Departamento de
Informática e Estatística
CTC • UFSC

Análise Ética em Segurança da Informação para o aplicativo KIM

Aluna: Jessica Regina dos Santos
Disciplina: INE5429 - Segurança em Computação
Entrega: 07/04/2025

Sobre o sistema

O aplicativo KIM é uma plataforma digital que oferece soluções integradas para mobilidade urbana e pagamentos, com o objetivo de simplificar a rotina dos usuários no transporte público e em suas transações cotidianas. O sistema possui mais de 1 milhão de clientes em 70 cidades do Brasil, destacando-se no mercado de tecnologia de mobilidade (KIM, 2025).

Dados pessoais do usuário como CPF, nome completo, data de nascimento, endereço residencial, endereço de e-mail, número de telefone, foto da cédula de identidade ou CNH, entre outros, são coletados diariamente, assim como dados voltados a análise comportamental do cliente (perfil e comportamento de compra, volume e número de transações em estabelecimentos e por meio de aplicações) para gerar dados estatísticos (KIM, 2025).

Neste relatório, propõe-se uma análise aprofundada do aplicativo focada em questões éticas voltadas à segurança da computação. A análise será embasada principalmente por fundamentos discutidos em aula, documentação organizada pela KIM+ TECNOLOGIA EM MOBILIDADE LTDA, assim como respeitadas referências no contexto.

Ao final deste relatório, espera-se que esta análise contribua para uma compreensão mais clara dos desafios de segurança enfrentados pelo KIM, ofereça ideias para a melhoria contínua de sua infraestrutura de proteção e responsabilidade quanto aos usuários.

1 Responsabilidade Social e Profissional

Em geral, os dados fornecidos pelos usuários do KIM são organizados em quatro grandes grupos: dados pessoais, dados de registro de atividade, dados comportamentais e dados gerais de navegabilidade (KIM, 2025).

Os dados pessoais estão ligados a qualquer informação relacionada a pessoa natural identificada ou identificável. Podem ser CPF, nome completo, data de nascimento, endereço residencial, endereço de e-mail, nome completo da mãe, número de telefone, foto da cédula

de identidade ou CNH, foto estilo auto retrato (*selfie*) e autodeclaração de Pessoa Exposta Politicamente (PEP). Entre as principais finalidades a serem atingidas estão a verificação da identidade do usuário, cadastro de serviços, análise de crédito, identificação e prevenção de eventuais situações de fraude e a identificação e prevenção de eventuais ameaças de segurança (KIM, 2025).

Os dados de registro de atividade dizem a respeito de IP do usuário, hora e data de acesso, geolocalização, dados sobre o seu dispositivo de acesso e cookies. A coleta dos dados ocorre de forma automatizada por meio do site ou do aplicativo, para fins de identificação e prevenção de situações de fraude e ameaças de segurança (KIM, 2025).

O grupo formado pelos dados comportamentais faz análise de crédito e, o que nos interessa bastante no contexto da segurança da computação, análise comportamental ou transacional para fins de identificação e prevenção de situações de fraude e ameaças de segurança. São agrupados dados que envolvem o perfil e comportamento de compra dos usuários, além do volume e do número de transações em estabelecimentos por meio de aplicações (KIM, 2025).

Já os dados gerais de navegabilidade (também de ênfase analítica), tem como funcionalidade principal reconhecimento de perfis e hábitos de consumo coletivos dos usuários dos serviços, a fim de gerar dados estatísticos que possibilitem melhor compreensão de como se dão as interações dos usuários com as aplicações (KIM, 2025).

Segundo a Política de Privacidade do aplicativo KIM (2025), “a empresa adota medidas como testes periódicos de detecção de vulnerabilidades, proteção contra softwares maliciosos, controles de acesso e segmentação de rede, além de manter cópias de segurança dos dados pessoais, para assegurar a proteção das informações dos usuários. Essa abordagem, aliada à orientação para que os próprios usuários adotem comportamentos seguros, reforça a responsabilidade do KIM na segurança de dados, especialmente em transações envolvendo terceiros.” Tais medidas não só cumprem obrigações legais, como reforçam o compromisso com seus clientes, que dependem da plataforma para o manejo seguro de suas informações pessoais e financeiras diariamente.

Mesmo assim, reforços como estes podem não ser suficientes. Em 15 de dezembro de 2022, a SPTrans, responsável pelo sistema de transporte público de São Paulo, confirmou um ciberataque que resultou no vazamento de dados pessoais de 13 milhões de usuários do Bilhete Único. As informações expostas incluíam: nome social, data de nascimento, Cadastro de Pessoa Física (CPF), número de RG, endereço residencial, telefone, e-mail e dados de matrícula estudantil.

Após a confirmação do incidente, a SPTrans adotou algumas medidas em conformidade com a Lei Geral de Proteção de Dados (LGPD), como notificar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados afetados, assim como a divulgação do ocorrido em suas redes sociais e canais oficiais, informando que as companhia estava reforçando as principais medidas de segurança nos sistemas do Bilhete Único. Em adição, a Delegacia de Crimes Cibernéticos (DCCIBER) da Polícia Civil de São Paulo foi acionada para investigar a origem e autoria do ataque (CYBER NEWS, 2022).

