

A “placa eletrônica” e o monitoramento de automóveis na Sociedade da Vigilância.

Danilo Doneda¹

Todos os automóveis brasileiros licenciados deverão portar uma “placa eletrônica” que os identifique automaticamente em todas as vias de circulação pública brasileiras. Este é o teor da Resolução nº 212 de 2006 do Conselho Nacional de Trânsito – CONTRAN, que estabelece, além desta obrigatoriedade, as normas técnicas a serem obedecidas e o cronograma de implementação do SINIAV - Sistema de Identificação Automática de Veículos².

A utilização de um sistema automatizado para o rastreamento do tráfego automotivo é, sob diversos aspectos, uma idéia interessante. O seu uso compulsório pode facilitar a repressão ao furto e roubo de veículos, bem como fornecer dados valiosíssimos para o planejamento viário e urbanístico, somente para citar dois dos exemplos mais evidentes – aliás ressaltados pela própria resolução.

Porém, como em tantas outras situações nas quais os benefícios das novas tecnologias parecem ofuscar quaisquer outras ponderações, há um certo lado obscuro na forma com que se pretende fazer tal implementação que suscita graves questionamentos sobre as liberdades pessoais que podem ser colocadas em risco.

A questão diz respeito propriamente à utilização das informações que serão coletadas. Tenha-se em conta, primeiramente, que um tal sistema, após implementado, resultaria na criação de um banco de dados com informações detalhadas sobre os locais em que estivemos com nossos automóveis em determinados dias e horas – fornecendo um esboço bastante completo de nossas andanças, disponível a quem quer que tenha acesso, autorizado ou não, a este banco de dados.

A bem da verdade, a universalização da vigilância eletrônica já existe a despeito desta novidade. Por exemplo, é possível às operadoras de telefonia celular traçarem um mapa dos deslocamentos de um determinado telefone (e de seu proprietário, o que aliás vem sendo usado em alguns países para fins de persecução penal) a partir das estações com as quais o telefone se conecta. Também as movimentações bancárias e de cartões de crédito, entre diversos outros atos cotidianos, deixam seus rastros, justificando a caracterização que deu David Lyon da “Sociedade da Vigilância”.

Este cenário condiz com a feição que a computação em rede vem tomando sob nossos olhos. As redes cada vez mais conectam não propriamente pessoas, porém objetos – este é o paradigma futuro de uma “Internet das coisas”. Coisas, objetos,

¹ Doutor em Direito civil pela UERJ; pesquisador na Università degli Studi di Camerino; professor na Faculdade de Direito de Campos e na UniBrasil. Mantenedor de <www.habeasdata.org.br>.

² Disponível em: <http://www.denatran.gov.br/download/Resolucoes/RESOLUCAO_212.rtf>.

conectados à rede, criando ambientes inteligentes que reagem à presença das pessoas e de movimentos; um paradigma que poderá enriquecer o nosso vocabulário cotidiano com expressões como “computação ubíqua” ou “inteligência ambiental”. O reflexo prático disto, por exemplo, é que a recepcionista de um edifício saberá a qualquer momento onde se encontra cada pessoa em seu interior. No limite, podemos chegar à situação aludida por Mark Weiser, de que poderemos ter um diário “que se escreve a si mesmo”³.

Este cenário, porém, não deve ser utilizado para justificar a inevitabilidade de mais uma medida de caráter tecnocrático, que possa acelerar a gradual erosão das liberdades fundamentais – pelo contrário, deve ser lido dentro deste contexto para que seus efeitos sejam devidamente considerados.

Há vários motivos que fundamentam o potencial prejuízo ao cidadão pela criação de mais um banco de dados a seu respeito. Por exemplo, os seus dados pessoais podem ser armazenados em sistemas suscetíveis de ataques informatizados e utilizados por terceiros contra o seu interesse. Esta é a idéia presente na noção de “risco informático”, um risco inerente às atividades de processamento de dados e que contribui a fragilizar a posição do cidadão na Sociedade da Informação. Outro ponto é que a utilização da informação pessoal deve ser tão transparente quanto possível para o cidadão, que deve sempre saber qual informação existe a seu respeito, qual a finalidade a que se destina e a quais pessoais ela estará disponível – ao contrário, cresce o risco da pessoa ser indevidamente julgada e controlada somente a partir de seus dados, sem que possa se defender e nem mesmo alegar uma eventual falsidade destes próprios dados.

A implementação de um banco de dados pessoais, em especial deste porte, há de ser considerada como uma atividade que implica em um risco por si mesma. A criação de um risco do gênero, para que possa se harmonizar com as previsões constitucionais de proteção à pessoa em relação à sua dignidade e privacidade, somente seria justificada mediante a verificação de duas condições (i) que seus respectivos benefícios o justifiquem, após uma necessária ponderação dos valores existenciais e patrimoniais em questão; e (ii) que sejam tomadas medidas para reduzir os danos potenciais a um mínimo possível. Esta idéia, aliás, pode ser verificada com clareza nas leis alemã e italiana sobre proteção de dados pessoais, no momento em que se referem ao chamado “princípio da necessidade”, segundo o qual o tratamento de dados somente se justifica quando for estritamente necessário para o fim a ser alcançado, sendo que os dados pessoais devem ser utilizados na menor medida possível⁴.

