Segurança e privacidade no ecossistema móvel

Principais temas e implicações para políticas públicas

A GSMA representa os interesses de operadoras móveis no mundo inteiro, reunindo quase 800 operadoras e mais de 250 empresas do ecossistema móvel, incluindo fabricantes de aparelhos, empresas de software, fornecedores de equipamentos e empresas de internet, assim como organizações de setores industriais adjacentes. A GSMA também organiza os principais eventos do setor, como o Mobile World Congress, Mobile World Congress Shanghai e as conferências Mobile 360.

Para mais informações, acesse o site da GSMA em **www.gsma.com**

Siga a GSMA no **Twitter: @GSMA**

Para saber mais ou se tiver alguma dúvida sobre essa publicação, escreva para **publicpolicy@gsma.com**

A A.T. Kearney é uma das principais empresas globais de consultoria em administração de empresas e está presente em mais de 40 países. Desde 1926, prestamos consultoria para algumas das organizações mais importantes do mundo. A A.T. Kearney é controlada pelos próprios consultores e tem como compromisso produzir resultados imediatos para seus clientes e gerar resultados vantajosos em áreas críticas.

Para saber mais, acesse **www.atkearney.com**

Índice

1 Sumário executivo

Nos últimos 30 anos, o mercado de telecomunicações móveis se expandiu enormemente e hoje inclui mais de 7,6 bilhões de dispositivos conectados[1], usados por 4,7 bilhões de clientes no mundo inteiro.[2] Esse crescimento deverá continuar. Em 2020, espera-se que quase três quartos da população da Terra será usuário de algum serviço móvel.[3]

Os efeitos desse crescimento se manifestam tanto nos países desenvolvidos como nos em desenvolvimento. Os serviços móveis permitem que indivíduos, empresas e governos inovem de formas criativas e muitas vezes inesperadas, enquanto consumidores no mundo inteiro adotam com entusiasmo as novas tecnologias. Em muitas economias desenvolvidas, a disseminação de smartphones e dispositivos móveis viabilizou o surgimento de modelos de negócios completamente novos, promovendo novas formas de interação empresarial e pessoal, e permitindo que o ecossistema móvel como um todo agregue US$ 3,1 trilhões de valor à economia.[4]

A internet, e principalmente a internet móvel, vem se tornando cada vez mais importante para a economia e para a sociedade. Isso criou a necessidade de proteger os usuários desses serviços e garantir que eles possam utilizá-los com segurança. Sem essa proteção, existe a chance de que os benefícios das tecnologias de comunicação sejam reduzidos. Consumidores que não confiam na integridade de um serviço de comércio eletrônico ou receiam que informações sigilosas possam ser interceptadas durante o uso de serviços de comunicação serão muito menos propensos a usar esses serviços e recorrerão a canais de comunicação mais caros e menos eficientes. Em casos extremos, por exemplo, um serviço lançado na década de 1990 que buscava melhorar a segurança de motoristas e pessoas vulneráveis viajando sozinhas e proteger a privacidade, viabilizando ligações de um dispositivo pessoal em vez de um telefone fixo na sala de estar da família, era passível de abusos que afetariam justamente esses dois aspectos fundamentais.

A indústria móvel vem trabalhando para orientar os consumidores e desenvolver novos recursos que promovam a confiança em seus serviços. A cada ciclo de inovação tecnológica, são lançados novos recursos, incluindo criptografia e validação da identidade dos usuários. Assim, os serviços móveis se tornam cada vez mais seguros e com menos riscos de fraude, furto de identidade e outras possíveis ameaças.

Esses serviços permitem que pessoas do mundo inteiro se comuniquem, realizem transações comerciais, compartilhem ideias e interajam, mas é preciso conquistar a confiança do consumidor. À medida que são lançados serviços mais avançados e complexos, surgem novos riscos em potencial e possibilidades de prejuízos. Fraudes e ataques cada vez mais sofisticados têm sido desenvolvidos e aplicados. Criminosos vêm buscando novas formas de interceptar comunicações, incluindo furtos de grandes volumes de dados, tal como a que obteve e revelou informações confidenciais durante as eleições de 2016 nos Estados Unidos. Outras fraudes menos divulgadas mas igualmente prejudiciais para as vítimas são esquemas de phishing, ransomware e fraudes financeiras. Evidentemente, essas fraudes têm como alvo as comunicações em geral e não apenas as comunicações móveis, de modo que é preciso considerar soluções que englobem todos os aspectos dos serviços em questão.

Governos e formuladores de políticas públicas naturalmente desejam evitar tais incidentes e proteger seus cidadãos tanto quanto possível. Entretanto, em ambientes complexos como esse, toda intervenção precisa ser cuidadosamente planejada. Qualquer decisão, por mais bem intencionada, pode acabar criando custos desproporcionais ou restringir o acesso aos serviços que se pretende proteger. Também é preciso analisar o equilíbrio complexo entre preservar o sigilo da comunicação individual e atender às necessidades dos órgãos de justiça e de segurança pública de interceptar algumas dessas comunicações para proteger a sociedade. A complexidade e o grande número de entidades envolvidas nesses serviços são outros fatores importantes. Por exemplo, quando duas pessoas participam de um chat, elas estão usando dois dispositivos diferentes, possivelmente com sistemas operacionais e aplicativos diferentes, e se conectam através de várias redes a uma mesma plataforma de mensagens, que muitas vezes se encontra em outra jurisdição que não a de um ou ambos os usuários. Cada um dos elos dessa cadeia apresenta possíveis fragilidades, brechas e ameaças como escutas, ataques de hackers ou malware. Tentativas de proteger esses consumidores que atuem em apenas uma vulnerabilidade podem ser insuficientes, e medidas que reforçam um componente já reforçado da cadeia em geral geralmente não funcionam para mitigar as fraquezas em outros pontos da cadeia.

1. Inclui conexões de máquina a máquina (M2M)
2. GSMA, 2016. "The Mobile Economy: 2016"
3. Ibid.
4. Ibid.

1

A indústria móvel já realizou grandes investimentos para permitir que seus serviços sejam usados com segurança e sigilo e, ao mesmo tempo, proteger a privacidade de seus clientes. Existe ainda, é claro, a dimensão tecnológica dessa iniciativa: os padrões melhoram continuamente, tecnologias melhores são instaladas e as redes são testadas para procurar fraquezas. Tudo isso aumenta a capacidade de detectar e impedir ataques. A GSMA exerce importantes atividades de coordenação e liderança de iniciativas como as relacionadas ao IMEI (códigos de identificação para impedir o uso de aparelhos roubados) e sistemas de acreditação de segurança para componentes críticos da infraestrutura. Muitas operadoras móveis e demais membros desse ecossistema têm forte atuação nos mercados e junto a organismos internacionais para maximizar a eficácia da tecnologia.

Entretanto, a tecnologia não consegue resolver sozinha todas as ameaças e desafios. Com o apoio da GSMA, o setor vem participando ativamente de programas para orientar consumidores e empresas sobre como usar com segurança as tecnologias móveis de modo a reduzir atividades ilícitas como abuso online, fraudes e violações de privacidade. Nesses casos, a resposta deve ser holística, envolvendo governos, outras agências e entidades sem fins lucrativos, assim como prestadores de serviços online ou via dispositivos móveis, como bancos e processadores de pagamentos.

São muito mais comuns os casos em que dados pessoais são compartilhados voluntariamente para acesso a serviços comerciais legítimos. Nesses casos, a indústria móvel enfrenta outro desafio: 8 em cada 10 consumidores se sentem inseguros com o grande volume de dados pessoais compartilhados, de modo que muitos usuários esperam que as operadoras abordem a questão. Entretanto, a tecnologia e questões de legislação antitruste dificultam ou até impossibilitam que as operadoras intervenham em interações entre um prestador de serviços online e o usuário final. Outra dificuldade é que as normas de proteção de dados variam entre diferentes jurisdições e, ainda mais importante, também variam entre o setor de telecomunicações e os prestadores de serviços online. Devido a essas discrepâncias, uma operadora móvel somente é capaz de proteger os dados de seus usuários se esses dados estiverem sob posse da operadora. Além disso, a operadora só é capaz de alertar seus usuários de que eles podem estar compartilhando dados com organizações que a operadora não controla. Os governos e o ecossistema como um todo devem colaborar para garantir soluções práticas, que permitam que os consumidores tomem decisões bem informadas, eficazes e que considerem o equilíbrio entre a privacidade e o desejo de obter aplicativos e conteúdos interessantes financiados por anunciantes em seus dispositivos móveis.

Outro desafio para a prestação de serviços móveis com sigilo e segurança é atender às necessidades dos órgãos de segurança pública. Esses órgãos precisam proteger os cidadãos. Para isso, eles às vezes tentam obter mandados amplos para acesso e utilização de dados pessoais, assim como para intervir ou bloquear determinados serviços de comunicação em situações especiais. A indústria móvel reconhece a obrigação legal e moral de contribuir para a segurança pública e acatar as demandas legítimas de governos que seguem o devido processo legal, e reconhece também as obrigações legais e morais de respeitar os direitos humanos. Cada vez mais, operadoras do mundo inteiro vêm precisando contestar intervenções específicas que consideraram desproporcionais, incompatíveis com normas internacionais de direitos humanos ou até contraproducentes para os objetivos de manutenção da segurança pública. Reconhecendo que há significativa complexidade do tema e diferenças entre jurisdições, a GSMA procura estabelecer princípios comuns e divulgar, com todas as partes envolvidas, o conjunto de melhores práticas. As operadoras móveis enfrentam dois outros desafios: estão na linha de frente quando governos tentam enfrentar empresas globais de internet sobre as quais as operadoras exercem pouca ou nenhuma influência; e, por vezes, as operadoras ainda são obrigadas a manter sigilo sobre essas atividades, embora desejem ser transparentes junto aos clientes que nelas depositaram sua confiança.

1

Principais implicações para governos, para o setor e demais partes envolvidas

Este relatório aborda os principais temas relacionados à proteção ao consumidor, à privacidade, à segurança pública e à infraestrutura; destaca possíveis problemas, explicando como eles vêm sendo abordados; e aponta as próximas medidas que poderão vir a ser tomadas. Diante da importância desses temas, os membros da GSMA concluíram que precisam trabalhar em conjunto, tanto em nível global como dentro de cada país, para responder da maneira mais eficaz possível. Esses problemas são tão complexos que não podem ser resolvidos por uma única organização ou setor. Para obter os melhores resultados para os usuários de serviços móveis e para a sociedade em geral, é preciso compromisso e ação de governos, órgãos de segurança pública, organizações multilaterais e não-governamentais e empresas de todo o ecossistema digital, além de iniciativas dos próprios consumidores. Alguns desses temas não são considerados prioridades em todos os países, e, consequentemente, por todas as operadoras, mas todos eles exigem estreita colaboração entre as várias partes envolvidas para fornecer serviços aos usuários de uma maneira que garanta a confiança e o sigilo. Devem-se desenvolver e adotar soluções as mais benéficas possíveis para a sociedade como um todo. Os sistemas modernos de comunicação são globais — incluindo normas, infraestrutura, equipamentos, serviços e operadores. Dessa forma, ações isoladas e unilaterais são menos eficazes que uma abordagem coordenada.

Este relatório apresenta uma série de princípios apoiados pelos membros da GSMA para proteger os consumidores e garantir a segurança das redes móveis. O relatório também é um convite para que os reguladores e formuladores de políticas públicas analisem esses temas com uma visão ampla para criar soluções que envolvam todos os participantes e, assim, proteger os interesses dos consumidores, das empresas e da sociedade. Com esse compromisso claro com a segurança, privacidade e sigilo dos serviços de comunicação móveis, o setor procura garantir que as comunicações móveis continuem a oferecer benefícios no futuro, mobilizando todo o potencial dessas tecnologias interessantes e dinâmicas para enriquecer as vidas das pessoas e da sociedade.