Assim, apesar do aplicativo KIM investir em sua segurança digital, o ocorrido na SPTrans nos demonstra que nenhum sistema é 100% à prova de falhas. Se um incidente semelhante atingisse o KIM, milhares de pessoas poderiam ser afetadas, com múltiplas

consequências. Assim como a SPTrans fez, tomar ações ágeis e transparentes não apenas minimizam danos, como preservam a confiança dos clientes, mostrando que a empresa prioriza a proteção de dados como um dever ético, e não apenas legal, transformando crises em oportunidades para demonstrar integridade profissional e social.

2 Conformidade com os Princípios Éticos da ACM

Após análise, a Política de Privacidade do sistema demonstrou estar alinhada com os princípios éticos fundamentais estabelecidos pelo Código de Ética da ACM, principalmente em relação a aspectos que envolvam a proteção de dados pessoais, a transparência nas práticas de segurança e o compromisso com o bem-estar dos usuários (SILVA, s.d).

Um dos pontos mais destacados é a preocupação com a privacidade e a confiabilidade dos dados, que correspondem aos princípios fundamentais 1.7 – Respeitar a privacidade de outros e 1.8 – Honrar a confidencialidade. O KIM adota medidas como a realização periódica de testes de segurança, controles de acesso e armazenamento mínimo de informações, garantindo que os dados dos usuários sejam protegidos contra acessos não autorizados (KIM, 2025), em paralelo a diretrizes da ACM que enfatizam a proteção da privacidade e integridade dos dados (SILVA, s.d).

O princípio 1.2 – Evitar prejudicar outros, é refletido em algumas práticas de segurança implementadas no aplicativo, como mecanismos de rastreabilidade e proteção contra softwares maliciosos (KIM, 2025). Tais medidas visam minimizar riscos que possam afetar negativamente os usuários (SILVA, s.d), alinhadas ao compromisso ético de prevenir danos causados por sistemas computacionais.

Ainda alinhado ao princípio 1.2, os usuários são incentivados a adotarem comportamentos seguros e a reportarem eventuais violações (KIM, 2025), promovendo uma cultura de responsabilidade compartilhada.

A transparência e a honestidade (princípio 1.3 do código) também são evidenciados na política do KIM. Citações como, “Caso sejam feitas alterações relevantes que necessitem de um novo consentimento seu, publicaremos essa atualização e solicitaremos um novo consentimento para você”, de Política de Privacidade do aplicativo KIM (2025), evidenciam o compromisso e preocupação da empresa em comunicar mudanças de forma clara e obter consentimento, refletindo o princípio da ACM que valoriza a confiança e a integridade nas relações profissionais (SILVA, s.d).

Alguns princípios do código não são explicitamente abordados na documentação. 1.4 – Ser imparcial e realizar ações sem discriminação (onde discriminações na base de qualquer característica social como raça, sexo, religião, idade, invalidez ou origem não são toleradas (SILVA, s.d) e princípios voltados a propriedade intelectual (como 1.5 – Honrar direitos de propriedade incluido copyrights e patentes e 1.6 – Conceder créditos apropriados para propriedades intelectuais) não foram mencionados.

Especialmente em uma era onde onde vieses em algoritmos, tratamento desigual de dados e grandes volumes de dados disponíveis ao público (Big data) são preocupações reais, abordar apenas a proteção genérica de dados e não mencionar fatores sociais e direitos apoiados por leis como a LGPD (Lei Geral de Proteção de Dados Pessoais), deixa uma brecha e enfraquece o alinhamento com os princípios éticos da ACM.

3 Impactos Éticos de Falhas no Sistema

Ainda sobre o caso do ataque cibernético a SPTrans, o vazamento de dados de 13 milhões de usuários do Bilhete Único expôs informações sensíveis, violando o princípio 1.7 da ACM, que exige a proteção da privacidade de todos os indivíduos.

O acontecimento serve como estudo de caso não só pela grandiosidade do ataque, mas para reflexão de como possíveis danos causados aos usuários seriam significativos (incluindo desde fraudes financeiras até ameaças à segurança pessoal), demonstrando como falhas técnicas podem ter consequências concretas na vida dos usuários.

No aplicativo KIM, um vazamento similar poderia comprometer dados igualmente sensíveis, como históricos de transações financeiras ou padrões de mobilidade dos usuários. Justamente o princípio 1.4 da ACM, não abordado na Política de Privacidade do KIM (2025), que trata da não discriminação, ganha relevância nessa discussão. Sistemas que coletam dados de mobilidade podem potencialmente ser usados para práticas discriminatórias, como a exclusão de determinados grupos sociais de benefícios ou serviços com base em seus dados cadastrais e padrões de deslocamento (SILVA, s.d). A questão da honra a confidencialidade (princípio 1.8 da ACM) também foi gravemente afetada no incidente em São Paulo. Criminosos poderiam utilizar os históricos de viagem vazados para mapear rotinas de usuários, expondo detalhes íntimos de suas vidas. Esse tipo de abuso seria igualmente preocupante no caso do KIM, especialmente porque o aplicativo pode armazenar dados sobre hábitos de consumo ou informações sensíveis vinculadas a serviços complementares.

