O paradoxo das redes privativas: controle local, patentes globais

Brenda Albuquerque (*)

As redes privativas têm se consolidado como uma solução estratégica para setores que demandam alto desempenho, baixa latência e maior controle sobre a infraestrutura de comunicação

Baseadas, em grande parte, em tecnologias 4G LTE e 5G, essas redes permitem que empresas e organizações operem sistemas dedicados, com ganhos relevantes em segurança, confiabilidade e eficiência operacional. No entanto, apesar dessa autonomia aparente, há um elemento estrutural que limita esse controle: a dependência de padrões tecnológicos globais, fortemente protegidos por patentes essenciais (SEPs).

Esses padrões incorporam tecnologias indispensáveis ao funcionamento das redes móveis modernas, incluindo mecanismos de modulação, codificação, acesso ao meio e gerenciamento de mobilidade. Grande parte dessas soluções é protegida por portfólios de patentes pertencentes a empresas como Qualcomm, Ericsson, Nokia e Huawei, o que faz com que qualquer implementação compatível com esses padrões dependa, necessariamente, do uso dessas tecnologias patenteadas.

É nesse ponto que emerge o paradoxo: embora as redes privativas ofereçam controle local sobre a operação e a infraestrutura, elas permanecem tecnicamente vinculadas a um ecossistema global de propriedade intelectual. Na prática, isso significa que empresas que implementam redes privativas precisam negociar licenças com múltiplos titulares de SEPs, geralmente sob condições FRAND (Fair, Reasonable and Non-Discriminatory).

Esse paradoxo se torna evidente em aplicações concretas. Um exemplo relevante no Brasil foi a utilização de infraestrutura 5G na transmissão do Carnaval tanto no Rio de Janeiro quanto em São Paulo pelo Grupo Globo. Nessas operações, a Globo utilizou soluções fornecidas pela Ericsson, integradas à rede 5G da Claro, o que possibilitou a transmissão sem fio de vídeo em alta definição diretamente das câmeras para a produção, com maior mobilidade das equipes, menor dependência de cabeamento e maior eficiência operacional. Trata-se, na prática, de uma arquitetura próxima ao conceito de rede privativa ou dedicada, ainda que apoiada em infraestrutura de operadora, evidenciando o uso combinado de soluções proprietárias e padrões globais.

No entanto, toda essa operação esteve ancorada em padrões internacionais que incorporam diversas patentes essenciais, evidenciando que, mesmo em um ambiente de controle operacional ampliado e com soluções tecnológicas avançadas, a base técnica permanece dependente de tecnologias padronizadas e licenciadas globalmente.

Situações semelhantes podem ser observadas em outros setores. Na indústria, redes privativas viabilizam a automação de processos e o controle em tempo real de máquinas e robôs. Em portos e centros logísticos, permitem o rastreamento eficiente de cargas e a operação remota de equipamentos. No setor de mineração, possibilitam o controle de veículos autônomos em ambientes de risco. Em eventos de grande porte, como a Copa do Mundo FIFA, redes dedicadas são utilizadas para oferecer suporte para transmissão de dados, operações técnicas e serviços ao público. Em todos esses casos, a dependência de padrões tecnológicos globais e, consequentemente, de SEPs, é inevitável.

No Brasil, esse cenário envolve não apenas questões tecnológicas e comerciais, mas também institucionais. O Instituto Nacional da Propriedade Industrial atua na concessão de patentes relacionadas a essas tecnologias, enquanto a Agência Nacional de Telecomunicações regula o uso do espectro e a implementação de redes. A coordenação entre esses atores é essencial para garantir um ambiente que favoreça a inovação sem comprometer o acesso às tecnologias necessárias.

Portanto, o avanço das redes privativas evidencia um equilíbrio delicado entre autonomia operacional e dependência tecnológica. O paradoxo que as caracteriza não é apenas conceitual, mas prático, influenciando decisões de investimento, estratégias de inovação e políticas regulatórias. Compreender essa dinâmica é fundamental para que empresas e formuladores de políticas consigam explorar todo o potencial dessas redes, ao mesmo tempo em que lidam de forma eficiente com as implicações associadas às patentes essenciais.

(*) Especialista em Patentes do Di Blasi, Parente & Associados.

