MONITORAÇÃO ELETRÔNICA E PROTEÇÃO DE DADOS PESSOAIS

ELECTRONIC MONITORING AND PERSONAL DATA PROTECTION

Daniel Marchionatti

Doutor pela USP. Mestre pela UFRGS. Juiz Auxiliar da Corregedoria Nacional de Justiça.
Ex-Magistrado Instrutor do Supremo Tribunal Federal. Ex-Juiz Auxiliar do Superior Tribunal de Justiça.
ORCID: 0000-0002-2200-9570
daniel.barbosa@trf4.jus.br

Resumo: A monitoração eletrônica coleta dados pessoais que podem ser de interesse da segurança pública e de investigações criminais. No Brasil, essas informações são sigilosas, o que impede o compartilhamento com a polícia, salvo mediante ordem judicial. Alguns outros países facilitam o acesso de órgãos policiais aos dados de monitoramento. *De lege ferenda,* poder-se-ia cogitar algum compartilhamento de dados com órgãos policiais, mediante processo de pseudonimização, o que preservaria a privacidade das pessoas monitoradas e evitaria direcionamentos indevidos.

Palavras-chave: Monitoração Eletrônica - Dados Pessoais - Pseudoanonimização.

Abstract: Electronic monitoring collects personal data that may be of interest to public safety agencies and criminal investigations. In Brazil, this information is confidential, which prevents sharing with the police, except by court order. Some other countries make it easier for law enforcement agencies to acquire that data. One could consider some sharing of data with police agencies, through a process of pseudonymization, which would preserve the privacy of the people being monitored and avoid misdirection.

Keywords: Electronic Monitoring - Personal Data - Pseudonymization.

Este artigo analisa o uso dos dados coletados pela monitoração eletrônica, em especial para fins processuais penais e de segurança pública. No Brasil, normas infralegais consagram o sigilo dos dados da monitoração, passível de afastamento apenas mediante ordem judicial.

A monitoração eletrônica coleta e armazena os dados de movimentação da pessoa em tempo real.[1] O equipamento preso ao corpo interage com a central, que armazena as coordenadas de localização espacial a cada momento. Com isso, é possível saber onde e quando o aparelho esteve – e, por consequência, reproduzir os deslocamentos do usuário.[2]

Os dados coletados pela monitoração eletrônica são pessoais. Enquadram-se no conceito amplo de "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I, da Lei Geral de Proteção de Dados Pessoais).[3]

Não há uma norma com *status* de lei dispondo sobre o uso desses dados. A legislação de execuções penais e de processo penal não avança nessa seara. A Lei Geral de Proteção de Dados Pessoais, por sua vez, exclui de seu âmbito de aplicação o tratamento de dados pessoais para fins de segurança pública, investigação e repressão a infrações penais (art. 4º, III, "a" e "d").

Apesar da falta de lei em sentido próprio, há normas que estabelecem o sigilo dos dados coletados pela monitoração. O Decreto 7.627/2011 dispõe que o "sistema de monitoramento será estruturado de modo a preservar o sigilo dos dados e das informações da pessoa monitorada" (art. 6º).[4] A Resolução 5, de 10 de novembro de 2017, do Conselho Nacional de Política Criminal e Penitenciária (CNPCP),[5] reforça o caráter sigiloso dos dados coletados (art. 22), afirmando que "devem ser considerados dados pessoais sensíveis", porque "apresentam, de forma inerente, potencialidade lesiva e discriminatória" (art. 23).

A Resolução do CNPCP[6] ainda procura limitar a coleta e o acesso ao estritamente necessário. Assim, veda aos bancos de dados "conter informações pessoais excedentes, desnecessárias ou em desconformidade com as finalidades dos serviços" (art. 23, parágrafo único) e limita o acesso ordinário aos "servidores expressamente autorizados que tenham necessidade de conhecê-los em virtude de suas atribuições" (art. 24), exigindo ordem judicial para acesso por investigação criminal (art. 24, parágrafo único).

A Resolução 412/2021, do Conselho Nacional de Justiça,[7] segue

linha semelhante. Estabelece o sigilo das informações (art. 13, § 1º), definindo como finalidade de sua coleta o "cumprimento das condições estabelecidas judicialmente", embora ressalve que os dados podem ser "utilizados como meio de prova para apuração penal" (art. 13). Determina que o compartilhamento dos dados exige ordem judicial (art. 13, § 2º), salvo "iminente risco à vida", hipótese na qual os órgãos de segurança pública podem requisitar a localização da pessoa em tempo real diretamente à Central de Monitoramento (art. 13, § 3º). O compartilhamento de dados, por iniciativa da Central de Monitoramento, só é permitido para atender aos incidentes da monitoração (art. 13, § 6º).

Tratar os dados como sigilosos é inegável acerto. São dados que dizem respeito à privacidade da pessoa monitorada e que são protegidos diretamente pela Constituição da República (art. 5º, X), muito embora não se aplique diretamente à legislação de proteção de dados pessoais.

