pix
powered by Banco Central

Tudo o que você precisa saber sobre pagamentos instantâneos e como implementar um Pix seguro

INCOGNIA™

Sumário executivo

Os pagamentos em tempo real - ou pagamentos instantâneos - estão em ascensão no mundo inteiro, e o Pix é a versão brasileira deste arranjo de pagamento já popular pelo mundo. Os pagamentos e e-commerce mobile são as forças motriz por trás desse crescimento, também acelerado pela Covid-19. De acordo com uma pesquisa da Pew Trust, em 2019, 56% dos entrevistados usavam o celular como forma de pagamento[1]. Em outro estudo da Mastercard 70% das pessoas dizem que irão mudar seu meio de pagamento para pagamentos digitais permanentemente, o que sugere que este tipo de pagamento está aumentando rapidamente[2].

A pandemia da Covid-19 fechou lojas físicas durante meses e isso obrigou varejistas e consumidores a mudarem seus hábitos. A quantidade de aberturas de e-commerce quintuplicou durante este período. Segundo a ABComm, até a segunda quinzena de março, mensalmente eram registrados 10 mil pedidos de abertura de e-commerce, esse número saltou para mais de 50 mil por mês de abril a maio deste ano[3]. Os consumidores também estão comprando mais no e-commerce. Enquanto o crescimento do faturamento do comércio eletrônico em 2019 foi de 22,7%, a projeção para 2020 é de impressionantes 38%, de acordo com eBit Nielsen[4].

Mas o que são pagamentos instantâneos?

Os principais atributos dos pagamentos instantâneos são disponibilidade e rapidez. Na maioria dos 18 países com este tipo de arranjo de pagamento o funcionamento é durante 24 horas por dia, 7 dias por semana, 365 dias por ano, e após um pagamento, os fundos geralmente estão disponíveis quase em tempo real. Outra característica dos pagamentos instantâneos é que o débito e os créditos são irrevogáveis, portanto, uma vez que um pagamento é feito, não há como voltar atrás. O celular é outro componente dos pagamentos instantâneos, já que com uma simples impressão de um QR Codes do lado dos comerciantes e um smartphone na mão dos usuários, a troca monetária fica a apenas alguns segundos de distância.

Todas essas qualidades são algumas das razões pelas quais os consumidores estão escolhendo adotar pagamentos instantâneos em todo o mundo, com profundos impactos econômicos e sociais.

1 Pew Report, Are Americans Embracing Mobile Payments, (Outubro de 2019)

2 Mastercard

3 Abcomm, Comércio Eletrônico ganha uma Loja Virtual por minuto no Brasil, (Junho de 2020)

4 eBit Nielsen, Vendas do e-commerce devem crescer 27% na Black Friday, (Outubro de 2020)

Por isso o Pix também pode se tornar muito popular no Brasil, a ponto de substituir totalmente o dinheiro em espécie. No entanto, o Brasil é um país fértil para os fraudadores. Hoje em dia, a maioria das fraudes de pagamento são restritas ao horário comercial, já que uma série de tipos de pagamentos não são compensados durante a madrugada ou aos finais de semana, e o Pix está prestes a quebrar essa regra e dar aos fraudadores mais do que o dobro do tempo para trabalhar.

O Banco Central do Brasil já deixou claro que as instituições processadoras de pagamento serão as responsáveis por garantir a segurança dos clientes. Com esse novo sistema de pagamento no país, no qual já existem mais de 50 milhões de chaves Pix registradas pela população, as instituições terão que usar novos métodos para autenticar pagamentos e identificar usuários confiáveis, de modo que uma boa experiência seja fornecida aos consumidores e o Pix se torne um sucesso.

Pagamentos instantâneos pelo mundo

Embora os pagamentos instantâneos sejam um tópico muito falado ultimamente, não é algo novo, já que o Japão foi o primeiro a oferecer pagamentos instantâneos com Zengin em 1973. Entretanto, somente nos últimos 10 anos a inovação atendeu às necessidades das pessoas e ao bom terreno tecnológico para que os pagamentos instantâneos prosperassem.

Alguns países estão adotando pagamentos instantâneos atualmente, mas para outros, já é uma realidade popular. Em 2008, o Reino Unido introduziu o Faster Payment Services, seguido pela China e Índia, que lançaram seus próprios sistemas em 2010. Um relatório da FIS (Fidelity National Information Services, Inc.) classificou a Índia como líder global em usabilidade do sistema de pagamento instantâneo.

Para se ter uma ideia, o Unified Payments Interface (UPI) contabilizou 1,22 bilhão de transações[5] em um único mês, em novembro de 2019, além de movimentar anualmente um valor que corresponde a 19% do PIB da Índia[6].

5 Financial Express, How far UPI can reach in India: After 1 billion transactions, this is next, (Dezembro de 2019)

6 Tech Crunch, Mobile payments firms in India are now scrambling to make money, (Abril de 2020)

A implementação do UPI resultou em uma maior democratização de pagamentos no país, facilitando os processos de transferência e reduzindo o número de desbancarizados. No entanto, o sucesso dos pagamentos instantâneos na Índia não ocorreu de forma tão imediata. O primeiro sistema lançado no país foi o IMPS (Immediate Payments Service), em 2010, mas teve baixa popularidade devido à complexidade e limitação do serviço. Foi apenas com a chegada do UPI em 2016 que a modalidade apresentou um crescimento exponencial.

A Austrália lançou o NPP em 2018, com 90 instituições financeiras no arranjo de pagamento, que foi projetado, principalmente, para pagamentos no varejo. O Swish, sistema de pagamento mobile instantâneo na Suécia, também é altamente adotado, por dois terços da população do país[7]. Nos Estados Unidos, o FedNow, ainda pouco conhecido, ainda é um plano para o futuro, mas colocará o país no mapa global de pagamentos em tempo real.