A existência de um repositório de informações tão rico sobre as idas e vindas de tantos cidadãos pode, conforme verificado, induzir a sua utilização de forma abusiva,

³ Mark Weiser. “The computer for the 21st century”, in: *Scientific American*, setembro, 1991.

⁴ A referida lei alemã, a *Bundesdatenschutzgesetz* (BDSG), estabelece, em seu § 3a, que “os sistemas de processamento de dados serão projetados e implementados de acordo com o objetivo de não coletar, processar ou utilizar dados pessoais ou tão poucos dados pessoais quanto for possível (...)”; na Itália, o *Código in matéria di protezione dei dati personali* (Decreto Legislativo n. 196, de 30 de junho de 2003), prevê em seu art. 3 o Princípio de necessidade no tratamento de dados, ao prever que “Os sistemas informativos e os programas informáticos serão configurados reduzindo ao mínimo a utilização de dados pessoais e de dados de identificação, de modo a excluir o seu tratamento quando as finalidades a serem atingidas em cada caso possam ser realizadas mediante, respectivamente, dados anônimos ou eventuais meios que permitam a identificação do interessado somente em caso de necessidade” (tradução livre).

quando não por parte dos que possuem acesso ao sistema, igualmente no caso de acesso não-autorizado - por exemplo, mediante a invasão de sistema informático. É necessária, a elaboração de uma política de acesso e de segurança de dados, com a identificação de procedimentos de segurança a serem adotados e respectivos responsáveis, tornando o sistema suficientemente robusto e seguro do ponto de vista da arquitetura da informação.

Em suma, um sistema poderoso como o SINIAV somente pode ser cogitado se levados na devida conta os riscos potenciais ao cidadão pelo uso abusivo ou indevido de suas informações pessoais. Isto seria possível com o delineamento de um sistema no qual o cidadão tenha claro quais as suas informações que serão coletadas, por quem e para quais finalidades serão utilizadas, quais os meios que ele terá para efetivar o seu direito de acesso à tais informações e, caso necessário, solicitar sua correção ou cancelamento. E, muito importante, garantias de que estas informações não serão repassadas a terceiros, a não ser com seu expresso consentimento ou por força de lei.

Outras iniciativas semelhantes de monitoramento, em outros países, costumam ser contrastadas pela devida consideração dos seus efeitos para as liberdades individuais. Para mencionar um exemplo mais recente, o relatório anual da CNIL (*Commission Nationale de l'Informatique et des Libertés*)⁵, a autoridade administrativa independente francesa encarregada de zelar pela proteção de dados pessoais, alerta justamente para os riscos da “Sociedade da vigilância”. Dentre os casos tratados está a “geolocalização” de veículos comerciais, que a autoridade considera possível somente quando determinadas condições e restrições são observadas.

Ao contrário do que a gravidade da situação sugere, a referida Resolução é demasiadamente sintética ao tratar das garantias referentes aos dados tratados, prevendo somente, em seu art. 7º, que “As informações obtidas através do SINIAV e que requeiram sigilo serão preservadas nos termos da Constituição Federal e das leis que regulamentam a matéria.”

No que diz respeito à proteção dos dados dos cidadãos, além do perigo potencial representado pela mera existência deste banco de dados, mencione-se também, em vista da única ressalva neste sentido prevista pela Resolução, que uma política de utilização dos dados pessoais do cidadão não pode basear-se somente em um modelo binário que classifique os dados entre “sigilosos” e “públicos”.

Tal sistema binário muitas vezes é evocado ao se cogitar da utilização de informações pessoais. O fato é que hoje, com as vastas possibilidades de coleta e processamento de informações, não mais podemos reputar categoricamente uma informação como “pública” ou “sigilosa”; “inócua” ou “sensível” – ou, melhor, esta categorização não é mais útil como o foi em um tempo no qual as possibilidades de acesso e intercâmbio de informações eram tremendamente menores do que são hoje. Toda e qualquer informação pessoal, na verdade, pode ser utilizada lícita ou abusivamente, dependendo da forma como é usada e da finalidade a que se destina. Assim, mais eficiente do que um mero sistema de proibições e permissões para uso da informação pessoal é um sistema que garanta a transparência da sua utilização para o seu titular e o seu amplo direito de acesso e retificação.

⁵ Disponível em: <http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-27erapport-2006.pdf>.

Um sistema como o SINIAV, portanto, deve vir acompanhado de previsões específicas sobre a utilização e segurança dos dados pessoais coletados, sob pena de representar uma concreta ameaça à privacidade e às garantias fundamentais dos cidadãos – suscitando mesmo legítimas dúvidas quanto à sua constitucionalidade, principalmente no que tange ao direito à privacidade dos condutores de veículos. Mesmo certas medidas paliativas aparentemente óbvias, como a anonimação dos dados para os tratamentos que tenham como finalidade a otimização do planejamento viário e urbano, estão ausentes da resolução. Uma medida deste gênero, em conclusão, somente será legítima caso seja capaz de fornecer a devida garantia e proteção a todos os interesses em questão e, acima de tudo, às garantias invioláveis do cidadão, o que não é o caso em sua atual formulação.