento adequado de Software (Sistema Operacional e Aplicativos), 2) sistema de controle de antivírus, 3) atualizações para a manutenção de segurança.

42 - A rede de dados que habilita acesso à Internet deverá possuir *firewall* devidamente instalado para minimizar invasões indesejadas oriundas da Internet.

43 - Profissionais habilitados e capacitados em Tecnologia da Informação deverão periodicamente: 1) verificar se as redes estão operando sem violações, 2) investigar e avaliar danos decorrentes de quebras de segurança; 3) validar as informações dos bancos de dados, procedimento direcionado à manutenção da qualidade dos dados, atualizações de informações para o cumprimento da finalidade de seu tratamento.

44 - Deverão ser criados mecanismos periódicos para a atualização dos dados pessoais do monitorado, além daqueles relacionados ao procedimento de coleta continuada de dados relativos à localização pessoal através de sistemas de geolocalização, com a finalidade exclusiva de acompanhar o cumprimento das condições determinadas judicialmente.

45 - No caso de haver interoperabilidade automática entre sistemas da Central de Monitoração Eletrônica junto a outros estabelecimentos, instituição ou órgão autorizado judicialmente para receber informações da Central, a Central de Monitoração Eletrônica deverá possuir mecanismos de garantia da autenticidade dos dados fornecidos e da identificação do sistema acessado.

46 - As empresas contratadas para desenvolver os serviços de monitoração deverão disponibilizar, quando solicitadas pela Central de Monitoração Eletrônica ou pelo Departamento Penitenciário Nacional, mecanismos de garantia da autenticidade dos dados fornecidos e da identificação do sistema acessado.

47 - Deverão ser criados mecanismos de segurança para evitar invasões aos bancos de dados ou acessos a documentos físicos, bem como transmitir de forma criptografada informações sigilosas entre sistemas que se integram.

48 - Os bancos de dados pessoais da monitoração eletrônica, incluindo todos os registros de incidentes deverão ser mantidos em sistemas informatizados através de redes seguras e preferencialmente com bancos de dados criptografados, ou seja, técnica de proteção de informação que consiste em cifrar o conteúdo de um banco de dados, uma mensagem ou um sinal, transformando-o em um texto ilegível.

49 - A criptografia[36] auxilia a manutenção de padrões adequados de segurança para garantir que os dados não sejam acessados por qualquer indivíduo sem autorização ou mesmo interceptações de transmissões de dados, mas como é passível de falhas, outros mecanismos de segurança deverão ser usados concomitantemente, como níveis de acessos ao sistema, auditoria, ofícios para deliberar autorização de acessos aos sistemas, protocolos de segurança para interoperabilidade entre sistemas, etc.

50 - A empresa de monitoração deverá executar rotinas de auditorias periodicamente (trimestral ou semestralmente) em seus bancos de dados a fim de identificar possíveis anomalias.

51 - O Departamento Penitenciário Nacional poderá manter auditorias para validação das informações, armazenamento dos dados, segurança física e lógica das informações que as Centrais informaram, a fim de garantir a credibilidade e autenticidade dos processos.

[36] A criptografia auxilia a percepção da existência de um nível maior de confidencialidade, privacidade, integridade, autenticação, irretratabilidade e disponibilidade.

52 - As Centrais de Monitoração Eletrônica deverão ser responsáveis pelo uso adequado dos ativos de informação, unicamente para os serviços de monitoração eletrônica, tais como: utilização da internet, gerenciamento de acessos físicos e lógicos, utilização do e-mail profissional, para que as informações sejam mantidas de modo íntegro e confiável.

53 - Em qualquer local ou sala das Centrais de Monitoração Eletrônica onde seja realizado qualquer tipo de tratamento ou proteção de dados pessoais dos monitorados, é vedado aos operadores e demais funcionários utilização de: 1) dispositivos móveis como aparelhos de telefone celular particulares, 2) *hard disk* externo, 3) *pendrive* ou qualquer outra unidade móvel e portátil de armazenamento de arquivos, 4) câmeras fotográficas, 5) câmeras filmadoras.