Em outros países, a baixa adesão pode ser explicada pelo fato de o sistema ter sido implementado apenas como opção, o que resultou em um número reduzido de bancos participando do programa. De acordo com um relatório de 2015 da SWIFT, rede internacional de pagamentos, uma série de fatores pode influenciar a adoção dessa modalidade[8]. Em geral, o estudo concluiu que a adoção ocorre de forma rápida quando é capitaneada por reguladores - como é o caso do Bacen liderando o Pix no Brasil - em locais em que os bancos se comprometem com a iniciativa, e quando as pessoas conseguem perceber que existe algum tipo de benefício.

Impactos econômicos e sociais dos pagamentos instantâneos

Redução da circulação de dinheiro em espécie e evasão fiscal

Atualmente, o Brasil tem cerca de 45 milhões de pessoas sem conta bancária. Este alto número de cidadãos desbancarizados recentemente representou um grande desafio no recebimento do auxílio emergencial do governo, relacionado à Covid-19[9]. Em situações como a pandemia da Covid-19, o dinheiro em papel oferece um risco maior de contaminação pelo contato com várias pessoas e pelo fato de que o vírus causador do Covid-19 é capaz de sobreviver por 28 dias em

7 NS Banking, What is Swish? The mobile payments system used by more than two-thirds of Swedes, (Julho de 2019)

8 SWIFT, The Global Adoption of Real-Time Retail Payments Systems (RT-RPS), (Setembro de 2018)

9 Instituto Locomotiva, Brasil tem 45 milhões de desbancarizados, (Agosto de 2018)

notas de dinheiro[10]. Com o Pix, as pessoas poderiam, além de fazer pagamentos no comércio, receber assistência do governo através de seus próprios telefones celulares em questão de segundos.

Ao redor do mundo, o conceito de "cashless society" (uma sociedade sem dinheiro em espécie) já tem se tornado tendência. O número de transações sem dinheiro em 2013 foi de 357,8 bilhões em todo o mundo; em 2018, esse número aumentou para 620,8 bilhões[11].
Na Suécia, as cédulas representam apenas 2% da economia[12], e a expectativa é que elas tornem-se totalmente obsoletas no país até 2023[13]. Mas, enquanto a o número médio de pagamentos sem dinheiro por pessoa na Suécia é de 529, essa taxa cai para 166 no Brasil.

Na Europa, o Reino Unido é o que lidera o ranking de transações sem dinheiro em espécie[14]. Ainda assim, há muitas discussões sobre o que isso significa para cerca de 1,2 milhão de desbancarizados do país. Durante a pandemia de Covid-19, muitos estabelecimentos passaram a recusar o pagamento com cédulas e moedas, o que intensificou a polêmica sobre o quão inclusiva seria uma sociedade apenas com pagamentos digitais[15].

Além das vantagens para a população, o sistema de pagamentos instantâneos como o Pix oferece benefícios para a economia do país. A redução da circulação de dinheiro em espécie ajuda a formalizar a economia. Diversos estudos associam o uso de dinheiro físico a uma maior taxa de evasão fiscal, enquanto os pagamentos eletrônicos são associados a uma redução nessa taxa devido à maior transparência que eles oferecem na economia informal.

Utilizando um método de simulação, um estudo descobriu que quando a participação do dinheiro físico na economia cai em 10%, há uma redução de 2% na economia subterrânea[16]. Caso o dinheiro físico deixasse de existir completamente, a queda seria de 20%.

10 Virology Journal, The effect of temperature on persistence of SARS-CoV-2 on common surfaces, (Outubro de 2020)

11 Statista, Number of cashless transactions worldwide 2013-2018, (Outubro de 2020)

12 Committee on Payments and Market Infrastructures, Statistics on payment, clearing and settlement systems in the CPMI countries, (Setembro de 2015)

13 Swissquote, The evolution of currency, (Junho de 2020)

14 Visual Capitalist, The Shift to a Cashless Society is Snowballing, (Maio de 2016)

15 The Guardian, 'You can't pay cash here': how our newly cashless society harms the most vulnerable, (Junho de 2020)

O Sinprofaz estima que, só em 2020 de 01 de janeiro até o momento da produção deste texto, já foram sonegados mais de 500 bilhões de reais[16]. A redução da sonegação colaboraria com o ajuste fiscal e o combate à corrupção.

Talvez um dos exemplos mais próximos do Pix seja o sistema de pagamento instantâneo criado pelo governo da Tailândia. Lançado em 2015, o PromptPay permite que as transferências sejam feitas pelo celular utilizando uma série de identificadores, como número do documento, endereço de e-mail e número de telefone. O serviço já conta com 36,2 milhões de usuários, mais de 92% da população economicamente ativa do país, sendo que 23,5 milhões registraram o número do documento de identidade, resultando em uma maior transparência nas transações financeiras, principalmente para os setores da economia informal[17].

Crescimento do mercado de trabalho e da Gig Economy

Após entrevistar 68 profissionais e donos de pequenas e médias empresas, de diferentes setores e países, a Deloitte descobriu que 63% dos entrevistados mantém uma reserva financeira apenas para cobrir o tempo necessário para receber pagamentos[18]. Uma das conclusões do estudo, portanto, é que essa limitação financeira acaba afetando a capacidade das empresas de criar mais empregos. Segundo o relatório, o maior acesso a recursos financeiros tem um efeito ainda mais acentuado na empregabilidade em empresas de pequeno e médio porte de países em desenvolvimento.

O termo 'gig economy' se popularizou nos últimos anos e refere-se a uma economia alternativa baseada em trabalhos temporários e sob demanda. De acordo com o relatório da Deloitte, um estudo de 2018 revelou que 84% dos trabalhadores entrevistados fariam mais desses serviços se recebem o pagamento mais rápido. Na Índia, o aplicativo de táxi Ola, por exemplo, utiliza uma API do Universal Payments Interface (UPI) que permite pagamentos instantâneos para agendar viagens. A média anual de corridas realizadas pela plataforma é de cerca de 1 bilhão, tornando o Ola uma das maiores empresas do mundo no ramo de aplicativos de corrida[19].