1

Proteção ao consumidor

Para incentivar o uso dos serviços e dispositivos móveis com segurança e responsabilidade, várias partes interessadas precisam contribuir. Governos e órgãos de segurança pública devem criar o ambiente apropriado, com marco regulatório, recursos e processos para deter, identificar e levar à justiça todas as práticas criminosas. Isso muitas vezes requer cooperação em escala global. Demais membros do ecossistema (por exemplo, fabricantes de aparelhos e fornecedores de serviços móveis) devem participar de iniciativas que ajudem a proteger os usuários e orientá-los sobre melhores práticas para que possam continuar se beneficiando desses serviços de forma segura. As operadoras móveis podem ajudar a lembrar seus clientes sobre a importância de permanecerem atentos e vigilantes, além de usar todos os recursos de segurança disponíveis. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras agirão de forma proativa para cuidar de problemas de proteção ao consumidor relacionados a atividades ilegais ou prejudiciais que utilizam ou que dependem de uso de celulares. Serão adotadas as seguintes medidas:

- **Trabalhar em parceria com outros órgãos para fornecer soluções multilaterais apropriadas.**
- **Adotar soluções projetadas para evitar que as redes sejam usadas para cometer fraudes ou outros crimes ou que os aparelhos sejam usados de forma lesiva ao consumidor.**
- **Orientar os consumidores sobre como agir com segurança para promover a confiança no uso de aplicativos e outros serviços móveis.**

Proteção à privacidade

O principal objetivo da proteção à privacidade é promover a confiança de que os dados pessoais serão devidamente protegidos, como previsto nas leis e marcos regulatórios de cada país. Isso requer que todas as partes envolvidas nesse ecossistema sigam uma abordagem consistente e neutra em termos de tecnologia, serviço e região. Os governos podem ajudar a garantir esse resultado sem sacrificar a flexibilidade necessária para a inovação adotando regras baseadas em riscos, preservando dados pessoais e incentivando práticas de governança digital responsáveis e alinhadas com a regulamentação local. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras adotarão medidas proativas para proteger e respeitar a privacidade dos consumidores, permitindo que eles tomem decisões informadas sobre quais dados serão coletados e sobre como seus dados pessoais serão usados. Para isso, adotarão políticas que promovem:

- **Armazenamento e processamento de dados pessoais de forma segura e de acordo com o marco legal aplicável.**
- **Transparência junto aos consumidores sobre dados que são compartilhados de forma anonimizada, conforme determinado pelo marco regulatório local.**
- **Fornecimento de informações e ferramentas aos consumidores para que eles tomem decisões simples e importantes sobre a própria privacidade.**

Manutenção da segurança pública

Para cumprir as leis e obrigações regulatórias, incluindo as relativas às licenças de operação, as operadoras móveis são obrigadas a assumir a tarefa de cooperar com órgãos de segurança pública em sua missão de zelar pela proteção ao público. Os governos devem garantir que o marco regulatório seja proporcional, indicando claramente quais são os poderes dos órgãos de segurança pública no país. O marco regulatório também deve garantir que os pedidos de assistência sejam: necessários; proporcionais às necessidades de cada caso; dirigidos ao serviço de comunicações ou provedor de tecnologia mais apropriado; e compatíveis com os direitos humanos. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

Ao lidar com questões envolvendo sigilo ou segurança pública nos países onde atuam, as operadoras cumprirão todas as obrigações perante a lei ou impostas como condicionamento de licença de prestação de serviço e, ao mesmo tempo, apoiarão questões relacionadas a direitos humanos. Colaboraremos com os órgãos competentes para proteger a segurança pública adotando as seguintes medidas:

- **Trabalhar junto aos órgãos competentes quando necessário, desenvolver e adotar soluções apropriadas para atingir o objetivo com transtornos mínimos para consumidores e serviços essenciais**
- **Desenvolver redes com funcionalidades para situações de emergência e risco à segurança**
- **Expor claramente os limites da nossa atuação dentro da cadeia de valor, destacando os pontos em que outros agentes podem atuar**

Segurança da rede e integridade dos dispositivos

Os membros do ecossistema precisam colaborar entre si e também com órgãos de segurança pública no mundo inteiro para compartilhar informações sobre ameaças e responder a ataques a redes e dispositivos móveis, além de identificar os autores. Isso requer tanto o engajamento das grupos já existentes de resposta a incidentes como a criação de novos grupos, conforme necessário, para cobrir lacunas existentes. Quando necessária, a regulamentação deve ser aplicada de forma consistente a todas as empresas da cadeia de valor, de forma consistente e neutra em termos de tecnologia e serviço, e sem prejudicar o modelo multistakeholder de governança e inovação na internet. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras se esforçarão para proteger a infraestrutura para garantir que os consumidores recebam os serviços de comunicação mais seguros e confiáveis. Para isso, serão adotadas as seguintes medidas:

- **Adotar providências para garantir a segurança da infraestrutura de rede que operamos e controlamos**
- **Promover parcerias público-privadas para minimizar os riscos de ataques de hackers ou de uso da rede para fins mal-intencionados por meio de abordagens coordenadas em nível global**
- **Definir claramente por quais elementos da infraestrutura as operadoras são responsáveis e os limites de atuação das mesmas em relação a outros elementos da infraestrutura ou da prestação de serviços**

2 Introdução

Em todas as regiões do mundo, a segurança nacional, a segurança pública e a privacidade individual encontram cada vez mais ameaças — algumas imaginárias, outras reais. As redes móveis são importantes para proteger a segurança pública. Alguns exemplos são a interceptação de chamadas e obtenção de registros de chamadas por órgãos de segurança pública em investigações criminais, comunicação em situações de emergência ou análise da disseminação de ameaças à saúde pública. Do ponto de vista do indivíduo, existem questões como fraude, furto de identidade, cyberbullying e outras atividades ilegais praticadas por meio de redes móveis e fixas ou através de serviços online. Alguns eventos recentes, tais como vazamentos de dados, geraram desconforto entre os consumidores, que desejam saber se sua privacidade e segurança estão protegidas, incluindo informações sobre suas vidas.

Nesse contexto, as operadoras móveis enfrentam o desafio de criar experiências móveis seguras para seus clientes e, ao mesmo tempo, cumprir suas obrigações junto à segurança pública. A GSMA e seus membros vêm desenvolvendo um extenso trabalho nas áreas de privacidade e segurança, buscando promover o uso seguro de dispositivos móveis e dos inúmeros serviços e aplicações por eles suportados.

Este relatório procura explicar as principais questões e desafios envolvendo segurança e privacidade no mundo das tecnologias móveis, destacando a complexidade e os trade-offs, e apresentando ainda as iniciativas do setor já existentes. O relatório também busca identificar as áreas em que há oportunidade de ir além dessas iniciativas, apresentando algumas ações para chegar nesses resultados, tais como orientar o consumidor, desenvolver parcerias com o ecossistema ou ainda adotar soluções técnicas envolvendo várias empresas da cadeia de valor. Este relatório aborda todos esses temas, reconhecendo que existem várias inter-relações entre eles.

Estrutura

Segurança e privacidade são assuntos extensos, mas podem ser divididos em quatro grandes áreas (Figura 1).

Figura 1

Um marco de privacidade e segurança

As próximas quatro seções deste relatório falam das seguintes áreas:

1. **Proteção ao consumidor** — promover o uso seguro de serviços móveis
2. **Privacidade e proteção de dados** — proteger a privacidade do usuário e processar e armazenar dados pessoais com segurança
3. **Manutenção da segurança pública** — definir o papel e as responsabilidades das operadoras móveis em apoiar agências do governo para proteger o público
4. **Proteger os dispositivos e a infraestrutura da rede** — garantir a integridade e a estrutura das redes móveis e dos dispositivos usados para acessá-las

A última parte do relatório explica os princípios fundamentais acordados entre membros da GSMA e apresenta um resumo dos planos para incluí-los em iniciativas futuras da entidade.

Como este relatório busca demonstrar, a natureza dessas questões requer ação coordenada em vários países por diversos segmentos do ecossistema. Nesse quesito, a indústria móvel assumiu um papel de liderança, mas diversos outros grupos — desde órgãos padronizadores como 3GPP, IETF e oneM2M, a entidades globais como a UIT, o Telecommunications Industry Dialogue (ID), a Global Network Initiative (GNI) e a Unicef — vêm atuando nessa área. Todas as partes têm um papel importante no debate e no desenvolvimento de soluções. A GSMA gostaria de contar com a colaboração e engajamento de todo o ecossistema móvel e de tecnologia da informação e comunicações (TIC) para abordar todos esses tópicos.

3 Proteção ao consumidor

À medida que se tornam cada vez mais importantes e abrangentes, os serviços móveis estão mudando de maneira fundamental a maneira como as pessoas se conectam e interagem, tanto umas com as outras como com empresas. Assim como com qualquer outra tecnologia tão disseminada, algumas pessoas tentam usar a tecnologia móvel para prejudicar outras.

Para que consumidores do mundo inteiro possam continuar a desfrutar os benefícios da tecnologia móvel, é importante que eles possam utilizar esses serviços com segurança e confiança. Esta seção trata de questões que afetam diretamente a segurança e o bem-estar dos consumidores de serviços móveis, principalmente aqueles que são expostos a ameaças oriundas de práticas ilegais ou. Alguns exemplos:

- Proteção de crianças e outras pessoas vulneráveis
- Furto e receptação de dispositivos roubados e uso de dispositivos falsificados
- Fraude e segurança de dispositivos móveis

Todas essas questões, que têm importantes repercussões para os governos, para as empresas e demais partes interessadas, serão aprofundadas neste capítulo.

3

Proteção ao consumidor

A colaboração multistakeholder é necessária para incentivar o uso dos serviços e dispositivos móveis com segurança e responsabilidade. Governos e órgãos de segurança pública devem criar o ambiente apropriado, com marco regulatório, recursos e processos para deter, identificar e levar à justiça todas as práticas criminosas. Isso muitas vezes requer cooperação em escala global. Demais membros do ecossistema (por exemplo, fabricantes de aparelhos e fornecedores de aplicativos móveis) devem participar de iniciativas que ajudem a proteger os usuários e orientá-los sobre melhores práticas para que possam continuar se beneficiando desses serviços de forma segura. As operadoras móveis podem ajudar a lembrar seus clientes sobre a importância de permanecerem atentos e vigilantes, além de usar todos os recursos de segurança disponíveis. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras agirão de forma proativa para cuidar de problemas de proteção ao consumidor relacionados a atividades ilegais ou prejudiciais que utilizam ou que dependem de uso de celulares. Serão adotadas as seguintes medidas:

- **Trabalhar em parceria com outros órgãos para fornecer soluções multilaterais apropriadas.**
- **Adotar soluções projetadas para evitar que as redes sejam usadas para cometer fraudes ou outros crimes ou que os aparelhos sejam usados de forma lesiva ao consumidor.**
- **Orientar os consumidores sobre como agir com segurança para promover a confiança no uso de aplicativos e outros serviços móveis.**

Crianças e pessoas vulneráveis

Os serviços móveis oferecem vários benefícios a grupos vulneráveis, e permite que eles se mantenham conectados, independentes e seguros. Entretanto, algumas crianças e indivíduos vulneráveis também praticam certos comportamentos negativos. Por exemplo, um estudo da GSMA analisou a diferença entre gêneros na posse e uso de dispositivos móveis e constatou que 68% das mulheres se preocupam com problemas de segurança, tais com assédio de estranhos.[5] 'Segurança e assédio' foi uma das principais barreiras à aquisição e uso de telefones celulares por mulheres.[6] Embora seja importante notar que somente uma fração de mulheres e homens esteja na categoria de vulnerabilidade, esse grupo precisa ter seus desafios reconhecidos e abordados para garantir que todos possam usufruir dos benefícios da conectividade, principalmente os grupos que podem se beneficiar mais do uso de serviços móveis.

Os consumidores precisam aprender a usar serviços e recursos de dispositivos móveis (por exemplo, câmeras) com segurança. Os aparelhos estão se tornando cada vez mais poderosos e podem realizar cada vez mais tarefas comuns, como facilitar o acesso à educação e ao aprendizado formal e informal, além de serviços bancários e de saúde. Isso torna sua utilização ainda mais importante. Na medida em que os consumidores se acostumam a esses e outros benefícios, cresce a relevância de expandir a educação sobre o comportamento digital com informações sobre segurança na internet, que podem ser divulgadas por meio de programas de informação e conscientização. Para criar programas como esses, que aumentam a "resiliência digital", é preciso que muitos atores participem ao mesmo tempo. As operadoras móveis precisam contribuir para esses programas e garantir que eles atendam às necessidades de um setor em rápida evolução e esclareçam o papel de cada elemento do ecossistema de TICs. As operadoras móveis já estão contribuindo para disseminar os benefícios das tecnologias móveis e, ao mesmo tempo, orientar grupos vulneráveis sobre como construir resiliência digital, usar os serviços com segurança e reagir a abusos, caso ocorram.

Apoio à inclusão e à segurança das mulheres

Em média, as mulheres têm 14% menos chances de possuir um telefone celular que os homens. Em algumas regiões, a diferença chega a 38%.[7] Isso significa que a diferença entre homens e mulheres quanto à posse de dispositivos móveis é de 200 milhões.[8] Mais de 1,7 bilhão de mulheres em países de renda baixa ou média não possuem dispositivos móveis.[9] Isso ocorre por diversos motivos. Para identificá-los e solucioná-los, a GSMA lançou o programa Connected Women. Em alguns países, em especial os de renda baixa, problemas de segurança e assédio vêm impedindo que algumas mulheres adquiram dispositivos móveis.[10] A GSMA e seus membros estão lançando uma iniciativa que expande o trabalho já realizado no programa Connected Women, mas com foco específico em questões de segurança e assédio.

As operadoras móveis sabem que o uso de serviços móveis de segurança permite que as mulheres continuem recebendo a segurança proporcionada pela conectividade e, ao mesmo tempo, reduzam as possibilidades de assédio. Por exemplo, as operadoras lançaram em vários mercados serviços que bloqueiam ligações indesejadas. Esses serviços interessam especialmente às mulheres. Existem também serviços para telefones básicos como o Banglalink Emergency, que envia automaticamente um SMS de alerta para três contatos predefinidos quando o usuário digita um código simples. Os contatos também recebem a localização do usuário[11], aumentando ainda mais a segurança do usuário.