54 - É proibido o acesso a contas de e-mail particulares em qualquer computador utilizado pelas Centrais de Monitoração Eletrônica ou em qualquer dispositivo móvel em local ou sala das Centrais onde seja realizado qualquer tipo de tratamento ou proteção de dados pessoais dos monitorados.

55 - É obrigatória a elaboração de um plano de continuidade de negócios que trate dos casos de incidentes e indisponibilidade dos serviços de monitoração eletrônica, devendo incluir qual o tempo e estratégia adotada para recuperação e restauração dos serviços.

56 - A elaboração do plano de continuidade de negócios que trate dos casos de incidentes e indisponibilidade dos serviços de monitoração eletrônica deverá ser de responsabilidade da empresa prestadora dos serviços de monitoração eletrônica, seguindo condições mínimas estabelecidas pelas centrais de monitoração eletrônica e demais normas aplicáveis.

57 - é obrigatória a realização de *backups* diário, semanal e mensal de todos os bancos de dados do sistema de monitoração eletrônica e do sistema de controle de incidentes.

58 - As mídias de *backups* deverão obrigatoriamente ser armazenadas em locais distintos da sala ou prédio onde foram efetuados os procedimentos e, preferencialmente, em cofres anti-chamas, com vistas a proteger os dados e possibilitar uma restauração dos dados ou serviços em casos de acidentes variados, como problemas elétricos, alagamentos, incêndios, etc.

59 - A Central de Monitoração Eletrônica deverá conter, preferencialmente, circuito de vigilância externa e interna com vistas a identificar todos os acessos, apresentando avisos afixados que alertem para a existência das câmeras, uma vez que o ambiente está suscetível a invasões ou entradas de pessoas não autorizadas, má utilização dos recursos e equipamentos pelos próprios funcionários, ações acidentais, armazenando por pelo menos 30 dias tais imagens.

60 - O Departamento Penitenciário Nacional deverá observar o devido cumprimento das normas aplicáveis no tratamento e proteção de dados pessoais na celebração de convênios, repasse de recursos ou qualquer tipo de investimento destinado aos serviços de monitoração eletrônica, podendo vedar o repasse de recursos às instituições públicas ou privadas que não tratarem e protegerem os dados pessoais dos monitorados e de seus familiares, amigos, vizinhos ou conhecidos em conformidade com as regras explicitadas no presente documento.

6 - CONSIDERAÇÕES FINAIS

O produto contextualiza e aprofunda aspectos da “sociedade em rede”, suas implicações no âmbito das políticas públicas até chegar à proposição de princípios, diretrizes e regras sobre tratamento e proteção de dados relativos à monitoração eletrônica de pessoas, considerando especialmente os casos de cumpridores de medidas cautelares diversas da prisão e medidas protetivas de urgência.

A pessoa monitorada deve ter todas as prerrogativas e condições necessárias para exercer sua cidadania e os direitos fundamentais que estatuto carrega. Mais do que isso, os serviços de monitoração eletrônica não devem ser marcados por uma lógica relacional que, inevitavelmente, induz formas abusivas de tratamento. É primordial pensar e desenvolver formas protocolares que sejam capazes de proteger os direitos fundamentais das pessoas monitoradas e das mulheres em situação de violência doméstica e familiar.

Esta iniciativa, como foi exposta em linhas anteriores, não somente permite o aprimoramento dos serviços para a pessoa monitorada em si, mas seus efeitos igualmente podem ser experimentados por todos aqueles que trabalham direta ou indiretamente com os dados oriundos da monitoração. É uma maneira de garantir a aplicação de normas e regras uniformes quanto à proteção e o tratamento dos dados pessoais sensíveis, garantindo modos localizados de responsabilização no caso do uso, tratamento ou proteção indevidos.

Os dados pessoais da monitoração eletrônica são sensíveis e constituem um dos principais “ativos” da política. Pensar e instaurar procedimentos com vistas a minimizar os impactos negativos causados durante e, igualmente, após o término da medida, compreende adotar novos paradigmas capazes de garantir a privacidade e, com isso, a dignidade das pessoas monitoradas eletronicamente, bem como das mulheres em situação de violência doméstica e dos familiares, amigos, vizinhos e conhecidos de ambos.