16 Quanto custa para o Brasil, Sonegômetro, (Outubro de 2020)

17 The World Bank, Statistics about Thailand, (Junho de 2020)

18 Deloitte, Economic impact of real-time payments, (Julho de 2019)

19 Tribune India, Ola drives into UK market to capture ride-hailing market share from Uber, (Agosto de 2018)

Inclusão financeira e maior controle sobre as finanças pessoais

Os métodos de pagamento instantâneo também têm demonstrado aumentar a inclusão financeira, de acordo com a Deloitte[20]. Em países em desenvolvimento que tendem a apresentar uma alta taxa de penetração de celulares, a introdução de serviços de pagamentos móveis resultou em uma maior inclusão financeira.

Em 2006, a taxa de inclusão financeira do Quênia era de apenas 27%. Com a chegada do M-Pesa, serviço de transferência monetária mobile, esse número passou para 75% em 2016, sendo que de 2010 a 2015, a quantidade de contas registradas no M-Pesa superou o número de contas bancárias no país.

Sistemas de pagamento instantâneo, combinados com o Open Banking, podem ajudar as pessoas a controlarem melhor suas finanças pessoais. Um relatório do Banco da Inglaterra sugeriu que o Faster Payment Service, combinado com as novas regulamentações de Open Banking, poderiam facilitar o processo de compensação automática de pagamentos em contas de diferentes bancos, ajudando os consumidores a evitarem as taxas do cheque especial, reduzindo os riscos financeiros.

Assistência governamental

Na África do Sul, o uso de métodos de pagamento instantâneo resultou em economias significativas com a identificação e prevenção de recebimentos fraudulentos de auxílio monetário governamental. A Agência de Serviços Sociais da África do Sul (SASSA) começou a distribuir o pagamento de benefícios para comunidades carentes, pessoas com deficiência física e aposentados por meio de soluções digitais em 2012. Os benefícios eram creditados em cartões de débito MasterCard da SASSA após a validação biométrica dos cidadãos, evitando que eles viajassem longas distâncias para receber o dinheiro. Ao requisitar a renovação do registro para o recebimento dos benefícios sociais, o

20 Deloitte, Economic impact of real-time payments, (Julho de 2019)

governo sul-africano cancelou 850 mil transações devido a coletas ilegais ou duplicadas que o sistema conseguiu identificar.

Isso resultou em uma economia de mais de US$ 200 milhões entre 2013 e 2014[21].

Redução de outros métodos de pagamento e transferência de dinheiro

O boleto é a forma de pagamento preferida para 75% dos brasileiros[22]. Mas é alarmante para o comércio eletrônico que mais de 50% dos boletos não sejam pagos[23]. O fato de que um boleto custa entre R$3 e R$5 para ser emitido e o Pix é praticamente gratuito, faz do novo método de pagamento uma forma mais interessante para os varejistas receberem pagamentos. O bom cliente também pode ganhar com esta mudança. Quando pagarem com Pix, não haverá espera do período de compensação do boleto para que a mercadoria deixe o estoque para ir até a casa do cliente. O varejo, que terá um custo para receber pagamentos via Pix muito menor do que para a emissão de uma conta, poderá até mesmo oferecer descontos ou cashback para o consumidor. O único perdedor na história será realmente o boleto.

Os pagamentos com cartão de débito também devem diminuir. Quando os clientes pagam com cartões de débito, eles já devem ter dinheiro em sua conta, portanto, para os clientes, pagar com cartões de débito ou Pix deve ser pouco diferente. Por outro lado, os comerciantes que recebem pagamentos com cartões de débito não só têm que pagar uma taxa de 1,5% da transação, mas também recebem o pagamento em até dois dias úteis. As empresas também podem oferecer benefícios para os clientes pagarem com Pix em vez de cartões de débito, acelerando a tendência de mudança do método de pagamento.

O Pix também pode mudar a forma como as pessoas fazem transferências bancárias. Com a possibilidade de fazer transferências mais rapidamente e sem custo para a pessoa física, estima-se que bancos e empresas de processamento de pagamentos e máquinas de cartões perderão uma receita de cerca de R$19 bilhões por ano[24]. Este valor corresponde à cobrança de taxas de transferência TED e DOC, uso de terminais de auto-atendimento, taxas de transação de cartões e taxas para gerar boletos de pagamento.

21 Deloitte, Economic impact of real-time payments, (Julho de 2019)

22 E-commerce Brasil e Sebrae, Pesquisa Nacional de Varejo Online (Junho de 2018)

23 Neoatlas, E-commerce Radar, (Julho de 2018)

24 Veja, Como o PIX promete mudar a relação do brasileiro com transações digitais (Setembro de 2020)

Os desafios de segurança e riscos do Pix

De acordo com uma pesquisa realizada pela consultoria Bain & Company, cerca de 63% dos brasileiros afirmam ter interesse em utilizar o Pix futuramente ou já terem cadastrado alguma chave[25]. No entanto, desse total, apenas 24% conhece o novo sistema, enquanto 38% admite não saber do que se trata. Dentre os que não demonstram interesse em aderir à novidade, o receio em relação à segurança do sistema está entre as principais razões citadas pelos entrevistados (18%). Os números revelam que existe uma falta de informação mesmo entre os interessados, o que pode levar muitos consumidores a não utilizarem o sistema a princípio, mesmo com as chaves registradas, porque não sabem como ele funciona e por medo de sofrer algum tipo de fraude.

Após analisar sistemas de pagamentos instantâneos em diferentes países da Europa, um relatório da Deloitte listou quatro principais desafios para que as provedoras do serviço viabilizem transferências em um espaço de tempo tão curto: baixa latência, disponibilidade, gestão de liquidez e prevenção a fraudes[26]. Entre os desafios citados, o mais sensível de todos diz respeito à fraude. Se com outros métodos os pagamentos podiam levar até dias para serem processados, com pagamentos imediatos, as instituições têm que reduzir o período de processamento e transferência de dinheiro para apenas alguns segundos.

Isto significa que as instituições também precisam realizar uma análise de risco complexa em tempo recorde para liberar o dinheiro para o destinatário.