5. GSMA, 2015. "Connected Women — Bridging the Gender Gap: Mobile Access and Usage in low- and middle- income countries"
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. O serviço Banglalink Emergency http://www.banglalink.com.bd/en/services/services/information-based-services/banglalink-emergency/

Proteção de menores online

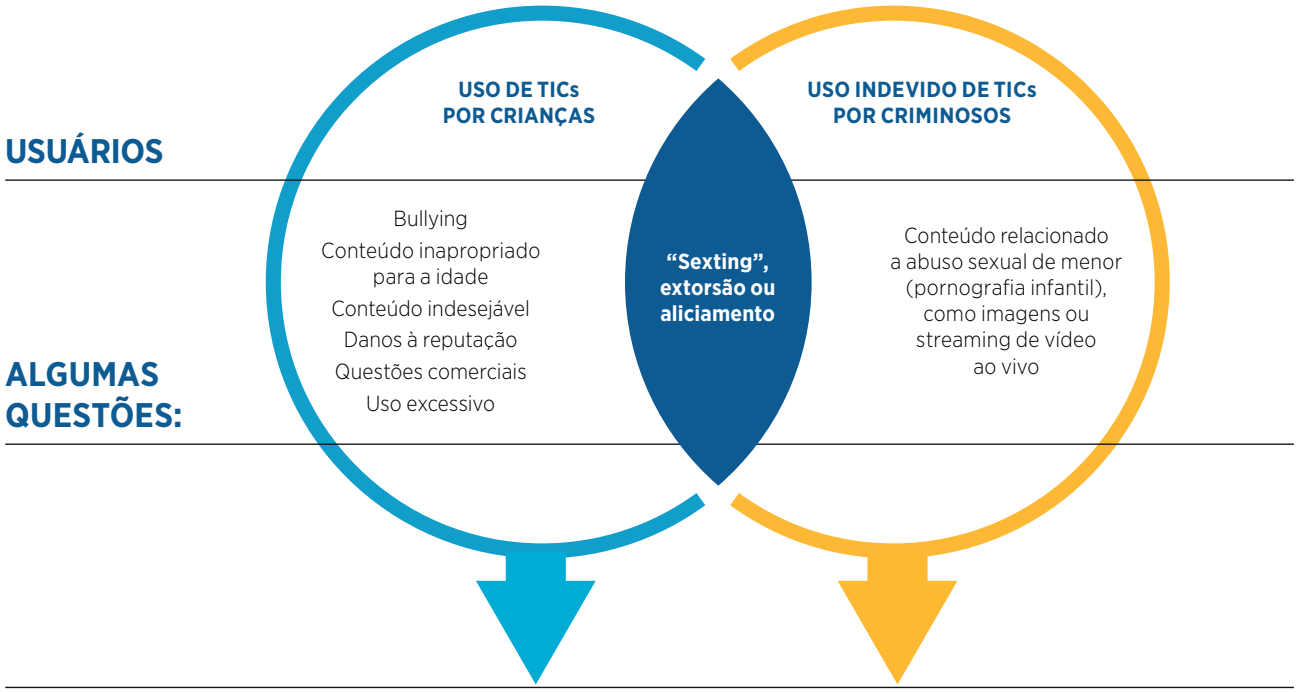
Outro grupo de usuários potencialmente vulneráveis de serviços móveis são as crianças. Para compreender melhor a proteção de crianças, deve-se distinguir entre duas questões diferentes:

1. Incentivar as crianças a usarem dispositivos móveis de forma segura e responsável
2. Combater o uso indevido de dispositivos móveis por adultos criminosos (por exemplo, produção, distribuição ou acesso a conteúdo ilegal relacionado ao abuso sexual de menores)

Conforme mostrado na Figura 2, devem-se distinguir entre esses grupos porque cada um deles requer uma resposta diferente.

Figura 2

Proteção de crianças online: questões e usuários



Para incentivar crianças e jovens a agir de forma mais segura no mundo digital, é preciso incentivar comportamentos positivos e orientá-los sobre possíveis riscos. Assim, eles poderão navegar pela internet com mais segurança e confiança. As operadoras móveis vêm contribuindo para isso em parceria com outros grupos interessados, como educadores, pais e grupos de jovens, adotando e aplicando políticas de uso aceitável, criando mecanismos de resposta para eventuais usos indevidos e disponibilizando controles parentais.

Para abordar o segundo problema e combater o uso indevido da tecnologia para acesso, compartilhamento ou exploração de conteúdos envolvendo abuso de menores, diversas entidades precisam agir em conjunto. O governo deve aprovar um marco regulatório apropriado, os órgãos de segurança pública devem estar preparados e autorizados para investigar casos envolvendo abuso de menores (do aliciamento ao compartilhamento de conteúdos envolvendo abuso sexual) e serviços de disque denúncia devem ser disponibilizados em nível nacional para reagir a denúncias de conteúdo online envolvendo abuso de menores. Nesse ambiente, o setor pode fazer sua contribuição no combate ao problema. Algumas possibilidades são trabalhar junto ao disque denúncia para remover conteúdos relacionados a abuso sexual assim que forem notificados, e, sempre que necessário, trabalhar junto a governos, seguindo os trâmites legais.

Nas áreas de sobreposição (Figura 2), ações adequadas requerem os dois tipos de abordagem mencionados. Por exemplo, para reduzir o risco de que jovens compartilhem imagens sexuais de si mesmos ("sexting"), é preciso que eles compreendam as possíveis consequências de compartilhar e perder o controle sobre essas imagens. Se esse tipo de conteúdo sexual for obtido e compartilhado indevidamente por um indivíduo mal intencionado, devem-se iniciar processos para impedir que o conteúdo seja visto (conforme discutido mais detalhadamente na seção sobre abuso sexual de crianças), além de identificar e processar o infrator.

Incentivar os jovens a usarem dispositivos móveis de forma segura e responsável

A indústria móvel vem procurando ativamente, em parceria com demais partes interessadas, incentivar o uso seguro de dispositivos móveis por menores. Colaborando com outras entidades do ecossistema móvel, ONGs e órgãos de governos, o programa GSMA mYouth[12] é dedicado a ajudar os jovens a desfrutar ao máximo sua experiência com dispositivos móveis. Assim como outras iniciativas, o programa mYouth procura novas maneiras de usar dispositivos móveis de forma segura e responsável. As operadoras vêm procurando orientar e informar o público por meio de campanhas de conscientização, além de oferecer soluções técnicas como sistemas de controle parental. A GSMA desenvolveu uma parceria com a Child Helpline International e elaborou diretrizes sobre como usar a internet com segurança. As crianças que encontram problemas online podem ser encaminhadas a serviços de ajuda com profissionais treinados para dar o suporte de que precisam.[13]

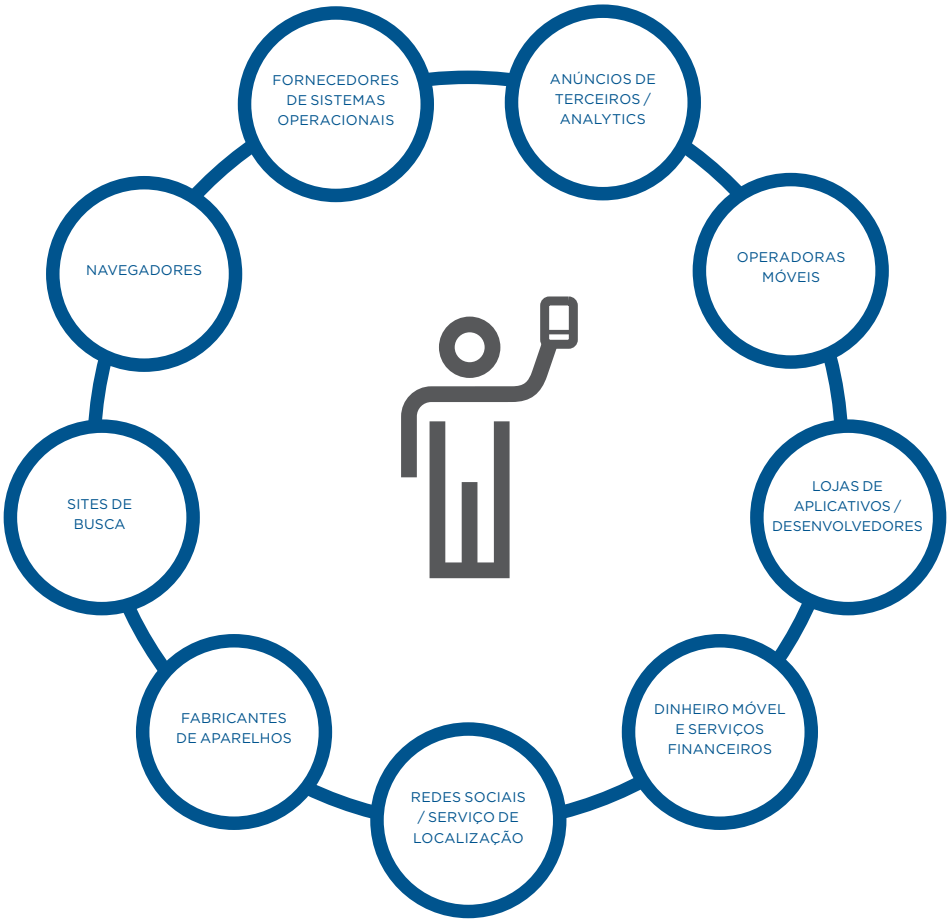
Para proteger os direitos de crianças online, as empresas e outras partes interessadas precisam definir cuidadosamente o equilíbrio entre os direitos da criança, considerando o direito à proteção e os direitos de acesso à informação e de liberdade de expressão. Portanto, as empresas precisam garantir que as medidas tomadas para proteger jovens online sejam bem direcionadas e não imponham restrições excessivas, nem para os jovens nem para outros usuários. As Diretrizes para a Indústria sobre Proteção de Crianças Online promovidas pela UIT e pela Unicef descrevem medidas que podem ser tomadas para ajudar a proteger e promover direitos das crianças no mundo digital.[14]

A rápida evolução do ecossistema móvel torna esse assunto bastante complexo. O modelo no qual as operadoras selecionavam serviços de conteúdo evoluiu, e hoje os usuários podem acessar diversos tipos de conteúdo digital através de seus dispositivos móveis. Esses recursos dependem da interação entre diversas entidades, incluindo operadoras móveis (ver Figura 3).

12. O programa GSMA mYouth promove o uso construtivo, seguro e responsável de dispositivos móveis por jovens. A iniciativa conta com a participação de várias entidades e desenvolve parcerias com a Child Helpline International e a Unicef. Para saber mais, acesse http://www.gsma.com/publicpolicy/customer-affairs/children-mobile-technology/myouth
13. As diretrizes estão disponíveis em http://www.childhelplineinternational.org/resources/manuals-toolkits/internet-safety-guides/
14. UIT e Unicef, 2014. "Guidelines for Industry on Child Online Protection"

Figura 3

O ecossistema móvel



As distinções tradicionais entre os setores de telecomunicações, radiodifusoras e empresas de internet estão rapidamente desaparecendo ou se tornando irrelevantes. A responsabilidade de incentivar o uso seguro de serviços móveis por crianças e jovens cabe ao governo, ao setor privado, a formuladores de políticas públicas, a educadores, à sociedade civil e aos pais.[15] Todos precisam cooperar para criar as bases para que a internet e as tecnologias a ela associadas sejam usadas com segurança.

A GSMA lidera um trabalho de autorregulação da indústria móvel e contribuiu significativamente para a elaboração das Diretrizes para a Indústria sobre Proteção de Crianças Online da Unicef e da UIT.
A GSMA interage ativamente com governos, agências regulatórias, formuladores de políticas públicas, órgãos de segurança pública e entidades do setor para facilitar o desenvolvimento de abordagens colaborativas que promovam o uso seguro e responsável da internet.

15. UIT e Unicef, 2014. "Guidelines for Industry on Child Online Protection"

Tema em foco

Diretrizes para a indústria sobre proteção de crianças online, desenvolvidas pela UIT e pela Unicef

As Diretrizes para a Indústria sobre Proteção de Crianças Online visam a estabelecer os princípios para que os serviços baseados na internet e em tecnologias associadas sejam usados de forma mais segura pelas crianças de hoje e gerações futuras.

As Diretrizes para a Indústria sobre Proteção de Crianças Online foram elaboradas a partir de consultas com membros da Child Online Protection Initiative, e também a partir de consultas mais amplas e abertas, com representantes da sociedade civil, empresas, universidades, governos, mídia, organizações internacionais e jovens para obter feedback sobre as propostas.

Cooperação e parcerias são fundamentais para garantir que a internet e as tecnologias a ela associadas sejam usadas com mais segurança. É preciso que o governo, o setor privado, formuladores de políticas públicas, educadores, sociedade civil, pais e responsáveis participem para alcançar esse objetivo. As iniciativas de autorregulação do setor podem atuar em cinco áreas principais:

1. **Integrar a preocupação com os direitos das crianças nas políticas corporativas apropriadas e nos processos de gestão**
2. **Desenvolver processos padronizados para lidar com materiais envolvendo abuso sexual de menores**
3. **Promover um ambiente online mais seguro e apropriado para menores**
4. **Conscientizar crianças, pais e professores sobre a segurança das crianças e uso responsável de tecnologias de informação e comunicação**
5. **Promover tecnologias digitais para incentivar o engajamento civil**

Combate a conteúdos envolvendo abuso sexual de crianças

A legislação sobre conteúdos ilegais varia bastante de países para país, mas conteúdos relacionados a abuso sexual de crianças são quase sempre ilegais. A exploração sexual de crianças por indivíduos ou organizações que desejam consumir, compartilhar ou lucrar com o esse tipo de conteúdo são práticas universalmente inaceitáveis.

Por isso, os governos precisam combater o uso indevido de conteúdos relacionados a abuso sexual de crianças. É preciso que haja legislação apropriada, que os órgãos de segurança pública disponham de autoridade e recursos para investigar e que haja serviços de disque denúncia para denunciar o abuso de menores online. Os provedores de internet e as operadoras móveis podem desempenhar um importante papel em impedir que crianças que sofreram abuso sexual tornem a ser vítimas ao restringirem o acesso ao conteúdo relacionado. Por exemplo, os membros da GSMA Mobile Alliance Against Child Sexual Abuse Content[16] vêm trabalhando para evitar que indivíduos e organizações usem serviços móveis para consumir ou lucrar com esse tipo de conteúdo. Para isso, eles colaboram entre si e compartilham informações, trabalham junto a serviços de denúncia, adotam processos de "notificação e retirada" e restringem o acesso a URLs ou websites que, na opinião das autoridades competentes, possuem conteúdo relacionado a abuso de menores. É importante frisar que uma autoridade competente (por exemplo, a Interpol, um serviço de denúncia ou um órgão de segurança) deve determinar quais URLs ou domínios precisam ser bloqueados. As operadoras móveis podem consultar essa lista e implementá-la sem serem obrigadas a decidir se um determinado conteúdo é lícito ou não.