TRATAR OS DADOS COMO SIGILOSOS É INEGÁVEL ACERTO. SÃO DADOS QUE DIZEM RESPEITO À PRIVACIDADE DA PESSOA MONITORADA E QUE SÃO PROTEGIDOS DIRETAMENTE PELA CONSTITUIÇÃO DA REPÚBLICA (ART. 5º, X), MUITO EMBORA NÃO SE APLIQUE DIRETAMENTE À LEGISLAÇÃO DE PROTEÇÃO DE DADOS PESSOAIS

Entre os agentes públicos, o acesso e o tratamento dos dados coletados devem ser limitados ao necessário para atingir as finalidades da medida. Apenas os agentes públicos com atribuição para executar essas finalidades devem ter a possibilidade de tratar os dados.

A primeira finalidade do tratamento dos dados pelos agentes públicos é a fiscalização das condições da monitoração. A monitoração eletrônica pode estar sujeita a condições, as quais somente podem ser estabelecidas judicialmente (art. 11, I, da Resolução 412/2021, do Conselho Nacional de Justiça).[8] Estão entre as condicionantes mais comuns, as áreas de inclusão ou exclusão e a vedação de aproximação de pessoas determinadas. Por exemplo, a decisão pode determinar que a pessoa monitorada deve permanecer em casa à noite, somente pode transitar durante o dia, de casa para o local de trabalho e que deve se abster de se aproximar da casa do ofendido, de forma que cometerá uma infração caso saia de casa à noite, ou se afaste do caminho entre a casa e o trabalho, ou se aproxime da casa do ofendido. Os agentes responsáveis pela execução penal ou pela fiscalização da medida imposta no curso do processo podem tratar os dados coletados para verificar se a pessoa monitorada está observando as condições impostas.

Ocorre que a fiscalização das condições não resume a finalidade da monitoração eletrônica. Em alguns casos concretos, nem sequer são estabelecidas condicionantes. A legislação não estabelece nenhuma condicionante obrigatória, deixando a cargo do juiz decidir pela sua imposição, conforme um juízo de proporcionalidade. É possível que o magistrado estabeleça a monitoração, sem fazer nenhuma especificação adicional em sua decisão.

A vigilância da pessoa monitorada é uma segunda finalidade da monitoração admitida em nosso Direito. Essa vigilância tem função precipuamente preventiva – desestimular a prática de crimes – e eventualmente investigatória – produção da prova inicial da responsabilidade penal ou da inocência. Saber que está sendo vigiada pode dissuadir a pessoa de se envolver em ilícitos. Caso um delito ocorra, a monitoração pode colher prova de localização da pessoa monitorada, levando à exoneração ou servindo como início de prova da responsabilidade penal.

Para alcançar essa finalidade, é necessário que os órgãos de persecução penal – e, eventualmente, de segurança pública – tenham acesso aos dados de monitoração.

Esse acesso, no entanto, traz uma série de preocupações. Como reconheceu o CNPCP, os dados produzidos pela monitoração são sensíveis e têm "potencial lesivo e discriminatório" (art. 4º, XI, da Resolução 5/2017).[9] O livre acesso pode levar ao direcionamento abusivo das apurações aos monitorados. Isso pode produzir acusações injustas e levar à impunidade dos verdadeiros culpados. Assim, surgem preocupações com a privacidade da pessoa monitorada, que tem sua rotina exposta a um círculo maior de agentes públicos, e com a própria qualidade das apurações.

No entanto, a falta de acesso dos investigadores aos dados também produz perplexidades. Ainda que haja elementos indicando que pessoas monitoradas tiveram algum contado com delitos – como vítimas, testemunhas ou perpetradores –, não será possível fazer a informação chegar à polícia judiciária, salvo se uma investigação prévia identificar pessoas monitoradas como possíveis envolvidos.

Também se perde a chance, desde logo, exonerar de suspeita pessoas inocentes. A semelhança de circunstâncias pode levar a suspeitas infundadas contra pessoas com contato anterior com os órgãos de persecução penal. Assim, uma pessoa monitorada pode

se tornar suspeita de um delito praticado em local no qual não estava. Isso contribui para a estigmatização e desperdiça recursos investigatórios.

O Direito Comparado demonstra que, de uma forma geral, os países fornecem considerável acesso aos dados de monitoramento aos investigadores. Nesse sentido vai a legislação da França, que permite o tratamento dos dados, diretamente pelos investigadores, para verificar a localização do monitorado em apurações de "crime ou delito", além de outras apurações sem caráter criminal claramente estabelecido – verificação de causa morte ou razão de desaparecimento, lesões de origem desconhecida ou localização de fugitivos (R57-30-2,[10] § 4º, e R57-30-5,[11] § 4º). Portugal prevê que as informações podem ser solicitadas diretamente pela polícia judiciária "para fins de investigação criminal" (art. 31 da Lei 33/2010).[12] No Reino Unido, os dados produzidos com a monitoração eletrônica são considerados "dados pessoais coletados para fins de aplicação da lei" e podem ser empregados para "qualquer outro propósito de aplicação da lei". Quando necessário e proporcional, o controlador dos dados pode enviar os dados com Agências para propósitos relevantes de aplicação da lei, como investigação, prisão e instrução de causas criminais.[13]