Existem três técnicas principais de fraude que podem ser relevantes no contexto do Pix:

Phishing com QR Code

QR Code fraudulento

Engenharia social para o roubo de conta

25 Bain & Company, (Outubro de 2020)

26 Deloitte, Instant Payments - Overcoming challenges to win the race against time (2018)

1. Phishing com QR Code

Até julho deste ano, por exemplo, já haviam sido detectados 10 milhões de ataques de phishing bancário[27]. Um levantamento realizado pela Kaspersky Lab ainda revelou que o Brasil é o país com maior número de vítimas de ataques de phishing no mundo[28]. De fato, antes mesmo de o Pix estrear no Brasil, muitas pessoas já estavam recebendo e-mails falsos para o cadastro das chaves. Portanto, um dos grandes desafios da Pix será a educação da sociedade para o uso da nova solução; seja do lado dos consumidores, que devem estar mais atentos a possíveis esquemas, ou das empresas, que precisam estar preparadas para garantir a segurança e a privacidade dos clientes.

Ainda de acordo com a Kapersky, o Brasil é o quinto país com maior número de vítimas de ataques de phishing[29]. De abril a junho deste ano, cerca de 13% dos internautas brasileiros acessaram um link que direcionava para páginas maliciosas, sendo que a média mundial foi de 8,26% no mesmo período. O phishing com QR Code poderá acontecer por diversas plataformas, como Whatsapp, SMS ou email. Esta é uma das principais formas para os fraudadores tirarem proveito deste novo método de pagamento.

2. QR Code fraudulento

Uma técnica comum envolve QR codes que podem ser enviados por um fraudador se passando por um conhecido, pedindo um pagamento Pix via escaneamento do código. Em alguns casos, os criminosos ainda substituem o QR code por um código falso, direcionando os usuários para páginas que se parecem com a original, mas que são utilizadas para levar os visitantes a baixarem malwares ou fornecerem suas informações pessoais. Em março deste ano, o MPDFT (Ministério Público do Distrito Federal e Territórios) denunciou uma quadrilha que roubava dados bancários de clientes por meio de QR Codes, resultando em um prejuízo de R$ 1,1 milhão apenas no Distrito Federal[30].

27 PSafe (Julho de 2020)

28 Kaspersky, Os sete maiores golpes online de 2018 (Dezembro de 2018)

29 Kaspersky, Golpes relacionados ao Pix já circulam pela internet, (Setembro de 2020)

30 Tecnoblog, Grupo faz roubo milionário usando senhas e QR Code de banco (Março de 2020)

Roubos com QR Codes fraudulentos já começaram a acontecer durante a quarentena. Por exemplo, golpistas se aproveitam da popularidade das lives realizadas por artistas para desviar dinheiro de doações[31]. Os criminosos transmitiam vídeos das apresentações de cantores sertanejos, substituindo o QR Code utilizado para arrecadar doações por um código adulterado que direcionava o dinheiro para a conta do fraudador.

Em outros países, onde o pagamento com QR Code já é mais comum, os golpes podem tomar outra proporção. Na Holanda, QR Codes foram colados em máquinas para o pagamento de estacionamentos, com um aviso de que as máquinas não estavam aceitando dinheiro[32]. Os indivíduos simplesmente, ao escanear o QR Code, transferiram a quantia para a conta do fraudador, e deixaram de pagar seu estacionamento.

3. Engenharia social para o roubo de conta

Em junho de 2019, uma reportagem da NBC News revelou que diversos usuários haviam sido roubados por meio do serviço de pagamento digital Zelle[33]. Assim como muitos sistemas similares, o Zelle permite enviar dinheiro para outras pessoas dentro de segundos utilizando apenas um endereço de e-mail ou número de telefone. Uma das vítimas relatou que havia recebido uma suposta ligação do seu banco pedindo que ela informasse o código enviado por SMS para que eles pudessem verificar a sua identidade. Com o código em mãos, os fraudadores puderam criar uma conta no Zelle no nome da vítima e ter acesso às suas contas bancárias.

Casos de engenharia social como esses são alguns dos golpes mais comuns. No Reino Unido, um tipo de fraude conhecido é o envio de um boleto emitido por uma suposta instituição ou serviço.

31 The Hack, “Lives falsas” são o golpe na moda e já fazem vítimas no Brasil (Junho de 2020)

32 Flashpoint, Emerging Trends in QR Code Fraud (Março de 2020)

33 NBC News, Instant fraud: Consumers see funds disappear in Zelle account scam (Junho de 2019)

Com os sistemas de pagamento instantâneos, o processo de transferência ocorre de forma muito rápida, muitas vezes antes de o esquema ser identificado como fraude e a transferência instantânea tem caráter irrevogável.

Nestes casos, o dinheiro só será recuperado se a instituição envolvida no pagamento ressarcir o cliente, algo difícil de acontecer em casos que fique provado que o usuário passou dados para fraudadores.

Com a chegada do Pix, é de se esperar que golpes similares sejam comuns, da mesma forma que ocorre com sistemas de pagamentos instantâneos de outros países. Apesar de o Banco Central afirmar que as transações via Pix poderão ser reembolsadas caso haja comprovação de fraude, o processo pode ser demorado, exaustivo e nem sempre garantido. Além disso, as instituições que apresentarem altos índices de irregularidade, poderão ser multadas e até mesmo impedidas de continuar a oferecer o serviço.

É esperado que técnicas de engenharia social sejam cada vez mais comuns quando o PIX começar a funcionar em novembro, assim como o phishing, já comentado. Ambas as técnicas, assim como outras, como o SIM Swap, poderão ser usadas para roubar as contas de usuários participantes do Pix. Um indivíduo com a conta roubada poderá ter problemas graves, já que, diferente de transferências ou compras que levam horas ou até dias para serem aprovadas, no Pix, os fundos serão transferidos instantaneamente. Se ficar provado que o usuário passou seus próprios dados ou clicou em algo que não deveria, será quase impossível recuperar o valor furtado.

Os riscos não são novos, mas o fato de um pagamento Pix fazer uma transferência de dinheiro irrevogável em apenas 10 segundos apresenta o maior desafio para as instituições financeiras, que é a prevenção de fraudes em tempo recorde.