A efetividade no tratamento e proteção de dados sensíveis da monitoração requer o compartilhamento dos protocolos propostos de forma ampla, agregando todos os atores do sistema de justiça, instituições de segurança pública, gestores do poder executivo, instituições da sociedade civil e equipes técnicas. A aderência ao que propomos é um processo normalizador com contornos marcados, de algum modo, pela ruptura e contenção

do poder punitivo de um lado e, por outro lado, a promoção da igual dignidade e liberdade dos cumpridores.

De modo macro, a proposta é potencializar, rever e formular proposições no sentido de contornar desigualdades na disponibilidade de informações e conhecimentos estratégicos, assim como desiguais posições no âmbito dos fluxos e dos fixos que compõem as redes de informação e comunicação na política penal:

> Alguns apostam inclusive que o desenho de cenários alternativos pode estar sendo traçado por aqueles que, aparentemente, estão 'fora do jogo' – países e regiões periféricos, pobres e grupos sociais e étnicos marginalizados (Moulier Boutang, cap.3; Cocco, 2010). Essa compreensão pode ser frutífera para a análise da inovação em países em desenvolvimento, especialmente na América Latina, onde certas características culturais, como relações pessoais e emocionais interferindo naquilo que deveriam ser decisões econômicas racionais e impessoais, foram consideradas obstáculos ao desenvolvimento. (ALBAGLI & MACIEL, 2011, p.33-34)

REFERÊNCIAS BIBLIOGRÁFICAS

ALBAGLI, Sarita; LASTRES, Helena Maria Martins. Chaves para o Terceiro Milênio na Era do Conhecimento. In: ALBAGLI, Sarita; LASTRES, Helena Maria Martins (orgs). *Informação e globalização na era do conhecimento.* Rio de Janeiro: Campus, 1999.

ALBAGLI, Sarita; MACIEL, Maria Lucia. (Org.). *Informação, conhecimento e poder: mudança tecnológica e inovação social.* 1a. ed. Rio de Janeiro: Garamond, 2011.

ARENDT, Hannah. *A condição humana*. 10. ed. Rio de Janeiro: Forense Universitária, 2004.

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. *O Tratamento de Dados Pessoais em Portugal – breve guia prático.* Portugal, 2014. Acesso em jan de 2015. Disponível em www.apdsi.pt

BRASIL. Código Civil, Lei 10.406, de 10 de janeiro de 2002.

_____. Código de Defesa do Consumidor, Lei 8.078, de 11 de setembro de 1990.

_____. Código de Processo Penal, Lei nº 3.689, de 3 de outubro de 1941.

_____. Conselho Nacional de Justiça. Resolução 213, de 15 de dezembro de 2015. Dispõe sobre a apresentação de toda pessoa presa à autoridade judicial no prazo de 24 horas. 2015a.

_____. Conselho Nacional de Justiça e o Ministério da Justiça. Processo nº: CNJ-ADM-2015/00800 Espécie: Termo do Compromisso CNJ/MJ nº 005/2015 Partícipes: Conselho Nacional de Justiça e Ministério da Justiça. “Acordo de Cooperação Técnica” celebrado com o propósito de compor e estruturar as diretrizes e a promoção da política de monitoração eletrônica de pessoas, em consonância com o respeito aos direitos fundamentais. 2015b.

_____. Conselho Nacional de Justiça e o Ministério da Justiça. Processo nº: CNJ-ADM-2015/00833 Espécie: Acordo de Cooperação MJ/CNJ nº 06/2015 Partícipes: Ministério da Justiça e Conselho Nacional de Justiça. “Acordo de Cooperação Técnica” celebrado com o objetivo de ampliar a aplicação de alternativas penais com enfoque restaurativo, em substituição à privação de liberdade. 2015c.

_____. Conselho Nacional de Justiça e o Ministério da Justiça. Processo nº: CNJ-ADM-2015/00936 Espécie: Termo do Compromisso CNJ/MJ/IDDD nº 007/2015 Partícipes: Conselho Nacional de Justiça, Ministério da Justiça e Instituto de Defesa do Direito de Defesa. “Acordo de Cooperação Técnica” celebrado para a instituição de Audiências de Custódia nas Comarcas de todo o país. 2015d.