Uma solução intermediária, que poderia ser avaliada em nosso país, é o compartilhamento de dados não atuais e pseudonimizados aos órgãos de investigação penal e de segurança pública. A "pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (art. 13, § 4º, da LGPD). O acesso aos dados de movimentação em datas pretéritas, sem identificação da pessoa monitorada, permitiria aos investigadores e policiais ter um ponto de partida, mas dificultaria o direcionamento das apurações e preservaria a privacidade. Se os dados apontassem para a proximidade temporal e espacial de um sujeito monitorado a um delito, seria possível, aí sim mediante ordem judicial, identificar quem seria essa pessoa. Nesse caso, o magistrado determinaria que a identidade daquele monitorado, mantida em separado pela Central de Monitoração Eletrônica, fosse fornecida à investigação.

Essa solução é apresentada apenas *de lege ferenda.* Atualmente, o regime em vigor consagra o sigilo e a necessidade de ordem judicial para acesso aos dados produzidos pela monitoração.

É importante ter em mente que a associação de pessoa monitorada a determinado perímetro não é, por si só, prova de responsabilidade criminal. A acurácia dos sistemas de monitoração não é absoluta e, ainda que a presença da pessoa no perímetro seja comprovada, a demonstração da autoria ou da participação em delito exige provas adicionais. Usar os dados de monitoração eletrônica como prova única para condenações seria fonte de injustiças contra as pessoas monitoradas e de impunidade dos verdadeiros autores de delitos.

Os dados coletados pela monitoração eletrônica dizem diretamente com a privacidade e devem ser protegidos. Informadas pela correta preocupação em proteger a pessoa monitorada contra abusos, as normas adotadas até o momento optaram por estabelecer o sigilo dos dados de monitoramento.

Notas

[1] Além desses, outros dados pessoais são coletados e armazenados pela monitoração. Dentre eles, estão dados cadastrais do monitorado, áreas de inclusão e exclusão, incidentes de perda de sinal ou descarga de bateria, etc. Também dados de terceiros – em especial, da pessoa ofendida, em casos envolvendo violência doméstica e familiar – podem ser coletados.

[2] Há fatores que podem influir na precisão das informações – limitações tecnológicas, relevo, fenômenos atmosféricos, etc. O grau de acurácia precisa ser levado em consideração, caso eventualmente os dados venham a ser empregados na persecução penal.

[3] BRASIL, 2018.

[4] BRASIL, 2011.

[5] BRASIL, 2017.

[6] BRASIL, 2017.

[7] BRASIL, 2021.

[8] BRASIL, 2021.

[9] BRASIL, 2017.

[10] FRANÇA, 2020.

[11] FRANÇA, 2016.

[12] PORTUGAL, 2010.

[13] REINO UNIDO, 2020. §§ 6 e 24.

Referências

BRASIL. Decreto 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7627.htm. Acesso em: 16 nov. 2021.

__. Conselho Nacional de Política Criminal e Penitenciária (CNPCP). Resolução 5, de 10 de novembro de 2017. Dispõe sobre a política de implantação de Monitoração Eletrônica e dá outras providências. Disponível em: https://www.gov.br/depen/pt-br/composicao/cnpcp/resolucoes/2017/resolucao-no-5-de-10-de-novembro-de-2017.pdf/view. Acesso em: 16 nov. 2021.

__. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 nov. 2021.

__. Conselho Nacional de Justiça (CNJ). Resolução 412 de 23 de agosto de 2021. Estabelece diretrizes e procedimentos para a aplicação e o acompanhamento da medida de monitoramento eletrônico de pessoas. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4071. Acesso em: 16 nov. 2021.

FRANÇA. Conselho de Estado. Décret nº 2016-261 du 3 mars 2016 relatif aux traitements automatisés du contrôle des personnes placées sous surveillance électronique et sous surveillance électronique mobile et modifiant le code de procédure pénale. Disponível em: https://www.legifrance.gouv.fr/loda/id/LEGIARTI000032155249/2016-03-06/. Acesso em: 16 nov. 2021.

__. Décret nº 2020-128 du 18 février 2020 portant application de diverses dispositions pénales de la loi nº 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. Disponível em: https://www.legifrance.gouv.fr/loda/id/LEGIARTI000041602601/2020-02-20/. Acesso em: 16 nov. 2021.

PORTUGAL. Lei 33, de 2 de setembro de 2010. Regula a utilização de meios técnicos de controlo à distância (vigilância electrónica) e revoga a Lei n.º 122/99, de 20 de Agosto, que regula a vigilância electrónica prevista no artigo 201.º do Código de Processo Penal. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1269&tabela=leis&so_miolo=. Acesso em: 16 nov. 2021.

REINO UNIDO. Code of Practice – Electronica Monitoring Data. Crown Copyright. Londres: 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/926813/em-revised-code-practice.pdf.). Acesso em: 16 nov. 2021.

Autor convidado