Um terço dos golpes digitais no Brasil envolve Pix

Estudo aponta o que Pix já é o principal meio utilizado por criminosos para obter recursos das vítimas; especialistas explicam como evitar fraudes e o que fazer após cair em um golpe


pixelshot_CANVA

O Pix transformou a forma como os brasileiros realizam pagamentos, transferências e compras. Mas a popularidade da ferramenta também chamou a atenção dos criminosos. Um levantamento divulgado pelo Observatório Lupa revelou que um terço dos golpes digitais aplicados no Brasil utiliza o Pix como principal meio para obtenção de dinheiro das vítimas. O estudo analisou mais de uma centena de conteúdos fraudulentos que circularam no país nos últimos dois anos e identificou que 33% dos golpes exigiam pagamentos exclusivamente via Pix. Além disso, 74% exploravam a credibilidade de empresas, marcas ou personalidades conhecidas para dar aparência de legitimidade às fraudes.

Para especialistas em segurança digital, o dado reforça uma constatação importante: o problema não está na tecnologia do Pix, mas na forma como os criminosos conseguem manipular o comportamento das vítimas. "Na prática, os criminosos exploram muito mais falhas no comportamento dos usuários do que vulnerabilidades técnicas do Pix. O sistema em si é seguro, com camadas robustas de criptografia e autenticação. O que vemos com mais frequência são golpes de engenharia social, em que a vítima é convencida a autorizar a própria transferência acreditando que está realizando uma operação legítima", explica Géssica Ribeiro, Analista Sênior de Governança de TI da Trio Grupo Financeiro e especialista em Segurança da Informação.

Segundo ela, a sofisticação dos golpes tem aumentado porque os criminosos não se limitam mais a ataques tecnológicos, passando também a explorar fatores emocionais como urgência, medo e confiança para aumentar suas chances de sucesso.

Falsos atendentes, WhatsApp clonado e QR Codes adulterados lideram fraudes

Entre os golpes mais comuns atualmente estão falsas centrais de atendimento bancário, clonagem de contas de WhatsApp, anúncios fraudulentos em plataformas de venda, QR Codes adulterados e falsas oportunidades de investimento. O padrão costuma ser semelhante: o criminoso cria uma situação de urgência ou apresenta uma oportunidade aparentemente vantajosa para convencer a vítima a transferir recursos rapidamente.

"O objetivo é fazer com que a própria pessoa realize a transação acreditando que está resolvendo um problema ou aproveitando uma oportunidade legítima. Por isso, é fundamental confirmar a identidade da pessoa ou empresa envolvida antes de qualquer pagamento", afirma Géssica Ribeiro. O próprio estudo do Observatório Lupa mostra que 71% dos golpes analisados prometiam algum tipo de benefício financeiro, como indenizações, promoções, brindes, vagas de emprego ou descontos inexistentes.

Como evitar cair em um golpe via Pix

Especialistas recomendam que os usuários adotem uma série de cuidados simples antes de confirmar qualquer transferência. A primeira medida é verificar atentamente o nome e o CPF ou CNPJ vinculados à chave Pix. Também é importante desconfiar de pedidos de dinheiro recebidos por mensagens ou ligações inesperadas, especialmente quando há pressão para que a transferência seja feita rapidamente.

"Em muitos casos, alguns segundos de atenção antes de concluir a operação são suficientes para evitar prejuízos. É importante utilizar apenas os canais oficiais das instituições financeiras, evitar clicar em links recebidos por aplicativos de mensagens e manter o celular protegido com senha, biometria e atualizações de segurança", orienta Géssica.

Outro recurso que pode aumentar significativamente a proteção é a autenticação multifator. "O uso de biometria, reconhecimento facial e autenticação em múltiplas etapas adiciona camadas extras de segurança. Mesmo que um criminoso obtenha a senha do usuário, ele ainda precisará passar por outras validações para acessar a conta", explica a especialista.

O Pix continua sendo seguro?

Apesar do crescimento das tentativas de fraude, especialistas ressaltam que o Pix continua sendo um sistema seguro. "O Pix foi desenvolvido com criptografia de ponta, autenticação mútua e tráfego exclusivo dentro da Rede do Sistema Financeiro Nacional", afirma Andressa Lipski, Diretora de Governança da Trio Grupo Financeiro.

Segundo ela, a segurança também é reforçada pela atuação constante do Banco Central. "O Banco Central exige que bancos e instituições de pagamento implementem mecanismos antifraude, limites transacionais por horário, alertas de fraude e controles rigorosos na abertura de contas. Além disso, responsabiliza instituições que não adotam medidas adequadas de prevenção", explica.

Caiu em um golpe? Ainda é possível recuperar o dinheiro

Uma das principais dúvidas de quem sofre uma fraude é se existe alguma chance de recuperar os valores transferidos. A resposta é sim, mas a velocidade da reação faz toda a diferença. "Atualmente existe o Mecanismo Especial de Devolução, conhecido como MED, que permite às instituições financeiras solicitar o bloqueio e analisar valores transferidos em situações de fraude. Quanto mais rápido o caso for comunicado ao banco, maiores são as chances de recuperação", explica Géssica.