Os membros da GSMA Mobile Alliance assumiram o compromisso de monitorar novas tendências que influenciem essa área e adotar medidas de resposta apropriadas. Por exemplo, a GSMA Mobile Alliance já começou a trabalhar junto a parceiros externos para entender, monitorar e, conforme apropriado, influenciar os possíveis efeitos da criptografia sobre restrições de acesso a conteúdos relacionados a abuso de menores.

16. Para saber mais sobre a Mobile Alliance, acesse http://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance

Tema em foco

Mobile Alliance Against Child Sexual Abuse Content: Uma iniciativa da GSMA

A Mobile Alliance Against Child Sexual Abuse Content (Mobile Alliance) foi fundada por um grupo internacional de operadoras móveis membros da GSMA para trabalhar em conjunto e evitar que indivíduos e organizações usem serviços móveis para consumir ou lucrar com conteúdos relacionados a abuso sexual de menores.

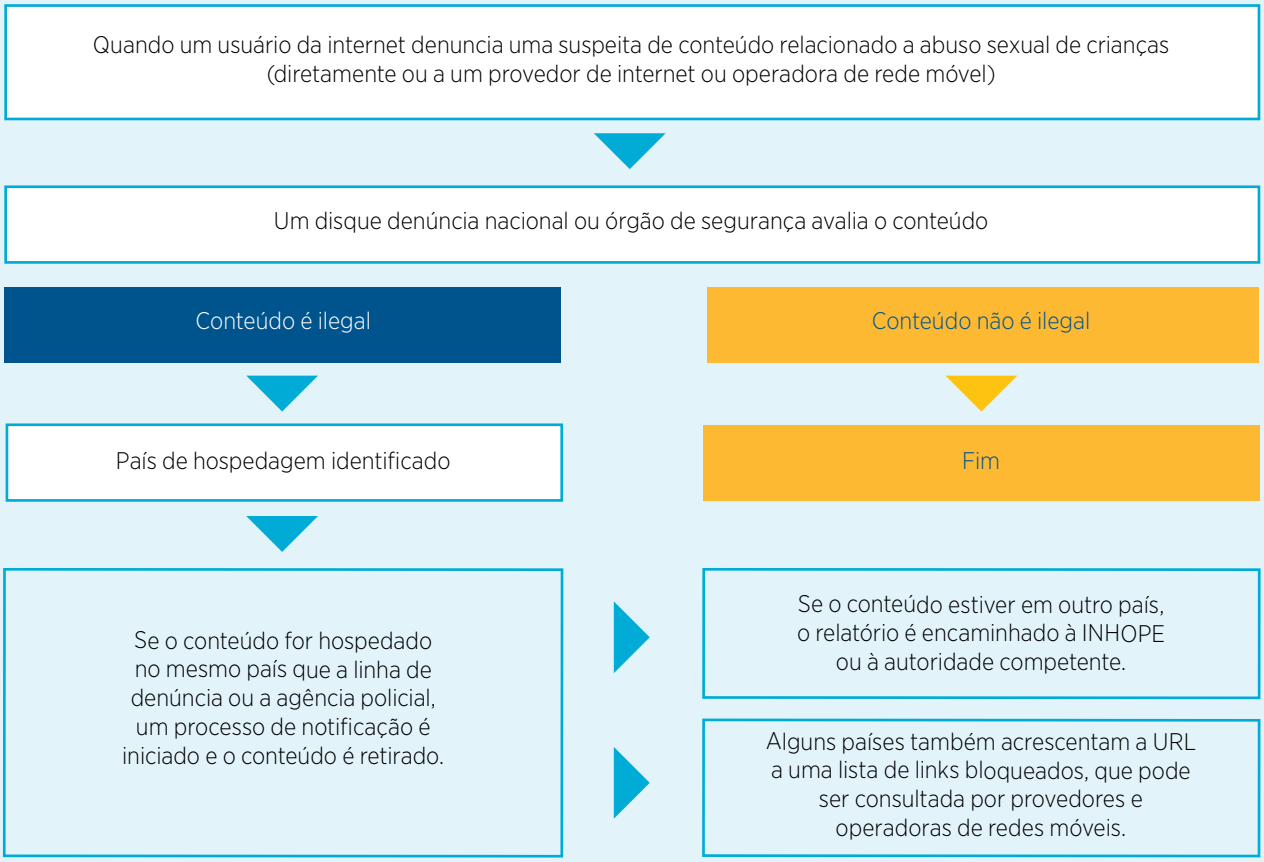
Os membros da Mobile Alliance assumiram os seguintes compromissos:

- **Implementar mecanismos técnicos para restringir acesso a URLs ou websites identificados por órgão internacional competente como hospedagem de conteúdo envolvendo abuso de menores**
- **Implementar procedimentos de notificação e retirada para permitir a remoção de conteúdos de abuso sexual de menores postados em seus sistemas**
- **Apoiar e promover serviços de disque denúncia e outros mecanismos para que os consumidores denunciem conteúdo envolvendo abuso de menores encontrado na internet ou em serviços móveis de conteúdo**

Usando uma combinação de medidas técnicas, cooperação e compartilhamento de informações, a Mobile Alliance tem buscado reduzir e reverter a proliferação de conteúdo relacionado a abuso de menores pelo mundo.

A Mobile Alliance também contribui para iniciativas mais amplas de erradicação desse tipo de conteúdo ao publicar diretrizes e ferramentas que podem ser utilizadas por toda a indústria móvel. Por exemplo, foram produzidos um guia para criar e manter um disque denúncia para denúncias, em colaboração com o INHOPE, uma organização que ajuda a desenvolver esses serviços em diversos países, e, em parceria com o Unicef, um guia de processos de notificação e retirada. Também foram desenvolvidas colaborações com a European Financial Coalition against Commercial Sexual Exploitation of Children Online e com a Financial Coalition Against Child Pornography.

Fluxograma descrevendo como serviços de disque denúncia e seus parceiros processam denúncias de conteúdo envolvendo abuso sexual de menores



3

Principais implicações para governos, entidades do setor e demais partes interessadas

Os dispositivos e serviços móveis melhoram as vidas dos jovens. Essa perspectiva precisa ser aceita, incentivada e melhor compreendida por todos os participantes para garantir que os jovens recebam o máximo de benefícios das tecnologias móveis. A melhor abordagem para proteger crianças online requer uma cooperação multistakeholder para incentivar o uso seguro e responsável de serviços online e dispositivos conectados à internet por crianças e jovens, assim como empoderar os pais e responsáveis a interagir com seus filhos e ajudar a protegê-los no mundo digital.[17]

Para combater o abuso de menores, é preciso uma resposta completa, que inclua legislação, linhas de denúncia, participação dos órgãos de segurança, apoio às vítimas e medidas e processos técnicos de apoio. Embora as operadoras móveis venham tentando enfrentar o problema (por exemplo, por meio da Mobile Alliance), é necessário que todas as organizações e entidades envolvidas deem apoio e assumam responsabilidades para realmente fazer diferença.

A indústria móvel condena veementemente a utilização de seus serviços para compartilhamento de conteúdo envolvendo abuso sexual de crianças.

- A Mobile Alliance Against Child Sexual Abuse Content da GSMA vem liderando esforços e combatendo de forma proativa o uso indevido de redes e serviços móveis por criminosos que querem acessar ou compartilhar conteúdo de abuso de menores[18]
- Para eliminar esse tipo de conteúdo, as operadoras utilizam termos contratuais, processos de notificação e retirada e mecanismos de denúncia[19]
- A indústria móvel está comprometida em trabalhar junto aos órgãos de segurança pública e demais autoridades competentes para remover rapidamente ou desabilitar casos confirmados de conteúdo ilegal hospedados em seus serviços,[20] incluindo conteúdos relacionados a abuso sexual de crianças.

Os governos devem definir de forma aberta e transparente o que é ilegal ou não antes de transferir a responsabilidade a serviços de disque denúncia, a órgãos de segurança pública e ao setor privado.[21] Entretanto, essas iniciativas proativas não devem ser estendidas de modo a violar convenções internacionais de direitos humanos ou responsabilidades do setor privado definidas nos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos. Os governos podem interagir com iniciativas como a WePROTECT Global Alliance, que oferece o "Modelo de Resposta para Países", uma ferramenta útil para orientar a reação dos países à existência de conteúdo online envolvendo abuso de menores.[22]

17. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Crianças e Tecnologia Móvel"
18. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Conteúdo Ilegal"
19. Ibid.
20. Ibid.
21. Ibid.
22. Para saber mais, acesse http://www.weprotect.org/the-model-national-response/

Dispositivos roubados ou falsificados

Furto e receptação de dispositivos móveis

Como os dispositivos móveis são pequenos, portáteis, caros e contêm informações valiosas, eles são visados por criminosos. Surgiu até um mercado negro internacional de dispositivos furtados. Em muitos países, tomadores de decisão vêm se preocupando cada vez mais com o furto de celulares e com o envolvimento do crime organizado na exportação em massa de aparelhos roubados.

Criando barreiras para o furto e a receptação de dispositivos móveis

A GSMA atribui números de identificação únicos, conhecidos como International Mobile Equipment Identifiers (IMEIs) aos fabricantes de dispositivos compatíveis com o 3rd Generation Partnership Project (3GPP)[23]. A base de dados de IMEI registra informações sobre faixas de números IMEI e informações sobre os aparelhos para os quais os números foram atribuídos. Entre as informações gravadas estão o nome do fabricante, o modelo do aparelho e os recursos de rede (por exemplo, frequências, interfaces de rádio e tipos de dispositivo).

Em 1996, a GSMA lançou uma iniciativa para bloquear dispositivos móveis roubados que emprega uma base de dados de IMEIs cujo roubo ou perda foi comunicado pelos próprios clientes às operadoras que integram a GSMA. Essa lista centralizada — comumente denominada de lista negra — está disponível para todos os membros da GSMA, que podem se conectar ao base de dados de IMEI e compartilhar dados sobre aparelhos roubados. Quando um dispositivo da lista negra tenta se conectar à rede móvel, a operadora pode bloquear o seu uso. Uma vez que os criminosos perceberem que poucas pessoas comprarão os dispositivos furtados, visto que provavelmente serão desabilitados logo após o furto, a atratividade desse tipo de crime será reduzida. Para apoiar essa iniciativa, a GSMA incentiva seus membros a adotar um registro de equipamentos EIR (Equipment Identity Register) em suas redes para bloquear a conexão de aparelhos roubados com base no identificador IMEI. O bloqueio de IMEI baseado na lista negra teve impacto positivo em vários países, mas uma campanha antifurto realmente eficaz requer outras medidas. O furto e receptação de dispositivos é um problema no mundo inteiro. Mesmo que todas as operadoras de uma região bloqueiem um determinado IMEI, o dispositivo pode ser usado em outra região na qual as operadoras não estejam conectadas à base de dados de IMEI da GSMA.

A GSMA vem trabalhando para conectar tantas operadoras móveis quanto possível à base de dados de IMEI. Ao final de 2016, a lista negra da base de dados da GSMA vinha sendo usada por mais de 140 operadoras móveis em mais de 40 países no mundo inteiro. Informações sobre dispositivos roubados são compartilhadas todos os dias. Na América Latina, onde são frequentes os furtos de aparelhos, 18 países se conectaram à base de dados IMEI para compartilhar dados sobre dispositivos roubados. A maioria das operadoras móveis da região já está conectada. Para empoderar e ajudar os consumidores e varejistas, um serviço público de verificação de IMEI foi lançado em alguns mercados para verificar a situação de dispositivos colocados à venda. Essa iniciativa foi lançada como parte da campanha Nós Ligamos[24] a GSMA. Até o final de 2016, mais de 1,5 milhão de consultas haviam sido realizadas.

23. A 3GPP é formada por sete organizações que desenvolvem normas de telecomunicações (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). As especificações da 3GPP são publicadas até quatro vezes por ano e seu acesso é gratuito. O termo "especificação da 3GPP" inclui todas as especificações GSM (incluindo GPRS e EDGE), W-CDMA (incluindo HSPA) e LTE (incluindo LTE-Advanced e LTE-Advanced Pro). Para saber mais, acesse www.3gpp.org
24. Para saber mais sobre a campanha We Care, acesse http://www.gsma.com/latinamerica/wecare

O sucesso do bloqueio dos IMEIs depende de que os fabricantes garantam a implementação segura do IMEI em todos os dispositivos móveis. Os principais fabricantes de aparelhos do mundo concordaram em apoiar duas importantes iniciativas da GSMA para tornar os IMEIs mais seguros. Uma delas é a definição de princípios para implementação segura de IMEI, e a outra é a participação no processo de relatoria e correção de vulnerabilidades de IMEI.[25] Alguns fabricantes poderiam fazer mais para melhorar a segurança relacionada à integridade do IMEI, que é essencial para o bloqueio efetivo de aparelhos. As operadoras móveis, outros grandes fornecedores e varejistas de dispositivos móveis poderão tomar decisões de compra fundamentadas em vários critérios ao escolher aparelhos para colocar à venda. Nesse sentido, a segurança proporcionada pelo IMEI e o cumprimento de normas técnicas podem até se tornar aspectos chaves para as decisões de compra. É importante que todos os envolvidos — fabricantes, operadoras móveis, governos e consumidores — trabalhem juntos para garantir a integridade do IMEI e corrigir rapidamente quaisquer problemas que surgirem. Os governos também precisam reconhecer que a integridade dos IMEI é essencial para permitir o bloqueio de dispositivos roubados. Por isso, a adulteração de IMEIs (também chamada reprogramação) deve ser criminalizada. Alguns países já proíbem a mudança de números IMEI de dispositivos móveis após a fabricação. Acreditamos que os outros países devem seguir esse exemplo e procurar identificar e punir quem realiza essa prática para desestimular a violação de mecanismos de segurança.