Equilíbrio entre a prevenção de fraudes e uma boa experiência do usuário

O sistema de prevenção de fraudes mais seguro do mundo, com tolerância zero para fraudes, é aquele em que os bons usuários são tão seguros que nem mesmo eles são capazes de fazer uma transação. Para a sorte dos consumidores e a sobrevivência das instituições, tal sistema não existe. No sistema ideal, há um equilíbrio perfeito entre falsos negativos, fraudadores não identificados pelas ferramentas anti-fraude, e falsos positivos, os bons usuários erroneamente identificados como fraudadores que são impedidos de fazer uma transação. O foco das empresas precisa estar na identificação dos bons usuários e deixá-los passar facilmente sem fricção.

O foco das empresas precisa estar na identificação dos bons usuários e deixá-los passar facilmente sem fricção.

Os modelos tradicionais de detecção de fraude buscam pelos fraudadores, e com isso, muitos bons usuários são travados e pagam o preço. Dados preocupantes do MIT mostram que para cada fraude detectada, 5 transações legítimas são barradas[34]. Estes usuários buscarão alternativas que dêem preferência para sua boa experiência, em aplicativos de pagamentos que não os tratem como criminosos.

Finalmente, a segurança, um fator essencial, porém o maior causador de fricção para os usuários legítimos. A fricção vem do fato do usuário ter que comprovar sua identidade no cadastro, e continuar se autenticando ao longo do uso. Por que os usuários legítimos, para não passarem por grandes inconvenientes como terem suas contas roubadas e valores saqueados, deveriam ter uma experiência ruim ao abrir uma conta e ao usar um app mobile?

Os fraudadores fazem milhões de pessoas idôneas terem que pagar o preço, provando constantemente que são elas mesmas. Um estudo mostra que hoje no Brasil, mesmo aplicativos de bancos digitais ou contas digitais de bancos tradicionais, fazem com que usuários legítimos passem por cerca de 33 telas em 11 minutos para abrir uma conta[35]. Este processo inclui várias etapas para provar a identidade reivindicada pelo usuário, desde a solicitação de documentos como comprovante de residência, até a coleta de impressões digitais, selfie e tokens SMS a serem copiados para o aplicativo. Não é de se admirar, de acordo com o mesmo estudo, apenas 2,4 de cada 10 usuários realmente ativam a conta do aplicativo que baixaram.

34 MIT, Reducing false positives in credit card fraud detection (Setembro de 2018)

35 idwall, Análise de mercado (Agosto de 2020)

Pix precisa funcionar 24/7/365, e um pagamento deve ser realizado em segundos. Usuários já se acostumaram com isso, dado que o mobile quebrou a dicotomia entre estar ou não online. O mobile garante que qualquer um possa fazer qualquer coisa a qualquer hora, desde pedir sua comida preferida até comprar uma roupa. A gratificação instantânea também se tornou comum: A maioria dos usuários não espera para páginas de site carregarem, não espera por produtos não disponíveis, eles simplesmente vão para o próximo site e o próximo app de e-commerce. Com a inauguração do Pix isso se estende a pagamentos e transferências financeiras.

No entanto, para que as expectativas de alta disponibilidade e velocidade sejam atendidas, existem pré-condições importantes. Uma série de soluções precisam estar presentes na arquitetura do app dos participantes diretos ou indiretos para prover o pagamento instantâneo. Uma delas é a solução que autentica a identidade do usuário no momento da transferência de valores. Em um sistema instantâneo, é algo que precisará acontecer automaticamente, e sem intervenção humana, do contrário o pagamento não será efetuado em segundos. Os apps que não utilizarem soluções de autenticação de identidade automática têm grande risco de não atenderem às expectativas. Qual será a reação de usuários, acostumados a terem velocidade e disponibilidade em todos os outros serviços, que tiverem um ou dois pagamentos negados ou demorando a acontecer, e lembrarem que existem mais de 900 outros apps disponíveis para usarem o PIX? Com três cliques conseguem desinstalar o app e instalar o próximo.

Na verdade, esta facilidade e velocidade fazem com que os usuários desinstalem aplicativos muito rapidamente.

Um estudo mostra que 77% dos usuários desinstalam um aplicativo apenas três dias após a instalação[36].

Quanto maior o número de aplicativos que oferecem praticamente o mesmo serviço, é necessário se diferenciar para não ser descartado. Oferecer facilidade de uso e a melhor experiência possível é um grande diferencial.

36 Quettra, New data shows losing 80% of mobile users is normal, and why the best apps do better (2019)

Pix, privacidade e conformidade com a LGPD e compliance com normativas do Banco Central

Uma possível porta aberta para violações de privacidade

Pix está estreando em um momento em que a Lei Geral de Proteção de Dados (LGPD) já está em vigor, ao contrário de outros sistemas de pagamento instantâneo em todo o mundo.

Um caso marcante foi da agência de crédito Equifax, condenada a pagar uma multa de US$ 700 milhões devido a um vazamento de dados em 2017[37]. Na ocasião, hackers roubaram os dados de 147 milhões de pessoas, entre norte-americanos, canadenses e britânicos. Na época, a General Data Protection Regulation (GDPR) ainda não estava em vigor, por isso o Reino Unido multou a empresa em £500 mil - caso o regulamento já estivesse valendo, esse valor poderia chegar a 4% do faturamento anual da companhia. Igualmente, a Comissão de Comércio Norte America (FTC) fez um acordo com a Equifax, segundo o qual a empresa pagou $575 milhões, além de ser obrigada a reforçar seus sistemas de segurança.

Casos como o da Equifax mostram que as instituições não estavam preparadas para proteger seus clientes.

Portanto, legislações como a LGPD e a GDPR acabam forçando as empresas a investirem em sistemas de segurança e adotarem iniciativas para promover uma maior transparência com os consumidores. Um relatório da Deloitte sobre o impacto da GDPR em serviços financeiros revelou que 51% das empresas do setor afirmam ter feito algum tipo de investimento para atender às exigências da nova lei[38]. Isso inclui desde a implementação de novas tecnologias até a contratação de especialistas em segurança da informação.