Andressa Lipski lembra que existe um prazo relativamente amplo para registrar a ocorrência. "A vítima tem até 80 dias após a realização do Pix para registrar uma notificação de infração junto à sua instituição financeira por meio do MED", afirma. No entanto, ela alerta que a devolução não é automática. "Quando os recursos já foram movimentados ou distribuídos para múltiplas contas, a recuperação se torna mais complexa. Por isso, agir rapidamente é fundamental", ressalta.

O Banco Central já trabalha em novas camadas de segurança para o sistema. Entre elas está o chamado MED 2.0, que permitirá rastrear e bloquear com maior rapidez recursos transferidos para diversas contas, além de ampliar o compartilhamento de informações entre instituições financeiras. "O principal desafio da governança do Pix daqui para frente é encontrar o equilíbrio entre velocidade e segurança. Quanto mais mecanismos de proteção são adicionados, maior tende a ser o atrito na experiência do usuário. O desafio será continuar oferecendo conveniência sem comprometer a proteção dos clientes", conclui Andressa Lipski.

Enquanto novas ferramentas são implementadas, especialistas reforçam que a principal barreira contra os golpes continua sendo a informação. "Em um cenário em que os criminosos exploram cada vez mais a confiança e o comportamento das pessoas, atenção e cautela permanecem sendo as melhores formas de proteção", completa Géssica.

BC registra maior inadimplência da história

Taxa média de inadimplência das operações de crédito chegou a 4,7% em maio, o maior patamar desde o início da série histórica, em 2011. O avanço da inadimplência no Brasil voltou a manifestar um sinal de alerta sobre a saúde financeira das famílias. Dados divulgados nesta quarta (1º) pelo Banco Central mostram que a taxa média de inadimplência das operações de crédito chegou a 4,7% em maio, o maior patamar desde o início da série histórica, em 2011. O indicador reforça um cenário de crescente pressão sobre o orçamento dos brasileiros e evidencia desafios que vão além do acesso ao crédito.

Embora o índice não represente diretamente o percentual de brasileiros inadimplentes, ele mede a parcela das operações de crédito com atraso superior a 90 dias dentro do Sistema Financeiro Nacional. Quando analisado em conjunto com outros números recentes, o quadro se torna ainda mais preocupante. O endividamento das famílias já corresponde a quase metade da renda, enquanto levantamento da Serasa aponta que 81,7 milhões de brasileiros estavam inadimplentes em 2026.

Para Carlos Akira Sato, co-founder da Syscapial e especialista em Educação Financeira, os dados revelam um problema estrutural que não será resolvido apenas por mecanismos de renegociação de dívidas. "Programas como o Desenrola cumprem um papel importante ao oferecer fôlego para quem enfrenta dificuldades financeiras, mas renegociar dívidas não é o mesmo que educar financeiramente a população. O Brasil precisa enfrentar a origem do problema e não apenas suas consequências", afirma.

Educação financeira como infraestrutura econômica

Na avaliação do especialista, o país ainda falha em oferecer uma formação financeira ampla e contínua desde os primeiros anos da vida escolar. "Formamos consumidores antes de formar cidadãos financeiramente conscientes. Muitas pessoas aprendem sobre juros, crédito e endividamento da pior forma possível: quando já estão enfrentando problemas financeiros. Isso gera um ciclo que se repete de geração em geração", explica.

Segundo ele, a prioridade nacional deveria ser a formação de poupadores. "Existe uma sequência que precisa ser respeitada. Antes de transformar alguém em investidor, é necessário ensiná-lo a organizar o orçamento, compreender o impacto dos juros, diferenciar consumo de patrimônio e criar o hábito de poupar. Educação financeira vem primeiro, depois a formação de poupadores e, só então, a construção de uma cultura de investimentos", destaca.

Akira defende ainda que a responsabilidade pela educação financeira não deve ficar restrita ao poder público. Empresas, bancos, fintechs, plataformas digitais e demais setores da economia também têm papel relevante nesse processo. "Educação financeira não é filantropia, é infraestrutura econômica. Um consumidor financeiramente saudável compra melhor, paga melhor e mantém relações mais sustentáveis com o mercado. A inadimplência recorde registrada hoje é mais do que uma notícia econômica: é um diagnóstico de que o Brasil precisa investir na formação de poupadores para construir um futuro financeiro mais sólido", conclui.