Outra forma de impedir o uso indevido de dispositivos móveis é o "Kill Switch". O Kill Switch desativa funções essenciais de dispositivos móveis e consiste basicamente em uma função do sistema operacional do dispositivo móvel que interrompe a operação quando ativada. O dispositivo só pode ser reativado ou voltar a ser utilizado com autorização do usuário. A GSMA elaborou um documento chamado Requisitos para Sistemas Antifurto de Dispositivos para fabricantes, operadoras móveis e governos, definindo uma série de características que o proprietário de um dispositivo pode usar para localizar, desabilitar ou reabilitar o dispositivo se ele for extraviado, perdido ou furtado.[26]

3

Figura 4

Como enfrentar o furto de dispositivos móveis

25. O processo de relatoria e correção de vulnerabilidades de IMEI é descrito em http://www.gsma.com/publicpolicy/wp-content/uploads/2007/07/IMEI-Weakness-Reporting-and-Correction-Process-3.2.0.pdf
26. GSMA, 2016. "Anti-Theft Device Feature Requirements, Version 3.0"

Principais implicações para governos, entidades do setor e demais partes interessadas

A GSMA procura ajudar todos os interessados em restringir a venda ou o uso de dispositivos roubados ou perdidos. Para ajudar governos e outros interessados em desenvolver soluções locais com foco no consumidor, a GSMA e seus membros podem oferecer recursos e expertise para desenvolver parcerias relevantes. A GSMA sugere, por exemplo:

- Promover a colaboração entre as principais partes interessadas:[27]
  - Os usuários podem comunicar o furto dos dispositivos às operadoras, habilitar recursos antifurto em seus dispositivos ou ainda, nos países onde as operadoras estão conectadas à base de dados de IMEI, verificar o IMEI para conferir a situação de dispositivos que pretendem comprar.
  - As operadoras móveis podem impedir que dispositivos roubados utilizem suas redes, conectar-se à base de dados IMEI para compartilhar dados de aparelhos da lista negra, e incentivar os fornecedores a garantirem a integridade do IMEI em seus produtos.
  - Os fabricantes de aparelhos podem projetar dispositivos mais seguros (por exemplo, impossibilitando a reprogramação do IMEI) e implementar funções como o Kill Switch para que os usuários possam desabilitar remotamente aparelhos perdidos ou furtados.
  - As lojas virtuais de aplicativos também podem obter os IMEIs de dispositivos roubados da GSMA e usá-los para bloquear o acesso desses dispositivos.
  - Os governos podem promulgar leis que proíbam a reprogramação ilegal de IMEIs e dar apoio de outras formas à indústria e aos órgãos de segurança pública em iniciativas de combate ao furto de dispositivos.
  - As agências regulatórias podem incentivar as redes locais a se conectaram à base de dados de IMEI da GSMA para compartilhar dados sobre dispositivos roubados, ou ainda a fornecer ou facilitar o acesso a serviços de verificação de IMEI. Assim, os usuários podem verificar um dispositivo antes de tomar a decisão comprá-lo. Essas medidas ajudam a criar um ambiente regulatório que promove soluções que empoderam o consumidor e são eficazes em combater o furto de dispositivos.
  - Os órgãos de segurança pública podem ter a possibilidade de verificar o status dos aparelhos acessando gratuitamente os dados da GSMA sobre dispositivos roubados. Assim, eles podem concentrar sua atenção e recursos no furto de aparelhos para identificar e apreender criminosos.
- É importante evitar soluções que possam ser menos eficazes ou trazer consequências negativas não planejadas.
  - A solução ideal para evitar o uso de dispositivos perdidos ou roubados é o uso de listas negras na rede. O uso de listas brancas para esse propósito deve ser evitado. As listas brancas foram criadas para outras finalidades, como ajudar no combate a dispositivos falsificados, apesar de que a efetividade dessa abordagem ainda não foi comprovada.
  - Soluções não padronizadas de combate a dispositivos furtados devem ser evitadas, pois são soluções proprietárias, e muitas vezes são caras e tecnicamente difíceis de implementar.
  - Abordagens distintas do previsto pelos padrões globais do setor, como vincular dispositivos específicos a usuários individuais, geralmente são difíceis, dispendiosas e podem produzir impactos desproporcionais sobre os usuários e os prestadores de serviços. Existe ainda o risco de criar problemas complexos no âmbito jurídico e concorrencial.
  - Criar bancos de dados de identificadores de dispositivos em nível nacional, além de significar um grande esforço, é um gasto desnecessário. A base de dados de IMEI da GSMA é capaz de atender às necessidades de bloqueio de dispositivos e de compartilhamento de dados. Manter um único repositório de dados de dispositivos para o mundo inteiro é preferível, pois garante a consistência, facilita o compartilhamento de dados e evita fragmentação, que reduziria a eficácia de todas as abordagens.

27. GSMA, 2016. "The Mobile Economy: Latin America and the Caribbean 2016"

Exemplo em foco

O setor vem contribuindo para combater o furto de dispositivos móveis na América Latina

Nos últimos anos, o furto de dispositivos móveis aumentou enormemente devido à adoção cada vez maior do telefone celular, e particularmente dos smartphones. Crimes relacionados a furtos de celulares vêm aumentando rapidamente em toda a América Latina. Por exemplo, nos primeiros 3 meses de 2014, 1,2 milhão de telefones celulares foram roubados no Peru. Isso corresponde a um aumento de 34% em relação ao mesmo período em 2013. Embora muitos desses crimes não sejam notificados, em 2014 a base de dados de IMEI tinha 14 milhões de registros de celulares roubados no Equador, Colômbia, Peru e Bolívia.

Muitos celulares roubados são contrabandeados para outros países para explorar oportunidades de arbitragem de preço ou para contornar iniciativas de países que tentam bloquear dispositivos usando o IMEI. Para combater esse crime, as operadoras precisam compartilhar informações, tanto no âmbito de cada país como em nível regional e até global.

Em 2011, a Comissão Interamericana de Telecomunicações (CITEL) aprovou uma resolução que recomendou, entre outras propostas: "regulação em nível regional do compartilhamento de bancos de dados de listas negras e do bloqueio de códigos de identificação (IMEI) para evitar que telefones roubados sejam ativados e usados em outros mercados, assim como para controlar atividades de tráfico ilegal de dispositivos de um país para outro dentro da região". Em 2012, 13 operadoras móveis latino-americanas se uniram e desenvolveram uma parceria com os governos da região para bloquear o uso de equipamentos roubados. Essa iniciativa voluntária levou ao compartilhamento de informações sobre dispositivos roubados para bloqueá-los e impedir o tráfico e o uso desses aparelhos em toda a região.

A GSMA continua trabalhando e promovendo a adoção dessas diretrizes por todos os membros da GSMA na América Latina. Diversas operadoras já assinaram memorandos de entendimento em cada país, buscando garantir o compartilhamento de dados em toda a região.

1

O CELULAR É FURTADO DO USUÁRIO

Samsung Galaxy

24%

47%

iPhone

são os modelos mais reportados na base de dados de IMEI

2

O USUÁRIO COMUNICA O ROUBO DO DISPOSITIVO À OPERADORA

Comunicados por dia

Argentina	**5000**
Colômbia	**4400**
Brasil	**8200**
Peru	**2800**

3

A OPERADORA ENVIA O IMEI DO CELULAR ROUBADO À BASE DE DADOS DA GSMA

18 países latino-americanos conectados à base de dados da GSMA

54 operadoras na região e 106 no mundo

Mais de 38 milhões de uploads desde a assinatura do termo de compromisso em julho de 2012

4

AS OUTRAS OPERADORAS DA REGIÃO BAIXAM OS IMEIs BLOQUEADOS

Em média, as operadoras da América Latina baixam dados relativos a pelo menos 34 operadoras da base de dados da GSMA

5

O CELULAR ROUBADO DO USUÁRIO 1 NÃO PODERÁ SER USADO EM OUTROS PAÍSES

Brasil (**6 milhões**), Argentina (**4,1 milhões**), Colômbia (**3,2 milhões**) e Peru (**2 milhões**) são responsáveis por

76%

de todos os IMEIs da região enviados à base de dados da GSMA

Venda e utilização de dispositivos falsificados

Um dispositivo móvel falsificado viola explicitamente a marca registrada ou design de um produto original, mesmo quando o nome da marca apresenta pequenas variações. Como são ilícitos, esses dispositivos geralmente são transportados e vendidos em mercados negros no mundo inteiro por redes de crime organizado. Por isso, os consumidores e os governos muitas vezes desconhecem a verdadeira natureza do impacto do comércio de dispositivos falsificados. Estima-se que 143 milhões de dispositivos móveis foram vendidos ilicitamente em 2013.[28]

A produção e a distribuição de produtos falsificados é um problema grave, que viola regras legítimas de comércio e propriedade intelectual, resultando na redução de receita dos fabricantes e de arrecadação dos governos. Além de todos esses problemas, dispositivos falsificados também podem prejudicar os consumidores. Em muitos mercados, a prevalência de dispositivos falsificados pode ser tão elevada que os consumidores adquirem esses dispositivos sem saber que são piratas.

Além de suas notórias deficiências de desempenho e utilidade, que resultam em pior qualidade de serviço para o usuário, muitos dispositivos falsificados podem conter materiais perigosos que trazem riscos ao meio ambiente. Diversos estudos encontraram materiais perigosos em dispositivos falsificados, como placas com solda de chumbo em níveis superiores aos considerados aceitáveis no mundo inteiro.[29] Esses limites são definidos por regulamentos que os dispositivos de fabricantes legítimos são obrigados a cumprir. Dispositivos falsificados contendo materiais perigosos são um risco ao meio ambiente se não forem descartados de forma ambientalmente correta.

Esses dispositivos podem ser difíceis de identificar e bloquear, e muitos deles contêm IMEIs que parecem legítimos. Há falsificadores que capturam sequências de IMEI atribuídas a fabricantes legítimos e as utilizam em seus produtos. Isso dificulta a distinção entre produtos legítimos e falsificados.

28. The Mobile Manufacturers Forum (MMF), 2014. "Counterfeit/Substandard Mobile Phones: A Resource Guide for Governments"
29. Ibid.

Restrições à venda e à utilização de dispositivos falsificados

Para ajudar a combater esse problema, os dados da lista branca (identificação dos intervalos de números atribuídos para todos os fabricantes legítimos) da base de dados de IMEI gerenciado pela GSMA podem ser usados para detectar e negar acesso à rede de dispositivos com IMEIs inválidos ou inexistentes. Entretanto, alguns IMEIs que pertencem a dispositivos legítimos foram usados em produtos falsificados. Nesses casos, é difícil identificar quais dispositivos são falsificados ou não. Alguns dispositivos falsificados podem ser bloqueados apenas depois que um consumidor, às vezes sem saber, comprou o dispositivo e tentou conectá-lo a uma rede móvel. Práticas como bloquear dispositivos que já foram vendidos muitas vezes punem inocentes e não os traficantes de produtos falsificados. As medidas não devem ser inconvenientes para usuários inocentes nem interferir no mercado legítimo. Mais especificamente, a fabricação e distribuição de dispositivos falsificados devem ser combatidas pelas autoridades competentes, que devem retirar os dispositivos de circulação antes que eles cheguem a consumidores que desconhecem sua procedência.

Em setembro de 2016, a GSMA e a Organização Mundial de Aduanas (OMA) iniciaram uma parceria para combater a falsificação e o contrabando de dispositivos móveis. A integração com a base de dados IMEI permite a verificação e a filtragem de dispositivos falsificados, que são identificados pelo IMEI no ponto de importação. Entretanto, essa solução não pode ser aplicada a dispositivos móveis contrabandeados que não passam pela aduana. Nesses casos, as alfândegas e órgãos de segurança pública precisam se concentrar no tráfico ilegal.

Como o assunto é complexo, as ações dos órgãos competentes para combater a distribuição e venda de dispositivos falsificados ainda são insuficientes para controlar o problema. Os marcos regulatórios nacionais atualmente são pouco eficazes, uma vez que os dispositivos falsificados são distribuídos no mundo inteiro e, por isso, os criminosos contornam facilmente iniciativas de países específicos. Além disso, não existe evidência que comprove a eficácia da utilização de listas brancas nacionais em combater a venda e o uso de aparelhos falsificados. Essa medida dificultaria o livre trânsito de aparelhos pelo mundo e seria ilegal em alguns países. O combate à falsificação requer soluções globais multistakeholder e será discutido na próxima seção desse relatório.

Principais implicações para governos, entidades do setor e demais partes interessadas

A GSMA reconhece que os dispositivos falsificados criam problemas para os usuários, redes, fabricantes e governos, e considera essencial manter a integridade do mercado de dispositivos móveis. A GSMA está disposta a trabalhar junto a seus membros, governos e demais partes interessadas para desenvolver soluções eficazes para combater a produção e a distribuição de aparelhos falsificados.