O Pix está em conformidade com o LGDP e com os regulamentos financeiros, e as instituições de processamento também devem estar

Voltando ao Brasil, o cenário é um pouco diferente. Por aqui, a LGPD já está em vigor e isso significa que o Banco Central precisou levar em consideração todas as exigências da lei para criar o novo serviço de pagamentos instantâneos. De fato, especialistas afirmam[39] que o Pix cumpre não apenas a Lei Geral de Proteção de Dados Pessoais, como também a Lei Complementar n. 150/2001 (Lei do Sigilo Bancário), a Resolução do Conselho Monetário Nacional n. 4.658/2018 (Política de Segurança Cibernética), a Circular do BACEN n. 3.909/2018, a Lei do Cadastro Positivo, o Código de Defesa do Consumidor e, inclusive, o Código Penal.

37 Federal Trade Comission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (Julho de 2019)

38 Deloitte, After the dust settles - How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on (2018)

39 VocêSA, Pix irá revolucionar a relação digital dos bancos com clientes (Outubro de 2020)

Considerando o artigo 5º, I, da LGPD, os dados bancários se enquadram na classificação de dados de natureza pessoal. Portanto, todas as atividades do Pix e o controle das chaves deve respeitar a legislação e tratar os dados conforme disposto no artigo 7º, que fala sobre a base legal adequada para tratar o dado do consumidor. Assim, o novo sistema de pagamentos só poderá coletar dados dos clientes para realizar transações financeiras, visto que o acesso e uso de informações deve se limitar à finalidade consentida pelo cliente, e deve observar, dentre outras coisas, os requisitos da LGPD.

O Banco Central exige que as instituições participantes do Pix disponham de sistemas de autenticação, criptografia, prevenção e detecção de invasores e prevenção de vazamento de informações (art. 3º, §2º da Res. 4.658 do CMN).

Somado-se a isso, as instituições também estão impedidas de compartilhar qualquer dado que esteja protegido sob a Lei de Sigilo Bancário (Lcp nº 105/2001) com terceiros, como operadoras de telefone e a Receita Federal, obrigação esta que, em regra, se estende ao próprio Banco Central.

Uma experiência segura e sem fricção para os usuários do Pix, respeitando sua privacidade

De acordo com os regulamentos do Banco Central, os processadores de pagamento serão responsáveis pela validação dos dados do usuário. Mas como garantir a segurança sem comprometer a boa experiência do usuário, que tem a expectativa de um pagamento instantâneo e sem fricção?

No Pix, a primeira verificação de segurança será feita pelo Banco Central. Ao confirmar a chave do destinatário, o pagador receberá as informações referentes ao destinatário e, se houver alguma inconsistência nos dados, a operação poderá ser cancelada. Caso o cliente confirme as informações, a transação será analisada pelo processador de pagamento. Se o processador de pagamento identificar qualquer problema suspeito, a transferência poderá ser retida por até 30 minutos durante o dia, ou até uma hora durante a noite.

Considerando que os processadores de pagamento serão responsáveis por garantir a segurança das transações, o que eles devem buscar é uma forma de proteger o usuário sem comprometer sua boa experiência com o serviço. Em caso de falsos positivos, por exemplo, a retenção de dinheiro por uma hora pode causar um grande descontentamento. Em um sistema que promete ser instantâneo, será que o usuário terá paciência para esperar?

Embora haja um esforço constante para conscientizar os usuários entre empresas, instituições e serviços de segurança, há maneiras mais eficazes de evitar possíveis golpes envolvendo o Pix.

A tecnologia de biometria comportamental por localização, por exemplo, é capaz de reduzir tanto as fraudes envolvendo o roubo de conta quanto os falsos QR Codes e phishing com QR Code.

Detectando QR Codes fraudulentos

No caso de QR Codes fraudulentos, a biometria comportamental por localização é capaz de confirmar se o pagamento está ocorrendo no local onde o usuário está e se o código escaneado foi, de fato, gerado pelo estabelecimento no local onde a pessoa está no momento. Este tipo de checagem pode trazer segurança tanto para os pagadores quanto para os destinatários no sistema do Pix.

Detectando o roubo de conta

Quando uma conta é acessada através de uma aplicação mobile, por exemplo, é possível comparar a localização atual e o histórico de localização do dispositivo, para uma análise de quão comum é o comportamento para determinar se é um comportamento confiável. Se a conta está sendo acessada de um local pouco ou nunca visitado pelo usuário antes, o sistema pode enviar um alerta para a instituição para solicitar outra camada de autenticação.

Respeitando a privacidade dos usuários e em conformidade com a LGPD

Além da facilidade e segurança, uma boa experiência também inclui privacidade. Para convencer os mais céticos, os prestadores de serviços de pagamento devem buscar soluções que atendam à LGPD e sejam capazes de evitar fraudes enquanto protegem a privacidade da identidade do usuário. A biometria comportamental por localização é uma solução sem fricção que previne fraudes mobile para os usuários. Funciona em segundo plano com dados dinâmicos em tempo real, prevenindo a fraude instantânea do QR code para usuários e comerciantes do Pix. A tecnologia cria uma identidade digital baseada no comportamento de localização dos usuários, sem utilizar dados pessoais e é perfeita para o Pix, uma vez que compara local do pagamento com o histórico de localização do usuário, e o local onde o pagamento está sendo feito à localização do dispositivo.

Como Incognia protege os pagamentos do Pix

Registro da chave do Pix

01 **O cliente se registra no aplicativo**

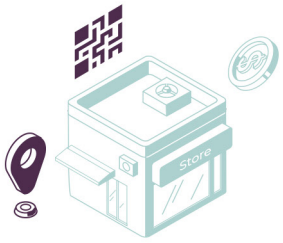
Incognia realiza uma verificação de integridade do dispositivo, verificando tentativas de falsificação de localização ou quaisquer outras anomalias, como Jailbrake ou Rooting e avalia se o usuário está em um local confiável (com base em seu histórico de comportamento). Esta verificação detecta tentativas de roubo de conta onde um fraudador tem as credenciais corretas, mas o comportamento de localização não é consistente com o usuário legítimo.

