Lippi: Imagens de vigilância, reconhecimento facial e a LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) está em vigor. Com a frequente utilização de câmeras de vídeo para segurança privada, inclusive com reconhecimento facial, surgem questões sobre a [illegible]pturadas à LGPD.

A lei considera a imagem da pessoa como um dado pessoal, mais ainda, como um dado pessoal sensível uma vez que é considerado dado biométrico, o que exige um cuidado mais rigoroso em seu tratamento.

Via de regra, o tratamento de dado pessoal sensível é possível desde que o titular do dado manifeste seu consentimento (autorização) para o uso de uma finalidade — o que seria impossível em um ambiente como o de shopping center. Entretanto, conforme artigo 11, II, alínea "e", da LGPD, há dispensa do consentimento para tais imagens/filmagens desde que para a finalidade de proteção da vida, integridade física do titular do dado ou de terceiros, mas o uso dessas imagens deve cumprir estritamente esta finalidade. Assim, não podem ser utilizadas para qualquer outra destinação ou finalidade, como, por exemplo, monitorar a atividade do cliente dentro do shopping e/ou utilização para análise de ações de marketing.

Passamos para uma zona cinzenta quando houver uma parceria com poder público, para que o shopping tenha acesso a um banco de dados de imagens de procurados pela polícia, para que os dados biométricos coletados imagem do cliente sejam utilizados para checagem. Isso porque as imagens estão sendo utilizadas para a finalidade de segurança pública que estão dispensadas da aplicação da LGPD, porém capturadas por uma empresa privada — que está obrigada à LGPD.

Essas situações ainda necessitam de regulação pela Agência Nacional de Proteção de Dados (ANPD), podendo ainda existir também a aplicabilidade de eventuais legislações locais. Entretanto, caso ocorra esta parceria com poder público é importante formalizar convênio específico, além de tratar a coleta desses dados sensíveis de forma muito cuidadosa, obedecendo os requisitos de segurança da informação, pois qualquer vazamento pode proporcionar danos não só financeiros, mas reputacionais ao shopping que coletou e tratou tais dados.

Outra forma de minimizar riscos nessa relação de parceira com poder público é divulgar de forma visível de que o ambiente está sendo filmado para a finalidade de segurança e caso seja identificado algum

procurado pela polícia que a mesma seja acionada para fazer a abordagem da pessoa, uma vez que, apesar de haver a tecnologia de reconhecimento facial, existe a possibilidade de ocorrer uma abordagem errônea proporcionando um constrangimento à pessoa e, consequentemente, responsabilização por danos.

Isso porque essa checagem se dará por meio de algoritmos que ainda possuem muitos vieses de seus programadores possibilitando margem para erros. Dessa forma, é imperativo o controle e revisão humana dos algoritmos, a fim de se evitar decisões equivocadas baseadas em informações inconsistentes.

Por fim, de forma geral, existem alguns fatores que pedem um exame maior da questão. Há necessidade de se deixar claro o balanceamento entre a necessidade da coleta do dado biométrico e a necessidade do tratamento. Por quanto tempo serão armazenadas as imagens? Como serão descartadas? Independentemente do consentimento ou não, o tratamento de dados biométricos deve ser feito mediante aviso prévio, as imagens dever ser tratadas dentre padrões de segurança da informação, não podendo haver desvio da finalidade do tratamento.

Em resumo, a utilização de imagens e o reconhecimento facial devem ser utilizados com finalidades muito bem definidas, específicas e limitadas, respeitando-se os direitos dos titulares dos dados pessoais, sendo possível minimizar riscos através de uma governança de dados transparente e com os mais altos níveis de segurança da informação.

Date Created
25/10/2020