

Patel vs. Facebook

País: Estados Unidos

Região: América do Norte

Número do caso: 18-15982

Data da decisão: 8 de agosto de 2019

Desfecho: Manutenção da decisão proferida na primeira instância

Órgão judicial: Segunda instância

Área do direito: Direito Civil

Temas: Privacidade / Proteção e Retenção de Dados

Palavras-chave: Privacidade, Dados biométricos, Mídia social, Facebook, Reconhecimento facial

ANÁLISE DO CASO

Resumo do caso e desfecho

O Tribunal de Segunda Instância do Nono Circuito dos Estados Unidos decidiu que a tecnologia de reconhecimento facial utilizada para criar modelos faciais sem consentimento prévio invade os interesses e a privacidade dos indivíduos. Em 2010, o Facebook começou a utilizar a tecnologia de reconhecimento facial para desenvolver a



sua funcionalidade "Tag Suggestions" (sugestões de marcação) sem o consentimento prévio por escrito dos usuários e sem um cronograma de retenção da informação biométrica. Três usuários do Facebook em Illinois propuseram uma ação em 2015, alegando que a tecnologia de reconhecimento facial do Facebook violava a Lei de Privacidade de Informações Biométricas de Illinois. O Tribunal confirmou a decisão do Tribunal Distrital dos Estados Unidos do Distrito Norte da Califórnia, entendendo que a tecnologia de reconhecimento facial do Facebook afetou a privacidade e os assuntos pessoais dos usuários e, ainda, sinalizou para o impacto que os avanços tecnológicos podem ter sobre a privacidade.

Fatos

Em 2010, o Facebook implementou um novo recurso, Tag Suggestions (sugestões de marcação), que utilizava a tecnologia de reconhecimento facial para identificar indivíduos em fotografias carregadas por um usuário que havia habilitado a função Tag Suggestions. Este recurso permitiu a marcação automática de outros usuários em fotografias carregadas no Facebook; foi além da marcação original que era manual e permitiu que o usuário identificasse outros usuários em suas fotografias, com um link para os perfis desses usuários. A tecnologia do Facebook era aplicada a fotografias digitalizadas quando eram carregadas e extraía "os diversos pontos de dados geométricos que fazem com que um rosto seja único, como a distância entre os olhos, nariz e orelhas, para criar uma assinatura ou mapa do rosto", comparava esse "mapa" com modelos de rostos de usuários salvos em seus bancos de dados e, em seguida, sugeria a marcação de um usuário específico na fotografia.

Em agosto de 2015, três usuários do Facebook que vivem em Illinois, EUA, Nimesh Patel, Adam Pezen e Carlo Licata, agindo como representantes de uma ação coletiva, propuseram uma ação contra o Facebook, alegando que a tecnologia de reconhecimento facial do Facebook violou a Lei de Privacidade de Informações Biométricas (Biometric Information Privacy Act, BIPA) do Illinois. Patel, Pezen e Licata são usuários do Facebook desde 2008, 2005 e 2009, respectivamente. A BIPA tinha sido implementada em 2008 e define um "identificador biométrico" como incluindo "uma 'digitalização da geometria da mão ou da face'" [p. 8].

Os autores argumentaram que o Facebook violou as seções 15(a) e 15(b) da BIPA porque coletou e utilizou informações biométricas dos usuários, especificamente os seus modelos faciais, sem o seu consentimento prévio por escrito para desenvolver o recurso de sugestões de marcação. Eles também afirmaram que o Facebook violou a BIPA porque não tinha um cronograma de retenção e destruição dos identificadores biométricos.

A seção 15(a) estabelece: "Uma pessoa jurídica na posse de identificadores biométricos ou informação biométrica deve desenvolver uma política por escrito, disponibilizada ao público, que estabeleça um cronograma de retenção e diretrizes para a destruição permanente de identificadores biométricos e informação biométrica quando o objetivo



inicial da coleta ou obtenção desses identificadores ou informação tiver sido satisfeito ou no prazo de três (3) anos após a última interação do indivíduo com a pessoa jurídica, o que ocorrer primeiro. Na ausência de um mandado ou intimação válida emitida por um tribunal competente, uma pessoa jurídica na posse de identificadores biométricos ou informações biométricas deve cumprir o seu cronograma de retenção estabelecido e as suas diretrizes de destruição".