- Colaboração de todas as partes interessadas é fundamental:
  - Os reguladores podem trabalhar junto a fabricantes de dispositivos e operadoras locais para saber quantos dispositivos falsificados estão sendo usados no mercado local. O trabalho em conjunto permite desenvolver medidas que não penalizem os fabricantes de produtos legítimos nem prejudiquem usuários inocentes explorados pelos fraudadores.
  - Os governos podem ajudar a combater o mercado negro de dispositivos reduzindo a tributação de aparelhos importados, diminuindo, assim, o custo total de propriedade de aparelhos legítimos, e apoiando campanhas de conscientização e orientação do consumidor para enfatizar os riscos da compra de dispositivos falsificados.
  - Autoridades aduaneiras podem ser capazes de verificar se os dispositivos contêm identificadores que comprovam sua legitimidade. Para tanto, podem obter acesso gratuito aos dados de IMEI da GSMA e concentrar sua atenção e recursos em identificar e apreender os criminosos.
  - Os fabricantes de dispositivos podem trabalhar junto a governos, agências regulatórias e aduanas para ajudar a orientar demais partes interessadas sobre dispositivos falsificados, e fornecer inteligência às autoridades competentes sobre atividades relacionadas à produção, distribuição e venda de dispositivos falsificados.
  - As operadoras móveis podem se conectar à base de dados de IMEI da GSMA e obter uma lista definitiva de identificadores de dispositivos e, se necessário, negar acesso aos dispositivos identificados como falsos.
  - Os usuários podem verificar se os dispositivos que pretendem comprar são autênticos usando serviços de verificação fornecidos por terceiros.
- É importante evitar soluções que possam ser menos eficazes ou trazer consequências negativas não intencionais.
  - Soluções não padronizadas de combate a dispositivos furtados devem ser evitadas, pois são soluções proprietárias, e muitas vezes são caras e tecnicamente difíceis de implementar.
  - Abordagens distintas do previsto pelos padrões globais do setor, como vincular dispositivos específicos a usuários individuais, geralmente são difíceis, dispendiosas e podem produzir impactos desproporcionais sobre os usuários e os prestadores de serviços. Existe ainda o risco de criar problemas complexos no âmbito jurídico e concorrencial.

Fraude em dispositivos móveis

A fraude pode assumir diversas formas, e alguns tipos de fraude são perpetradas por meio de dispositivos móveis. Alguns exemplos são fraudes envolvendo serviços (por exemplo, furto de identidade ou fraudes financeiras), spam em dispositivos móveis[30] e, cada vez mais, a chamada "engenharia social" (por exemplo, phishing, phishing por SMS e Vishing),[31], que induz a vítima a revelar informações confidenciais, tanto pessoais como sobre os serviços que consomem, sem perceber que comprometeram a própria segurança.

As fraudes de engenharia social manipulam a vítima para induzi-la a realizar ações lesivas, como compartilhar dados pessoais ou senhas. Depois que obtêm esses dados pessoais, os criminosos podem armazenar essas informações e usá-las para cometer outras fraudes como furto de identidade e fraudes bancárias. Os fraudadores geralmente interagem com a vítima e tentam conquistar sua confiança, às vezes se valendo de informações disponíveis publicamente.

As fraudes envolvendo engenharia social estão crescendo. A Interpol (agência de polícia internacional) considera esse tipo de fraude como uma das que mais crescem no mundo. Por exemplo, o National Fraud Intelligence Bureau do Reino Unido constatou um aumento de 21% do número de incidentes entre outubro de 2014 e outubro de 2015.

Combatendo e reduzindo fraudes

Para um fraudador, o sucesso está em convencer sua vítima de que ele é quem afirma ser, seja pessoalmente ou por meio de um serviço ou website. Soluções tecnológicas oferecem certa proteção. Por exemplo, as operadoras móveis adotaram recomendações técnicas da GSMA para detectar e lidar com a transmissão internacional de spam fraudulento nas redes móveis.

Embora isso seja pouco comum, sistemas de correio de voz foram visados no passado para tentar comprometer a segurança de usuários de redes móveis, permitindo que indivíduos não autorizados ouvissem as mensagens de voz ou realizassem chamadas fraudulentas. Sistemas de correio de voz podem ser usados para perpetrar fraudes. A GSMA forneceu orientações às operadoras e consumidores sobre como instalar um sistema robusto de autenticação para proteger correios de voz e garantir que apenas o proprietário tenha acesso a esses serviços — tudo isso de forma que concilie a facilidade de uso com a necessidade de segurança.

Terminologia

Exemplos de fraude por engenharia social

- **Phishing —** método usado para infectar computadores ou dispositivos móveis para obter informações pessoais valiosas para o invasor. O phishing normalmente emprega recursos como o e-mail para induzir as pessoas a acessarem sites ou serviços que parecem legítimos e, a partir daí, obter informações pessoais.
- **Phishing por SMS —** usa mensagens de texto no telefone para jogar uma "isca" e induzir o usuário a divulgar suas informações pessoais.
- **Vishing —** ocorre quando os criminosos se passam por um prestador de serviços (por exemplo, um banco) ao telefone e convencem as vítimas a dar detalhes pessoais ou transferir dinheiro.

30. 'Spam móvel' se refere a mensagens comerciais não solicitadas enviadas para dispositivos móveis. A maioria das mensagens desse tipo procura fraudar ou enganar o destinatário e se aproveita do modelo de cobrança: como o destinatário paga pelo serviço, o remetente não incorre em custo nenhum.
31. Consulte o destaque sobre engenharia social
32. L. Gilman, 2012. "Mitigating the risk of fraud through consumer communication", GSMA

Principais implicações para governos, entidades do setor e demais partes interessadas

A fraude assume várias formas, é um tema complexo e é proibida por lei em quase todos os países. As operadoras móveis podem apenas influenciar o comportamento de seus clientes visando a prevenir e a minimizar os riscos de fraude. A legislação e a regulamentação deve se concentrar nos criminosos. Para proteger os consumidores, as principais medidas são a educação e a conscientização. Especialmente em mercados com baixos níveis de conhecimento tecnológico, muitos consumidores hoje ainda não utilizam plenamente os recursos de segurança disponíveis.

- É importante que os prestadores de serviços (como bancos, por exemplo) implementem os melhores níveis de segurança possíveis, de forma apropriada para os mercados em que atuam.
- Ações preventivas, como campanhas de conscientização do consumidor, devem ser utilizadas para ajudar os consumidores a se protegerem contra fraudes.
- Por sua vez, as operadoras móveis precisam desenvolver estratégias robustas de gestão de risco para reduzir as fraudes. Os tipos de medidas adotadas e o nível de implementação dependem da análise dos riscos para cada operadora e dos serviços que oferecem aos consumidores nos mercados em que atuam.

Estudo de caso

Gestão de riscos em dinheiro móvel: comunicação com os consumidores

O M-PESA da Safaricom é um exemplo de como as comunicações foram usadas para ajudar a evitar fraudes financeiras. Uma das maiores prioridades desse serviço é reduzir o risco de esquemas fraudulentos contra seus clientes. Além das medidas reativas, e em vez de usar apenas métodos de detecção (como monitorar e identificar tendências após o fato), a Safaricom utiliza controles preventivos para reduzir os riscos de fraudes contra seus clientes. A Safaricom descobriu que o melhor tipo de controle preventivo é conscientizar os consumidores por meio de comunicação clara. Para atingir e conscientizar os clientes do serviço M-PESA, a Safaricom adota uma abordagem multifacetada, que inclui campanhas por SMS, spots de rádio em dialetos locais e anúncios em jornais. O sucesso da Safaricom em conscientizar seus clientes por meio de mensagens claras foi essencial para que a empresa controlasse as fraudes envolvendo o serviço M-PESA.

A comunicação com os clientes deve ser integrada em uma estratégia mais ampla de gestão de riscos, complementada por acompanhamento e controle de dados, assim como procedimentos internos bem definidos. Por exemplo, a GSMA desenvolveu um modelo abrangente de gerenciamento de riscos relativos ao dinheiro móvel e uma ferramenta pronta para uso das operadoras.

Entretanto, o comportamento humano também é parte importante da questão das fraudes em dispositivos móveis. Para reduzir esse risco, os consumidores precisam conhecer as ameaças e saber proteger suas informações pessoais. As operadoras móveis podem ajudar a orientar os consumidores sobre a necessidade de se manter atento e vigilante. Mensagens mais específicas devem ser reforçadas por prestadores de serviços como bancos e lojas, que estão mais bem posicionadas para fornecer e exigir as medidas de segurança específicas relacionadas aos serviços que prestam.

Para ajudar as operadoras móveis nessa iniciativa, a GSMA recomenda que três princípios básicos[32] sejam sempre observados ao se elaborar mensagens voltadas ao consumidor:

1. A mensagem deve ser relevante e específica
2. A mensagem deve ser simples e fácil de entender
3. A mensagem deve ser reforçada durante interações com o cliente

4 Proteção à privacidade

Na última década, os serviços de comunicação se tornaram consideravelmente mais poderosos. A natureza desses serviços significa que as empresas de internet têm acesso a enormes quantidades de informações sobre os usuários, como sua identidade, com quem se comunicam e sua localização física, além de insights sobre seus interesses pessoais por meio dos sites que acessam e serviços que utilizam. Esses provedores de serviço podem analisar o conteúdo nas comunicações do usuário (por exemplo, as palavras digitadas em sites de busca ou locais procurados em aplicativos de mapa) e agregar os dados para descobrir interesses e intenções.

As operadoras móveis utilizam alguns dados pessoais para permitir o fornecimento de serviços de comunicação. As informações pessoais são usadas mais intensamente por outras empresas no ecossistema da internet.[33] Embora os usuários nem sempre percebam, muitos desses serviços online são oferecidos gratuitamente com a condição de que o provedor do serviço possa usar dados pessoais dos usuários para vender anúncios ou serviços pagos. Esta seção explica quais dados dos usuários são coletados no ecossistema da internet e como eles são armazenados, processados e acessados, assim como quais as implicações disso para a privacidade.

Os temas específicos tratados nessa seção são os seguintes:

- Coleta e utilização de dados, com foco no apoio à inovação
- Escolha do consumidor, com foco em incluir a capacidade de escolha em serviços e aplicativos online
- Fluxos de dados trasfronteiriços, reconhecendo a necessidade de considerar questões de segurança nacional

Todas essas questões, que têm importantes repercussões para os governos, para as empresas e demais partes interessadas, serão aprofundadas neste capítulo.

Proteção à privacidade

4

O principal objetivo da proteção à privacidade é promover a confiança de que os dados pessoais serão devidamente protegidos, como previsto nas as leis e marcos regulatórios de cada país. Isso requer que todas as partes envolvidas nesse ecossistema sigam uma abordagem consistente e neutra em termos de tecnologia, serviço e região. Os governos podem ajudar a garantir esse resultado sem sacrificar a flexibilidade necessária para a inovação adotando regras baseadas em riscos para preservar dados pessoais e incentivando práticas de governança digital responsáveis e alinhadas com a regulamentação local. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras adotarão medidas proativas para proteger e respeitar a privacidade dos consumidores, permitindo que eles tomem decisões informadas sobre quais dados serão coletados e sobre como seus dados pessoais serão usados. Para isso, adotarão políticas que promovem:

- **Armazenamento e processamento de dados pessoais de forma segura e de acordo com o marco regulatório aplicável.**
- **Transparência junto aos consumidores sobre dados que são compartilhados de forma anonimizada, conforme determinado pelo marco regulatório local.**
- **Fornecimento de informações e ferramentas aos consumidores para que eles tomem decisões simples e importantes sobre a própria privacidade.**

33. Para ler uma discussão mais detalhada desses serviços, consulte o documento que a A.T.Kearney editou em 2016 para a GSMA, "The Internet Value Chain: A study on the economics of the internet", pg. 11

Coleta e utilização de dados

Segundo previsão da GSMA, o número de smartphones aumentará de 2,6 bilhões em 2015 para 5,8 bilhões em 2020. Nesse mesmo período, o tráfego de dados deve aumentar a uma taxa de crescimento anual composta de 49%.[34] Essa proliferação de dispositivos e dados vem permitindo que indivíduos, empresas e governos inovem de formas novas e inesperadas.[35]

Entretanto, algumas pesquisas mostraram que, embora os consumidores venham usando cada vez mais esses serviços, eles também se preocupam com a própria privacidade e querem ter certeza de que podem confiar seus dados a essas empresas. Um estudo da GSMA constatou que 8 de cada 10 usuários de tecnologias móveis se preocupam com o compartilhamento de informações pessoais ao usar aplicativos. A pesquisa sugeriu também que cerca de metade dos usuários de dispositivos móveis preocupados com a privacidade usariam menos os aplicativos se não tivessem certeza de que suas informações pessoais estivessem bem guardadas.[36]

Ao analisar assuntos relacionados à coleta e utilização de dados pessoais, é importante fazer algumas distinções:

- As leis de privacidade (quando existem) variam de jurisdição para jurisdição e não existe um marco global único. Entretanto, muitas organizações sujeitas a essas leis têm presença global. Isso cria incerteza sobre qual a base legal apropriada e dúvidas sobre qual país tem jurisdição sobre o uso dos dados: o do usuário ou o do prestador do serviço? A situação se complica ainda mais se o prestador de serviço armazena e processa os dados em outro país.
- Deve-se distinguir também entre a operadora móvel e os serviços e aplicativos de terceiros que usuários podem acessar pela rede. A maioria das operadoras móveis está sujeita a obrigações legais e de licenciamento para proteger a privacidade, as quais não se aplicam a outros serviços online existentes no ecossistema da internet.

As discrepâncias atuais entre leis de países e setores diferentes praticamente impossibilitam, diante dos fluxos de dados globais atuais, que as expectativas de privacidade do consumidor sejam atendidas de forma consistente por todos os envolvidos. A aplicação inconsistente das regras deverá piorar ainda mais,

4

Terminologia

Dados pessoais

Dados pessoais — pode significar coisas diferentes para cada pessoa online e possui várias definições em lei. Este documento não pretende reinterpretar nenhuma lei. O termo dados pessoais significa, entre outras coisas, informações relacionadas a um indivíduo vivo que:

- **Foram coletadas diretamente de um usuário (por exemplo, digitadas na interface de um aplicativo) e podem incluir nome, endereço e dados de cartão de crédito**
- **Foram coletadas indiretamente (por exemplo, número de telefone, e-mail, nome, sexo, data de nascimento, dados de localização, endereço IP, IMEI e identificador do telefone)**
- **Descrevem o comportamento de alguém (por exemplo, dados de localização, dados sobre uso de produtos e serviços e acessos a websites)**
- **Foram geradas por um usuário e mantidos no dispositivo do usuário (por exemplo, logs de chamadas, mensagens, imagens geradas pelo usuário, listas de contato e agendas, anotações e credenciais de segurança)**

Usuário — Usuário significa o usuário final do dispositivo móvel, que inicia o uso de um aplicativo ou serviço e que pode ou não ser o cliente da aplicação ou do prestador de serviços em questão.