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

_____. Decreto nº 7.627, de 24 de novembro de 2011. Regulamenta a monitoração eletrônica de pessoas prevista no Decreto-Lei 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.

_____. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição. 2012a.

_____. Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. 2012b.

_____. Instrução Normativa GSIPR Nº 1, de 13 de junho de 2008.

_____. Lei de Acesso à Informação. Lei nº 12.527, de 18 de Novembro de 2011. 2011a.

_____. Lei de Execução Penal, Lei 7.210, de 11 de julho de 1984.

_____. 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.

_____. Lei nº 12.403, de 04 de julho de 2011. Altera dispositivos do Decreto-Lei no 3.689, de 3 de outubro de 1941 - Código de Processo Penal, relativos à prisão processual, fiança, liberdade provisória, demais medidas cautelares, e dá outras providências. 2011b.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

_____. Ministério da Justiça / Departamento Penitenciário Nacional / Programa das Nações Unidas para o Desenvolvimento. *Elaboração de proposta de conceitos, princípios e diretrizes para as alternativas penais no âmbito do Projeto BRA/011/2014*. Brasília: PNUD, 2015e.

_____. Ministério da Justiça / Departamento Penitenciário Nacional / Programa das Nações Unidas para o Desenvolvimento. *Elaboração de proposta de princípios e diretrizes para a política prisional no âmbito do Projeto BRA/011/2014.* Brasília: PNUD, 2015f.

_____. Ministério da Justiça / Departamento Penitenciário Nacional. *Levantamento Nacional de Informações Penitenciárias. Infopen – Junho de 2014*. Brasília: DEPEN, 2015g.

_____. Ministério da Justiça / Departamento Penitenciário Nacional / Programa das Nações Unidas para o Desenvolvimento. *Relatório - 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: PNUD, 2015h. Acesso em dez 2015. Disponível em https://www.justica.gov.br/noticias/mj-divulga-primeiro-diagnostico-nacional-sobre-monitoracao-eletronica-de-pessoas

_____. Ministério do Planejamento, Orçamento e Gestão Secretaria de Logística e Tecnologia da Informação Departamento de Governo Eletrônico. Padrões de Interoperabilidade de Governo Eletrônico – Documento de referência. 2016a. Acesso em fev 2016. Disponível em http://www.governoeletronico.gov.br/eping

_____. Norma Complementar N º 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008.

_____. Norma Complementar N º 03/IN01/DSIC/GSIPR, de 30 de junho de 2009.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 2000.

_____. Presidência da República. Casa Militar. Departamento de Segurança da Informação e Comunicações. *Guia básico de orientações ao gestor em segurança da informação e comunicações: versão 2.0*. Danielle Rocha da Costa, José Ney de Oliveira Lima (orgs). Brasília: Presidência da República, 2016b.

_____. Tribunal de Contas da União (TCU). *Boas Práticas em Segurança da Informação*. 2ª edição, Brasília, 2007.

_____. Tribunal de Contas da União (TCU). Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal, Relator Ministro Benjamin Zymler. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008.

CANOTILHO, J.J.. *Direito Constitucional e Teoria da Constituição*. 7ª ed.. Coimbra: Ed. Almedina, 2003.

CASTELLS, Manuel. *A Sociedade em rede a era da informação: Economia, Sociedade e Cultura*. *Volume I*. 2.º edição. Lisboa: Fundação Calouste Gulbenkian, 2005.

_____. *Communication Power.* New York: Oxford University Press, 2009.

COUNCIL OF EUROPE - TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM. *Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais*. Roma,1950.

DONEDA, Danilo. A Tutela da Privacidade no Código Civil de 2002. In: *Anima Revista Eletrônica*. 1ª Ed. Vol I., 2009, p. 89-100.

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

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

DOUGLAS, Mary. *Pureza e Perigo*. São Paulo: Editora Perspectiva, 1991.

ELIAS, Norbert; SCOTSON, John L. *Os Estabelecidos e os Outsiders.* Rio de Janeiro: Jorge Zahar Ed., 2000.