A seção 15(b) estabelece: Nenhuma pessoa jurídica pode coletar, capturar, comprar, receber por meio de comércio, ou obter, de qualquer outra forma, o identificador biométrico ou a informação biométrica de uma pessoa ou de um cliente, a menos se primeiro: (1) informar, por escrito, ao titular dos dados ou seu representante legalmente autorizado que um identificador biométrico ou que uma informação biométrica está sendo coletada ou armazenada; (2) informar, por escrito, ao titular dos dados ou seu representante legalmente autorizado a finalidade específica e o período em que um identificador biométrico ou informação biométrica está sendo coletado, armazenado e utilizado; e (3) receber uma autorização por escrito, assinada pelo titular dos identificadores biométricos ou da informação biométrica ou seu representante legalmente autorizado.

A BIPA reconheceu que "biometria é diferente de outros identificadores únicos que são usados para acessar informações financeiras ou outras informações confidenciais" porque são 'biologicamente exclusivos' de um indivíduo e nunca poderiam ser alterados se a sua integridade fosse comprometida. A Legislatura de Illinois descreveu o propósito da legislação como: "o bem-estar, a segurança e a proteção pública serão garantidos por meio do controle da coleta, uso, salvaguarda, manuseio, armazenamento, retenção e destruição de identificadores e informações biométricas".

O Facebook interpôs um pedido de extinção da ação, argumentando que os usuários não provaram a existência de uma ilegitimidade.

O Tribunal Distrital negou o pedido do Facebook. O Facebook recorreu da decisão do Tribunal Distrital junto ao Tribunal de Segunda Instância dos Estados Unidos do Nono Circuito.

Visão geral da decisão

O Juiz Ikuta proferiu a sentença do plenário composto por três juízes. A principal questão perante o Tribunal era se a tecnologia de reconhecimento facial do Facebook violava as seções 15(a) e 15(b) da BIPA e o direito dos usuários à privacidade. A questão era se a "violação às exigências legais constituía uma inobservância dos seus direitos substantivos de privacidade" [p. 13].

Os usuários argumentaram que o Facebook violou as seções 15(a) e 15(b) do BIPA e os direitos de privacidade dos autores.

O Facebook alegou que os usuários descreveram violações procedimentais na ação e



não um dano.

O Tribunal apontou para a necessidade de se aplicar uma abordagem em duas etapas em casos como estes, a saber: a) determinar se há "uma violação a um interesse legalmente protegido que seja concreto e pormenorizado; e b) real ou iminente, não conjectural ou hipotético" [p. 10].

O Tribunal analisou a história do direito à privacidade, observando que os tribunais primeiro o reconheceram depois que Samuel D. Warren e Louis D. Brandeis publicaram um artigo, "The Right to Privacy" (O Direito à Privacidade, em tradução livre), na Harvard Law Review em 1890. Acrescentou que os processos do Supremo Tribunal Federal dos Estados Unidos, Departamento de Justiça vs. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 e n.º 15 (1989) e Cox Broadcasting Corp. vs. Cohn, 420 U.S. 469, 488 (1975) aceitaram essas "raízes do *common law* do direito à privacidade" [p. 15]. Entretanto, o Tribunal salientou que "estes direitos de privacidade estabelecidos pelo *common law* estão entrelaçados com zonas de privacidade constitucionalmente protegidas" e remeteu para os casos de Gibson vs. Fla. Legislative Investigation Comm., 372 U.S. 539, 569 n.º 7 (1963) e Kyllo vs. Estados Unidos, 9th Cir. 533 U.S. 27 (2001) que sustentaram que o direito à privacidade fazia parte das proteções constitucionais nos termos da Primeira Emenda (o direito à liberdade de expressão) e a Quarta Emenda (a proibição de buscas e apreensões desproporcionais). Em relação à Quarta Emenda, o Tribunal observou que a jurisprudência do Supremo Tribunal Federal "reconheceu que os avanços da tecnologia podem aumentar o potencial de intromissões desproporcionais na privacidade pessoal" [p. 16].