02 **O cliente introduz o registro de chave Pix no aplicativo**

Com base na pontuação de risco e na classificação de confiança desse usuário, o aplicativo pode decidir se será necessária alguma autenticação por etapas. Se o risco for baixo, o usuário pode ser autenticado sem fricção de etapas extras, como OTP por SMS ou e-mail, pois tudo será validado em segundo plano.

03 **O cliente confiável está autenticado e pronto para usar a chave para uma transação Pix.**

Pagamentos do Pix em loja com QR Code



01 **O cliente entra na loja e efetua o login no aplicativo de pagamento**

Incognia realiza uma verificação de integridade do dispositivo, verificando tentativas de falsificação de localização ou quaisquer outras anomalias, como Jailbrake ou Rooting e avalia se o usuário está em um local confiável (com base em seu histórico de comportamento). Esta verificação detecta tentativas de roubo de conta onde um fraudador tem as credenciais corretas, mas o comportamento de localização não é consistente com o usuário legítimo.

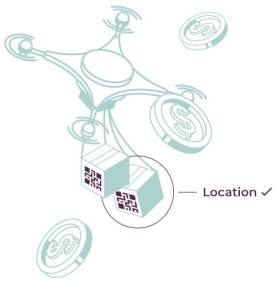
02 **O cliente escaneia o QR Code**

Incognia aprende com qual local um QR Code está associado para garantir que o código que está sendo escaneado pelo usuário seja o registrado naquele local. Isto evita a ocorrência de pagamentos não intencionais e as perdas resultantes por fraude de QR Code.

03 **O pagamento é autorizado**

Se o comportamento de localização de um usuário coincide com seu histórico de comportamento, então a Incognia fornecerá uma alta taxa de confiança, baseada nesses sinais de localização. Se qualquer anomalia de localização for detectada, nossa pontuação de risco pode então apresentar apenas para esses usuários a um novo fator de autenticação, deixando os clientes confiáveis com a melhor experiência possível e sem fricção.

QR code remoto



01

O cliente efetua login em seu aplicativo

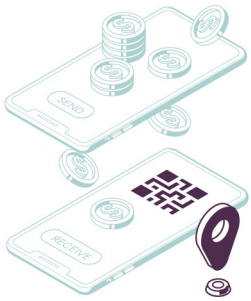
Incognia realiza uma verificação de integridade do dispositivo, verificando tentativas de falsificação de localização ou quaisquer outras anomalias, como Jailbrake ou Rooting e avalia se o usuário está em um local confiável (com base em seu histórico de comportamento). Esta verificação detecta tentativas de roubo de conta onde um fraudador tem as credenciais corretas, mas o comportamento de localização não é consistente com o usuário legítimo.

02

O cliente escaneia o QR Code e o pagamento é autorizado

Se o comportamento de localização de um usuário coincide com seu histórico de comportamento, então a Incognia fornecerá uma alta taxa de confiança, baseada nesses sinais de localização. Se qualquer anomalia de localização for detectada, nossa pontuação de risco pode então apresentar apenas para esses usuários a um novo fator de autenticação, deixando os clientes confiáveis com a melhor experiência possível e sem fricção.

P2P



01

Ambos usuários logan em seus aplicativos de pagamento

Incognia realiza uma verificação de integridade do dispositivo, verificando tentativas de falsificação de localização ou quaisquer outras anomalias, como Jailbrake ou Rooting e avalia se o usuário está em um local confiável (com base em seu histórico de comportamento). Esta verificação detecta tentativas de roubo de conta onde um fraudador tem as credenciais corretas, mas o comportamento de localização não é consistente com o usuário legítimo.

02

Usuário 1 escaneia o QR Code do usuário 2

Incognia verifica se ambos os usuários estão no mesmo local e fornece uma pontuação de risco indicando o nível de risco de qualquer tentativa de pagamento fraudulenta. Tudo isso acontece em segundo plano, sem acrescentar nenhuma fricção à experiência dos usuários.

03

O pagamento é autorizado

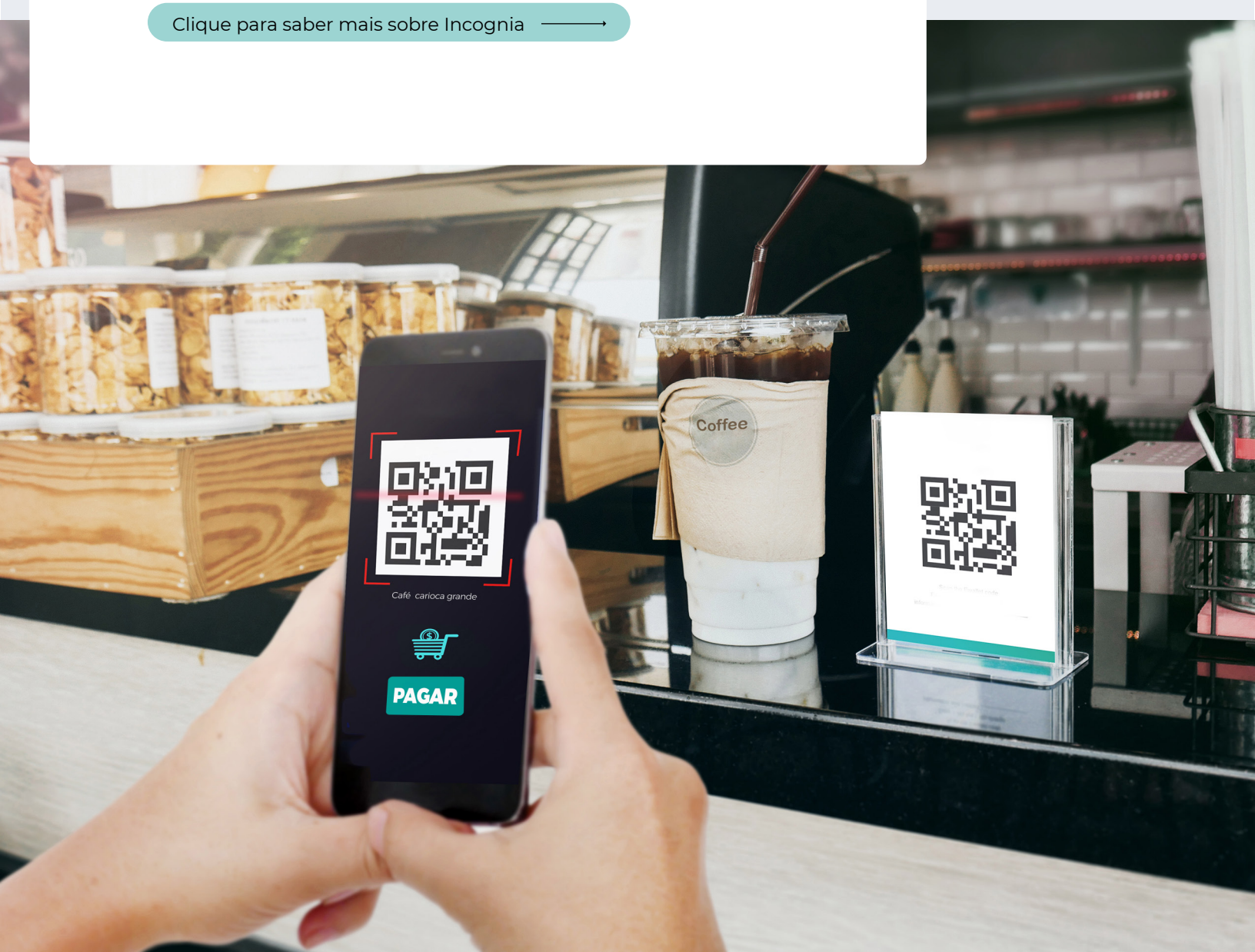
Se o comportamento de localização de um usuário coincide com seu histórico de comportamento, então a Incognia fornecerá uma alta taxa de confiança, baseada nesses sinais de localização. Se qualquer anomalia de localização for detectada, nossa pontuação de risco pode então apresentar apenas para esses usuários a um novo fator de autenticação, deixando os clientes confiáveis com a melhor experiência possível e sem fricção.