34. GSMA, 2016. "The Mobile Economy: 2016"
35. Ibid.
36. GSMA, 2014. "Mobile Privacy: Consumer research insights and considerations for policymakers"

pois cada vez mais dispositivos e sensores estão sendo interconectados pela Internet das Coisas (IoT)[37], que inclui serviços em escala global com vários tipos de prestadores que atuam em diversos setores.

Esses requisitos de privacidade inconsistentes em vários serviços e aplicativos podem fazer com que o usuário autorize sem perceber o acesso a seus dados pessoais, expondo-se de forma indesejável ou não intencional. Além disso, alguns serviços e aplicativos online levam os consumidores a "concordarem" com termos e condições de privacidade sem ler ou entender as implicações das decisões que tomaram. Uma pesquisa da GSMA mostra que 82% dos usuários concordam com termos de privacidade sem ler, pois geralmente eles são longos demais e contêm linguagem jurídica.[38] Como a diferença entre as operadoras móveis e outros serviços que os usuários acessam em seus dispositivos móveis nem sempre é percebida, existe também o risco de os consumidores não saberem quem está processando seus dados, ou, em alguns casos, de acreditarem que sua privacidade está mais bem protegida do que realmente está.

Tema em foco

Big Data

O aumento na capacidade computacional e a redução de custos das máquinas, assim como novas técnicas de análise, machine learning e disciplinas relacionadas hoje permitem processar e analisar grandes volumes de dados. Em alguns casos, essas análises permitem tirar conclusões apenas a partir da correlação entre os dados, sem necessidade de identificar conexões causais. Essas técnicas de análise são comumente chamadas de big data. Isso representa uma enorme mudança na capacidade da sociedade de criar novos produtos e serviços e permitirá a solução de importantes desafios de política pública — desde a gestão de rodovias em áreas urbanas congestionadas e poluídas a mais informações para compreender e evitar a disseminação de doenças.

Cada vez mais, as operadoras móveis usarão seus próprios dados e dados de outras fontes para análise de big data. Portanto, elas precisam assumir a responsabilidade pelos dados e, talvez no futuro, facilitar o acesso a dados desse tipo em uma espécie de marketplace.

Por exemplo, para ajudar a combater a epidemia de ebola, a Orange Telecom (África Ocidental) trabalhou junto com a Escola de Saúde Pública de Harvard (HSPH) e a Fundação Flowminder para prever a disseminação da doença usando dados de telefones celulares. A Orange Telecom agregou e anonimizou dados de telefones celulares na Costa do Marfim (2011) e no Senegal (2013). A Flowminder analisou esses dados e desenvolveu um modelo de análise dos deslocamentos populacionais na região, cujos resultados foram usados para emitir recomendações sobre como direcionar recursos de assistência à saúde (MIT Review, 2014. "Cell-Phone Data Might Help Predict Ebola's Spread").

O Telenor Group, a Telenor Pakistan e a HSPH realizaram pela primeira vez no Paquistão um projeto para compreender e modelar a disseminação da dengue a partir de dados anonimizados de mobilidade. Até hoje, nenhum projeto analisou um número maior de assinantes, mas, além disso, essa foi a primeira tentativa de analisar surtos de dengue usando análise de CDRs para criar estratégias de prevenção. A Telenor empregou sua capacidade analítica e conjuntos de dados exclusivos para criar valor tanto para a sociedade como para a própria Telenor. O estudo mostrou um modo de processar dados de consumidores obtidos por uma operadora móvel para resolver problemas sociais sem violar a privacidade dos usuários. Essa abordagem criou mapas de risco de dengue, que poderão ajudar profissionais de saúde e o governo do Paquistão a desenvolverem estratégias melhores de prevenção. (Telenor, 2017).

A indústria móvel está determinada a ajudar a realizar os benefícios econômico-sociais da análise de big data, observando sempre boas práticas de responsabilidade digital, para que a sociedade possa obter todos os benefícios dessa técnica sem violar princípios bem estabelecidos de privacidade e criando um ambiente de confiança mútua.

A GSMA vem colaborando com representantes do ecossistema móvel em relação aos aspectos de privacidade em big data, que se baseiam nos princípios de privacidade móvel promovidos pela GSMA.

37. A internet das coisas é discutida mais detalhadamente no capítulo Segurança de rede e integridade dos dispositivos.
38. GSMA, 2014. "Mobile Privacy: Consumer research insights and considerations for policymakers"

Preservando a privacidade do consumidor ao coletar e processar dados

A GSMA desenvolveu um conjunto de Princípios de Privacidade Móvel, que explicam como a privacidade dos consumidores de tecnologias móveis deve ser respeitada e protegida durante o uso de aplicativos e serviços móveis que processam ou coletam dados pessoais. Os princípios não substituem nem superam a legislação em vigor, mas são baseados em princípios reconhecidos e aceitos internacionalmente de privacidade e proteção de dados.[39] Esses princípios buscam equilibrar a proteção da privacidade individual e garantir tratamento justo e, ao mesmo tempo, permitir que as organizações atinjam seus objetivos em termos comerciais, sociais e também de políticas públicas. De modo geral, os princípios são flexíveis o bastante para acomodar novas tecnologias e métodos empresariais à medida que surgem. Dos nove princípios, seis são especialmente relevantes para a coleta e processamento de dados pessoais.

- Abertura, transparência e notificação
- Segurança
- Propósito e uso
- Crianças e adolescentes
- Minimização e retenção de dados
- Responsabilidade e fiscalização

Figura 5

Princípios de privacidade móvel da GSMA[40]

ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO

Os indivíduos responsáveis devem informar a seus clientes de forma aberta, clara e oportuna quais são suas práticas de proteção da identidade e da privacidade dos dados. Os usuários devem ser infomados sobre quais entidades coletam seus dados pessoais, o propósito de aplicativos e serviços, e sobre o acesso, coleta, compartilhamento e uso subsequente de suas informações pessoais, incluindo informações sobre com quem essas informações pessoais poderão ser compartilhadas. Assim, os usuários podem tomar decisões informadas sobre se desejam usar um determinado aplicativo ou serviço móvel.

SEGURANÇA

As informações pessoais devem ser protegidas com salvaguardas apropriadas para a sensibilidade da informação

RESPONSABILIDADE E FISCALIZAÇÃO

Todos os indivíduos responsáveis devem garantir que esses princípios sejam seguidos.

PROPÓSITO E USO

O acesso, coleta, compartilhamento e uso posterior de informações pessoais dos usuários deve ser limitado a interesses legítimos, como fornecer aplicativos ou serviços solicitados pelos usuários e para cumprir exigências legais.

CRIANÇAS E ADOLESCENTES

Aplicativos e serviços para crianças e adolescentes devem garantir que a coleta, acesso e utilização de informações pessoais seja sempre apropriada e observe a legislação em vigor.

MINIMIZAÇÃO E RETENÇÃO DE DADOS

Deve-se coletar, acessar e ou usar apenas o mínimo necessário de informações pessoais para finalidades legítimas da empresa e para fornecer, manter ou desenvolver aplicativos ou serviços. As informações pessoais não devem ser armazenadas por mais tempo que o necessário para tais finalidades ou para atender a exigências legais, e devem eventualmente ser apagadas ou anonimizadas.

RESPEITO AOS DIREITOS DOS USUÁRIOS

Usuários devem ser informados e dispor de meios fáceis para exercer seus direitos sobre o uso de suas informações pessoais.

CONTROLE E ESCOLHA DO USUÁRIO

OPT IN OPT OUT

Os usuários deverão ter oportunidades de fazer escolhas relevantes e controlar suas próprias informações pessoais

EDUCAÇÃO

Os usuários devem receber informações sobre privacidade, segurança e modos de gerenciar e proteger sua privacidade.

39. GSMA Mobile Privacy Principles (2016), consulte http://www.gsma.com/publicpolicy/mobile-privacy-principles
40. http://www.gsma.com/publicpolicy/mobile-privacy-principles

Principais implicações para governos, entidades do setor e demais partes interessadas

A GSMA e seus membros consideram a privacidade e a segurança elementos essenciais para construir a confiança nos serviços móveis. Por isso, eles assumiram o compromisso de trabalhar junto a participantes de todo o setor para desenvolver uma abordagem consistente para proteger a privacidade e promover a confiança em serviços móveis. Ao prestar serviços para seus clientes, as operadoras móveis procurarão proteger as identidades digitais e manter o sigilo das comunicações e dos dados pessoais. Os diversos serviços móveis disponibilizados por terceiros oferecem níveis variados de proteção à privacidade. Portanto:

- Para que os consumidores tenham certeza de que seus dados pessoais serão bem protegidos em todo e qualquer serviço ou dispositivo, é preciso fornecer um nível de proteção consistente.
- As proteções necessárias devem incluir uma combinação de melhores práticas internacionais, leis nacionais e medidas tomadas pelo próprio setor.

Para zelar pela transparência e manter os consumidores bem informados, a indústria, as autoridades responsáveis por proteção de dados e outros reguladores devem:

- Explicar claramente aos consumidores quais informações são protegidas e o que eles podem esperar em termos de privacidade
- Esclarecer quais áreas estão fora do controle dessas entidades, como aplicativos e serviços fornecidos por terceiros. Alguns perfis de usuários conseguem fazer essa distinção, mas essas informações não são conhecidas por todos os consumidores

Ao elaborar ou rever leis e regulamentos:

- Os governos devem garantir que a lei trate todas as tecnologias e serviços igualmente, e que as regras sejam aplicadas de forma consistente a todas as entidades que coletam, processam e armazenam dados pessoais.
- Como os serviços móveis inovam continuamente, a legislação deve se concentrar nos riscos à privacidade do usuário e não tentar criar mecanismos e exigências para tipos específicos de dados. Por exemplo, alguns dados podem ter valor comercial (por exemplo, serem vendidos a terceiros), operacional (por exemplo, influenciar decisões internas e distribuição de recursos) ou para o público (por exemplo, orientar iniciativas de resposta a desastres)

Escolha do consumidor

Empoderando o consumidor para escolher

Muitos serviços online são oferecidos gratuitamente aos consumidores, de modo que o prestador do serviço ganha dinheiro com publicidade. Para maximizar esses ganhos, a maioria dos serviços online (de websites a aplicativos) utiliza informações sobre o usuário. Os anunciantes que desejam anunciar para um usuário com um determinado perfil dão um lance para colocar um anúncio (em diferentes formatos) à vista do usuário. Esse tipo de microsegmentação e leilões que duram milissegundos vêm se tornando cada vez mais comuns. Para que isso funcione, o prestador de serviço precisa usar informações específicas do usuário, que podem ser obtidas diretamente ou compradas. Embora seja claramente necessário definir um equilíbrio entre o compartilhamento de algumas informações em troca do uso de serviços gratuitos, os usuários precisam ser capazes de tomar decisões claras e bem informadas sobre o que estão compartilhando.

Uma pesquisa contratada pela GSMA[41] mostra que os usuários de serviços móveis desejam escolhas simples e claras para controlar a maneira como suas informações são usadas. O estudo constatou que mais de 80% dos usuários de internet móvel do mundo inteiro se preocupam com o compartilhamento de seus dados pessoais ao acessar aplicativos e serviços. Foi observado também que a maioria dos usuários (65%), antes de instalar um aplicativo, procura saber quais informações o aplicativo deseja acessar em seu dispositivo, ou seja, mostram interesse em saber como sua privacidade poderá ser afetada. A maioria dos usuários de dispositivos móveis (81%) também deseja que sua permissão seja solicitada antes de terceiros terem acesso a seus dados pessoais em dispositivos móveis, e deseja, ainda, que ter melhor controle sobre os tipos de dados que serão compartilhados com diferentes empresas.

4

41. A GSMA vem trabalhando em parceria com seus membros para abordar de maneira proativa os principais desafios à privacidade em serviços móveis. Para esse fim, a GSMA contratou uma pesquisa global, que incluiu mais de 11.500 usuários no Brasil, Cingapura, Colômbia, Espanha, Indonésia, Malásia, e Reino Unido. O estudo mostrou que usuários de serviços móveis de todos os países têm atitudes e preocupações similares com a privacidade. O artigo "Mobile Privacy: Consumer research insights and considerations for policymakers" apresenta os principais resultados da pesquisa e discute suas implicações para formuladores de políticas públicas. O relatório completo está disponível em http://www.gsma.com/publicpolicy/mobile-privacy-consumer-research-insights-and-considerations-for-policymakers

Principais implicações para governos, entidades do setor e demais partes interessadas

Dos nove princípios de privacidade móvel desenvolvidos pela GSMA, três são especialmente relevantes em relação a informações pessoais:

- Escolha e controle do usuário: será dada a oportunidade aos usuários de fazer escolhas relevantes e controlar suas informações pessoais[42]
- Respeito aos direitos dos usuários: usuários devem ser informados e dispor de meios fáceis para exercer seus direitos sobre o uso de suas informações pessoais.
- Educação: usuários devem receber informações sobre privacidade, segurança e formas de gerenciar e proteger sua privacidade.