O Tribunal descreveu as ameaças à privacidade colocadas pela tecnologia de reconhecimento facial do Facebook e observou que a tecnologia atualmente permite que o Facebook identifique usuários individuais do Facebook, suas localizações e seus amigos, e que, no futuro, isso poderá viabilizar a identificação de indivíduos a partir de fotografias de vigilância. O Tribunal concluiu que o "desenvolvimento de um modelo facial usando tecnologia de reconhecimento facial sem consentimento (como alegado aqui) invade os assuntos particulares e interesses concretos de um indivíduo" [p. 17]. O Tribunal observou que, ao adotar a BIPA, a Assembleia Legislativa de Illinois havia reconhecido as ameaças à privacidade que os dados biométricos representavam e que, no caso Rosenbach vs. Six Flags Entertainment Corp., IL 123186 (em 2019, o Supremo Tribunal Federal de Illinois constatou que o propósito da BIPA era proteger a privacidade biométrica) [p. 17-18]. O caso Rosenbach também estabeleceu que um indivíduo pode sofrer danos devido à violação da BIPA quando uma pessoa jurídica não cumpre as suas obrigações nos termos da seção 15 porque essa inobservância causa uma invasão dos direitos dos indivíduos.

Desta forma, o Tribunal decidiu que as disposições da BIPA protegem os interesses concretos e a privacidade dos indivíduos e "não apenas determinações procedimentais" [p. 18].

Ao avaliar a segunda questão, "se as violações procedimentais específicas alegadas neste caso prejudicam realmente ou apresentam um risco material de dano a tais



interesses", o Tribunal se referiu ao caso Rosenbach ao observar que as disposições da BIPA são essenciais para proteger os direitos de privacidade em um mundo digital. O Tribunal enfatizou que a BIPA protege a privacidade biométrica, e a coleta desses dados pelo Facebook "necessariamente" viola os "direitos substantivos de privacidade" dos usuários [p. 19].

Portanto, o Tribunal decidiu que os usuários tinham demonstrado "dano concreto e pormenorizado" [p. 20].

O Tribunal também reiterou a decisão do Tribunal Distrital.

ORIENTAÇÃO DA DECISÃO

Ampliação da liberdade de expressão

O Tribunal reconheceu a proteção da privacidade biométrica ao abrigo da lei e afirmou que a violação dessa proteção legal é suficiente para constatar uma violação do direito à privacidade.

PERSPECTIVA GLOBAL

Leis internacionais e regionais correlatas

- EUA, *Whitney vs. Califórnia*, 274 U.S. 357 (1927)
- E.U.A., *Rosenbach vs. Six Flags Entertainment Corp.*, IL 123186 (2019)
- E.U.A., *Kyllo vs. Estados Unidos*, 533 U.S. 27 (2001)
- E.U.A., *Estados Unidos vs. Jones*, U.S. 10-1259, (2011)
- E.U.A., *Carpenter vs. Estados Unidos* (2018), No. 16-402
- E.U.A., *Riley vs. Califórnia*, 134 S.Ct. 2473 (2014)
- E.U.A., *Gibson vs. Fla. Legislative Invest. Comm.*, 372 U.S. 539 (1963).
- E.U.A., *Cox Broadcasting Corp. vs. Cohn*, 420 U.S. 469 (1975)
- E.U.A., *Departamento de Justiça Americano vs. Reporters Comm. for Freedom of the Press*, 498 U.S. 749 (1989)

SIGNIFICÂNCIA DO CASO

A decisão estabelece um precedente vinculante ou persuasivo dentro de sua jurisdição



DOCUMENTOS OFICIAIS DO CASO

Documentos oficiais do caso:

- **Decisão (Inglês)**
-