Embora o KIM destaque algumas práticas de segurança em sua Política de Privacidade – como criptografia de dados pessoais e de conteúdo de transações, prevenção e detecção de intrusão e acessos não autorizados, prevenção de vazamento de informações, realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra softwares maliciosos, mecanismos de rastreabilidade, entre outros – , o caso da SPTrans ainda serve como um alerta para a importância de ir além. O vazamento ocorreu justamente em um sistema que também afirmava possuir "controles rígidos", mas falhou em garantir a segurança de APIs terceirizadas em uma metrópole que, apenas em outubro de 2024, registrou 194,9 milhões de viagens de ônibus municipais (METRÓPOLES, 2024).

4 Ética no Gerenciamento de Riscos

Geralmente a terceirização de serviços representa um desafio significativo no gerenciamento de riscos de uma empresa, especialmente quando envolve o compartilhamento de dados pessoais. Dados coletados pelo KIM no Brasil podem ser transferidos para os EUA quando a empresa responsável pela hospedagem estiver localizada em território americano. Entretanto, essa transferência só ocorrerá após a garantia de que o país de destino oferece um nível adequado de proteção de dados, conforme exigido pela Política de Privacidade da empresa.

A política também menciona que, em transações realizadas com terceiros, a responsabilidade pela proteção dos dados recai sobre o provedor do serviço. No entanto, isso não isenta a empresa de sua obrigação ética de garantir que esses parceiros adotem padrões

de segurança rigorosos. Um exemplo de ação antiética seria a empresa fechar parcerias com terceiros sem realizar auditorias ou exigir conformidade com normas de segurança, como a LGPD. Por exemplo, se um site parceiro sofrer um vazamento de dados, a empresa original (a KIM) poderia ser considerada cúmplice por negligência.

Além disso, omitir dos usuários que seus dados serão compartilhados ou transferidos, violaria princípios éticos como transparência e consentimento informado. Uma prática questionável seria a empresa transferir dados para terceiros em países com leis de proteção mais frágeis (como é o exemplo dos EUA), expondo os usuários a riscos maiores sem seu conhecimento.

Por exemplo, se o provedor de hospedagem nos EUA estiver sujeito a leis como a Lei de Esclarecimento do Uso Legítimo de Dados no Exterior (ou CLOUD Act), que oferece mecanismos para que autoridades americanas solicitem dados armazenados no país (AWS, 2025), os usuários brasileiros poderiam ter sua privacidade comprometida.

Conclusão

A partir desta análise, conclui-se que, em geral, a empresa adotou medidas alinhadas com princípios fundamentais de proteção de dados, como privacidade, confidencialidade e transparência. No entanto, alguns desafios persistem e devem ser analisados e mitigados com responsabilidade profissional, social e ética.

Referências

AMAZON WEB SERVICES. *Lei CLOUD (Clarifying Lawful Overseas Use of Data Act)*. Disponível em: https://aws.amazon.com/pt/compliance/cloud-act/#:~:text=A%20Lei%20CLOUD%20%C3%A9%20uma,interesses%20nacionais%20de%20outros%20pa%C3%ADses. Acesso em: 7 abr. 2025.

CYBER NEWS. *Cybersecurity and Data Protection: Legal Framework and Best Practices*, [s.d]. Disponível em: https://tozzinifreire.com.br/site/conteudo/uploads/cn-24en-(2)-63d41c1a6d87f-63dbee5a00748.pdf. Acesso em: 7 abr. 2025.

ESTADÃO EXPRESSO. *Ataque hacker ao Bilhete Único expõe dados de 13 milhões de pessoas*. 2022. Disponível em: https://expresso.estadao.com.br/naperifa/ataque-hacker-ao-bilhete-unico-expoe-dados-13-milhoes-de-pessoas/. Acesso em: 7 abr. 2025.

KIM. *Política de Privacidade*. Disponível em: https://usekim.com.br/politica-de-privacidade/. Acesso em: 7 abr. 2025.

KIM. *Novo App KIM 2.0*. Disponível em: https://usekim.com.br/novo-app-kim-2-0/. Acesso em: 7 abr. 2025.

METRÓPOLES. *Recorde de passageiros e frota em queda lotam ônibus em São Paulo*. 2024. Disponível em: https://www.metropoles.com/sao-paulo/recorde-de-passageiros-e-frota-em-queda-lotam-onibus-em-sao-paulo. Acesso em: 7 abr. 2025.

SILVA, Flávio de Oliveira. *Código de Ética e Conduta Profissional em Computação*. Faculdade de Computação - UFU, [s.d.]. Disponível em: https://www.facom.ufu.br/~flavio/psi/files/02-PSI-Codigo-Etica-ACM.pdf. Acesso em: 7 abr. 2025.