Sumário

Neste whitepaper apresentamos métodos de pagamento instantâneo, seus impactos, riscos de segurança e desafios em todo o mundo com o objetivo de tentar projetar o que o lançamento do Pix poderia significar para o Brasil. Apresentamos a importância do equilíbrio entre fraude e fricção, e também, como as empresas podem e devem estar em conformidade com a LGPD e respeitar a privacidade dos usuários, mantendo ao mesmo tempo suas transações e conta Pix seguras.

Desenvolvido como resultado de quase uma década de trabalho com tecnologia de localização mobile, Incognia oferece às empresas de serviços financeiros detecção instantânea de fraudes para evitar fraudes no Pix sem acrescentar fricção para os usuários. Incognia é uma solução de prevenção a fraudes criada para o mundo móvel.

Clique para saber mais sobre Incognia →



Sobre Inloco e Incognia

Inloco é uma empresa de identidade privada baseada na tecnologia de localização. Incognia é o produto que permite a prevenção de fraudes mobile para bancos, fintechs e e-commerces usando biometria comportamental baseada em localização, e oferece verificação e autenticação de identidade sem fricção. Temos sede em Recife e São Paulo, e nossa empresa-irmã que leva o mesmo nome do produto de prevenção à fraudes, Incognia, tem escritórios em Palo Alto e Nova Iorque. Temos atualmente mais de 60M+ de dispositivos com nossa tecnologia de localização.

Utilizamos dados comportamentais de localização para aumentar a segurança da conta de usuários, reduzir fraudes e fornecer serviços de localização privada sensíveis ao contexto. Nossa tecnologia utiliza sinais de rede e sensores no dispositivo para fornecer informações de localização altamente precisas. Ao construir um padrão de comportamento anônimo, único para cada usuário, Incognia fornece contexto de localização e cria uma identidade digital privada para a segurança das contas.

Empresas com aplicativos móveis e dispositivos conectados usam Incognia para verificação de identidade de usuários sem fricção, autenticação dinâmica adaptativa, avaliação de risco e detecção de fraude, tudo isso enquanto protegem a privacidade do usuário.

Privacidade

A privacidade do usuário é uma preocupação central da Inloco. A arquitetura de nossos produtos é feita sob os princípios do privacy by design, implementando técnicas de proteção da privacidade desde a concepção até o uso final de nossos produtos e soluções.

A tecnologia da Inloco foi projetada para impedir o acesso à informação capaz de re-identificar os usuários. Isto significa que a Inloco não coleta identificadores de dispositivos estáticos únicos (tais como IMEI e MAC), contas associadas (e-mail e telefone), dados de identificação civil (nome e CPF), bem como alguns dados sensíveis como informações que revelam etnia, religião, opinião política, religião, filosofias, entidades políticas ou sindicais ou dados sobre saúde, vida sexual, genética e biometria física.

Nosso objetivo é, após tratamento, transformar os dados de localização em uma versão ilegível dos originais, para que ainda possam ser utilizados como a prova de conhecimento zero, mas não podem ser lidos sem uma chave de criptografia, ou, em certos casos, de forma alguma. Outras técnicas que usamos incluem uma estrutura de conjunto probabilística, privacidade diferencial e k-anonimato, aproximando os dados de uma anonimização completa.

Os dados coletados pela Inloco para oferecer seus serviços vêm do dispositivo móvel através de nosso Software Development Kit (SDK). Cada aplicativo deve apresentar para seus usuários a Política de Privacidade da Inloco em seus próprios Termos e Condições de Uso e Políticas de Privacidade, informando que os dados serão coletados pela Inloco. Uma vez autorizado, nosso SDK começa a coletar os dados sem identificar os usuários. Os usuários também podem negar a coleta de dados optando por não permitir e não dando consentimento, o que desativa os recursos para eles. Além disso, cada aplicativo deve permitir que os usuários optem por não coletar os dados a qualquer momento, dando aos usuários a propriedade de seus dados.

A equipe da Inloco compreende o poder e a sensibilidade dos dados de localização e é por isso que temos um compromisso interno de ir muito além para manter a proteção da privacidade do usuário.

Peça uma demonstração: contato@incognia.com
Saiba mais: www.incognia.com/pt