ESTORILIO, Rafael Martins. A substituição das penas restritivas de direito pelo juízo de execução penal. In: *Revista CEJ.* Brasília, Ano XVI, n. 58, p. 15-25, set./dez. 2012.

FOUCAULT, Michel. *Microfísica do poder*. Rio de Janeiro: Graal, 2003

GIDDENS, Anthony. *Modernidade e identidade.* Rio de Janeiro: Jorge Zahar Ed, 2002.

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

GÓMEZ, Maria Nélida González. Informação, Conhecimento e Poder – do ponto de vista das relações entre política, economia e linguagem. In: ALBAGLI, Sarita; MACIEL, Maria Lucia. (Org.). *Informação, conhecimento e poder: mudança tecnológica e inovação social*. 1a. ed. Rio de Janeiro: Garamond, 2011. p. 183-210.

HOLANDA, Sérgio Buarque de. *Raízes do Brasil*. 26ª ed. São Paulo: Companhia das Letras, 1995.

KANT DE LIMA, Roberto. Entre as leis e as normas: Éticas corporativas e práticas profissionais na segurança pública e na Justiça Criminal. In: *Revista Dilemas.* Vol. 6 - n. 4, out-nov-dez, 2013.

KUHN, Thomas*. A estrutura das revoluções científicas*. 2. ed. São Paulo: Perspectiva, 1978.

LEVY, Pierre. *A inteligência coletiva*. São Paulo: Edições Loyola, 1998;

LOBÃO, Ronaldo J. da S. *Servidor Público: a serviço do Estado ou a Serviço do Público?* Niterói: Monografia de conclusão do curso de Bacharelado em Ciências Sociais da Universidade Federal Fluminense, 1997.

MIRANDA, Ana Paula Mendes de. Antropologia, Estado Moderno e Poder: perspectivas e desafios de um campo em construção. In: *Avá. Revista de Antropología*, 2005, p. 1-27.

MISSE, Michel, et.al.. *"Autos de Resistência": uma análise dos homicídios cometidos por policiais na cidade do Rio de Janeiro (2001-2011).* Relatório de pesquisa - coordenação Michel Misse, 2011.

NAVARRO, Ana Maria Neves de Paiva. *O Direito Fundamental à Autodeterminação Informativa*. 2011. Acesso em jan.2015. Disponível em http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*, adotada em 10 de dezembro de 1948.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Declaração Americana dos Direitos e Deveres do Homem*, 1948.

PARLAMENTO EUROPEU e CONSELHO DA UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

_____. Regulamento (CE) n. 45/2001 do Parlamento Europeu e do Conselho de 18 de Dezembro de 2000 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

_____. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas).

_____. Decisão-Quadro 2008/977/JAI do Conselho de 27 de Novembro de 2008 relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal.

_____. Decisão 2009/426/JAI do Conselho de 16 de Dezembro de 2008 relativa ao reforço da Eurojust e que altera a Decisão 2002/187/JAI

relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade.

PEZZI, Ana Paula Jacobus. *A Necessidade de Proteção de Dados Pessoais nos Arquivos de Consumo: em busca da concretização do direito à privacidade*. Universidade do Vale do Rio dos Sinos. Programa de Pós-Graduação em Direito. Dissertação (mestrado). São Leopoldo, 2007.

PIMENTA, Victor; MOURA, Tatiana. Sem Informação Não se faz Política Penal. In: *Informativo da Rede Justiça Criminal - Os Números da Justiça Criminal.* 8ª edição, Fev-2016.

PORTUGAL. Lei n.º 67/98, de 26 de Outubro. Lei da Protecção de Dados Pessoais - transpõe para a ordem jurídica portuguesa a directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

SERRA, Paulo. Informação e democracia – o sentido da crítica Rousseauniana da informação. In: CORREIA, João Carlos et.al. (orgs). *Comunicação e Poder*. Universidade da Beira Interior – Estudos em Comunicação: Covilhã - Portugal, 2002

WEBER, Max. Os fundamentos da organização burocrática: uma construção do tipo ideal. In: CAMPOS, Edmundo (org). *Sociologia da Burocracia*. RJ: Zahar editores. 1979, p. 15-28.