Com base nesses princípios, a GSMA também publicou, em parceria com representantes do ecossistema móvel, diretrizes de privacidade para o desenvolvimento de aplicativos móveis. Essas diretrizes foram concebidas para ajudar desenvolvedores de aplicativos a incluir a privacidade em novos aplicativos e serviços desde seu desenvolvimento.

Contudo, a aplicação desses princípios não é suficiente para dar aos consumidores todas as opções de que precisam. As operadoras móveis influenciam pouco ou nada os termos e condições de privacidade usados por prestadores de serviços online. Existe ainda o risco de que novas leis e regulamentos possam ter causar efeitos não intencionais, sobrecarregando os usuários finais ou criando "fadiga de privacidade" ao pedir que os usuários concordem com termos e condições que não foram entendidos ou sequer lidos.

Em relação aos serviços por elas prestados, as operadoras móveis procurarão adotar políticas de privacidade claras para que os usuários possam entender e controlar a maneira como seus dados pessoais são usados.

A GSMA assumiu o compromisso de trabalhar junto a demais partes interessadas para desenvolver uma abordagem consistente para proteger a privacidade e promover a confiança em serviços móveis. Esse compromisso levou, entre outras iniciativas, à liderança nesse espaço por meio das diretrizes de privacidade para o desenvolvimento de aplicativos móveis da GSMA, que destacam o seguinte:

- As operadoras móveis deve garantir que os riscos à privacidade sejam considerados ao desenvolver novos aplicativos e serviços, e oferecer soluções que deem aos consumidores maneiras simples de compreender as opções de privacidade e de controlar seus dados.
- Desenvolvedores de aplicativos para dispositivos móveis devem adotar princípios de privacidade propostos pela indústria, tal como os princípios de privacidade móvel desenvolvidos pela GSMA.
- A proteção precisa ser embutida em todos os novos aplicativos e serviços (isto é, privacy by design) para garantir transparência, dar opções e manter o usuário final no controle. Assim, pode-se criar confiança.

42. Nos Princípios de Privacidade Móvel da GSMA, os dados pessoais são denominados informações pessoais

Transferências transfronteiriças de dados pessoais

O terceiro aspecto da privacidade do consumidor diz respeito às jurisdições nas quais os dados pessoais são armazenados e/ou processados e às implicações dos fluxos de dados transfronteiriços. A centralização do armazenamento e processamento de dados muitas vezes permite que as operadoras móveis melhorem o desempenho e prestem serviços de forma mais eficiente do que seria viável se operassem em um único país. Isso permite vários serviços, inovações e suporte, os quais beneficiam os consumidores. Quando os dados são transmitidos de um território a outro, podem surgir dúvidas sobre a jurisdição à qual estão sujeitos. Se as estruturas e mecanismos de responsabilidade forem interoperáveis, os governos poderão solucionar questões de jurisdição e facilitar os fluxos de dados transfronteiriços.

Novos marcos regulatórios como as Regras de Privacidade Transfronteiriça (CBPR) da Cooperação Econômica da Ásia e do Pacífico (APEC) e as Regras Corporativas Vinculantes da União Europeia (UE) estão definindo princípios internacionais comuns, incluindo mecanismos de responsabilidade que regem a manipulação de dados transferidos de um país para outro. Entretanto, a adoção dessas regras é dificultada por governos que adotam regras de localização de dados (também conhecida como "soberania de dados"), que exigem armazenamento no país ou o emprego de tecnologia nacional.[43] Essas regras de localização se aplicam a vários setores e assuntos específicos, como prestadores de serviços financeiros, confidencialidade pessoal ou o setor público. Elas às vezes são adotadas por países que acreditam que as autoridades locais podem inspecionar dados armazenados localmente com mais facilidade.[44] Algumas dessas regras visam a proteger a privacidade, mas, em conjunto, elas criam um sistema fragmentado de leis e regulamentos, que é confuso, aumenta os riscos e diminui os benefícios de uma infraestrutura de rede aberta. Essas regras de localização de dados podem prejudicar o comércio digital e o crescimento econômico global.

Mantendo a privacidade e a segurança em fluxos de dados transfronteiriços

A operação de redes móveis gera grandes quantidades de dados diariamente. Cada chamada e transferência de dados precisa ser registrada e depois processada com dados sobre tarifas e saldos de conta para o faturamento dos serviços utilizados por cada usuário. Grandes quantidades de dados operacionais também são gerados e armazenados, incluindo dados sobre volumes de tráfego, logs de erros e solicitações de clientes (por exemplo, mudanças de tarifas ou mudanças de endereço). Para comportar esse grande volume de dados, as operadoras móveis são um dos principais usuários de serviços processamento e armazenamento de dados no mundo. Ao acessar esses serviços globais, os consumidores se beneficiam de diversos serviços, inovações e soluções avançadas que as operadoras podem oferecer, seja diretamente ou por meio de terceiros.

Nesses casos, garantir a integridade e a segurança dos dados é uma tarefa difícil que requer soluções complexas. Muitas operadoras móveis, sobretudo aquelas que são subsidiárias de grupos internacionais ou que contratam outros fornecedores, podem optar por armazenar esses dados em vários países. Isso permite criar economias de escala e concentrar recursos, pois uma única solução holística e robusta atende às necessidades de vários países, oferecendo mais recursos, segurança e redundância do que seria possível em uma abordagem fragmentada por país. Uma abordagem centralizada permite que as operadoras desenvolvam melhor expertise e adotem soluções redundantes que poderiam ser economicamente inviáveis em uma operação em um único país. Evidentemente, soluções como essas requerem a transferência dos dados dos clientes para data centers internacionais, que muitas vezes se encontram em outros países que não aquele do operador da rede.

Embora os benefícios técnicos sejam evidentes, as implicações legais são complexas. Quais regras de proteção de dados devem ser usadas: a do país onde os dados são processados, do país do usuário final ou do país no qual o controlador dos dados (por exemplo, uma operadora móvel) é sediado?

Os países podem adotar regras de localização de dados por diversos motivos, incluindo a ideia de que as autoridades podem inspecionar dados armazenados no próprio país com mais facilidade. Outro motivo comum é o desejo de proteger a privacidade individual e garantir que as expectativas e normas do país sejam atendidas. Uma maneira óbvia de garantir isso é exigir que os dados permaneçam no país. Entretanto, existem

43. Anupam Chander e Uyen Le, 2015. "Data Nationalism", Emory Law Journal; e Jonah Force Hill, 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", Hague Institute for Global Justice
44. Comissão Europeia, "Construir uma Economia de Dados Europeia", pg. 5

soluções e princípios que podem reduzir esses riscos sem restringir os fluxos de dados e os benefícios que eles trazem.

As restrições nem sempre melhoram a proteção dos dados pessoais. Se a proteção for fragmentada (por exemplo, diferenças entre jurisdições e setores sobre o que pode ser armazenado e por quanto tempo), ela se torna inconsistente e confusa, dificultando a gestão segura de dados pessoais. A fragmentação por meio de regras de localização também pode criar barreiras que tornam caríssimos os investimentos em segurança. Em conjunto, esses fatores podem impedir que as operadoras móveis criem tecnologias e serviços que protejam a privacidade do consumidor.

É importante enfatizar a distinção entre os dados pessoais aos quais as operadoras têm acesso e podem processar e os dados pessoais coletados e armazenados por prestadores de serviços online e intermediários no ecossistema da internet. Conforme discutido na seção sobre escolhas do consumidor, esses serviços são muito diferentes entre si. O fato de que são operados do lado de fora do país em que são usados pode gerar ainda mais complexidade jurídica. As questões de privacidade também são relevantes nesse caso, mas isso está fora do controle das operadoras móveis, que não tem acesso aos dados transferidos pelos usuários nem aos meios desse acesso.

Principais implicações para governos, entidades do setor e demais partes interessadas

O fluxo internacional de dados é importante para a inovação, concorrência e desenvolvimento socioeconômico. Portanto:

- Restrições e condições impostas para fluxos de dados internacionais devem ser minimizadas e aplicadas apenas em situações excepcionais.
- As regras de transferência transfronteiriça de dados devem ser baseadas no gerenciamento de risco, e devem incluir medidas para garantir que os dados sejam processados com proteções apropriadas e proporcionais e, ao mesmo tempo, ajudem a gerar benefícios socioeconômicos.
- Se um governo precisar inspecionar dados para fins oficiais, isso deve ser feito através de meios legais e usando mecanismos intergovernamentais apropriados que não restrinjam o fluxo de dados.

As operadoras móveis reconhecem a importância de manter dados segurança e de garantir que os direitos individuais não sejam lesados. Elas também reconhecem os complexos desafios envolvendo monitoramento e vigilância doméstica e internacional. Contudo:

- Os governos devem impor medidas restritivas de fluxos de dados transfronteiriços apenas quando absolutamente necessário para atingir um objetivo legítimo de uma política pública
- A aplicação dessas medidas deve ser proporcional e não discriminar contra fornecedores ou serviços estrangeiros

Um dos principais problemas atuais é que as transferências transfronteiriças de dados são reguladas por diversos mecanismos legais em nível regional, nacional e internacional. Embora essas leis sigam princípios comuns, elas não criam um marco regulatório interoperável que reflita as realidades, desafios e potenciais de uma rede conectada em nível global. As regras de proteção de dados devem, tanto quanto possível, ser interoperáveis em todos os países e regiões. A interoperabilidade cria um marco legal mais bem definido e previsível, permitindo que empresas criem estruturas escaláveis e transparentes de proteção de dados e privacidade.

Marcos de proteção de dados interoperáveis ajudariam a fortalecer e promover mecanismos apropriados e eficazes para garantir que os dados sejam gerenciados de forma a não comprometer os direitos e interesses de consumidores e cidadãos. Marcos interoperáveis que incorporem mecanismos eficazes de responsabilidade podem ajudar a fortalecer e proteger direitos importantes, que são essenciais para o progresso de indivíduos e da economia como um todo. Por exemplo, iniciativas para tornar o sistema CBPR da APEC interoperável com as Regras Corporativas Vinculantes da UE poderiam beneficiar o setor, o comércio digital e os interesses e direitos do consumidor.

A GSMA e seus membros continuam comprometidos em trabalhar junto a todas as partes interessadas para garantir que os fluxos de dados transfronteiriços sejam gerenciados de forma a proteger os dados pessoais e a privacidade individual. A GSMA e seus membros também reconhecem que é importante abordar os desafios relacionados ao fluxo transfronteiriço de dados, incluindo questões de jurisdição.

5 Manutenção da segurança pública

Como são parte essencial da infraestrutura do país, as redes móveis têm um papel essencial na manutenção da segurança pública e da sociedade como um todo. Por exemplo, as redes móveis são usadas como meio de comunicação por serviços de emergência, especialmente em casos de incidentes graves. Muitos desses incidentes são comunicados ao público através de dispositivos móveis.

Para cumprir as leis e obrigações regulatórias, incluindo as relativas às licenças de operação, as operadoras móveis são obrigadas a assumir a tarefa de cooperar com órgãos de segurança pública em sua missão de zelar pela proteção ao público. Por exemplo, um órgão de segurança pública pode obter uma ordem judicial para monitorar comunicações entre suspeitos no âmbito de investigações criminais. Portanto, a maioria das licenças concedidas a operadoras móveis requer que as empresas forneçam os recursos técnicos para cumprir a obrigação legal de auxiliar os órgãos de segurança pública. Na maioria dos países, essas intervenções são limitadas e sujeitas a um procedimento legal.

A Declaração Universal dos Direitos Humanos (DUDH)[45] e o Pacto Internacional sobre Direitos Civis e Políticos (ICCPR)[46] reconhecem que indivíduos no mundo inteiro têm o direito de se comunicar uns com os outros de forma privativa, e o direito à liberdade de expressão,

45. A Declaração Universal dos Direitos do Homem (DUDH) foi proclamada pela Assembleia Geral das Nações Unidas em Paris no dia 10 de dezembro de 1948 como um padrão comum a ser atingido por todos os povos e todas as nações. O documento definiu, pela primeira vez, direitos humanos fundamentais, que devem ser sempre protegidos. O direito à privacidade é previsto no Artigo 12 e o direito à liberdade de expressão, no Artigo 19. A DUDH é descrita em http://www.un.org/en/universal-declaration-human-rights/

46 O Pacto Internacional sobre Direitos Civis e Políticos (ICCPR) é um tratado multilateral adotado pela Assembleia Geral das Nações Unidas em 16 de dezembro de 1966, que está em vigor desde 23 de março de 1976. O direito à privacidade é previsto no Artigo 17 e o direito à liberdade de expressão, no Artigo 19. O tratado é descrito em https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en

sujeito aos limites, fronteiras e moralidade pública dos respectivos Estados nacionais. Ainda segundo os instrumentos internacionais de direitos humanos, esses direitos podem ser restritos apenas em situações muito específicas, e eventuais limitações devem ser aplicadas apenas quando necessário e de forma proporcional à possível ameaça.

Os objetivos de segurança nacional e de aplicação da justiça, que buscam proteger a segurança do público, às vezes conflitam com os direitos à privacidade, liberdade de expressão e acesso à informação. Na maioria dos países, essas diferenças entre necessidades levam a uma situação na qual as pessoas podem se comunicar livremente e sigilosamente, e eventuais interrupções e intervenções devem ser aplicadas apenas quando necessário, de forma proporcional e de acordo com um procedimento legal. A maioria dos países adota salvaguardas para evitar abusos e uso indevido de poderes que podem prejudicar a privacidade das comunicações.

Esta seção apresenta três exemplos típicos de intervenções realizadas para manter a segurança pública e os problemas que surgem quando várias partes tentam aplicá-las na prática, notadamente:

- Pedidos de assistência dos órgãos de segurança pública, com foco na necessidade de transparência e de salvaguardas
- Restrições do serviço, com foco específico no uso de bloqueadores de sinal
- Registro de usuários, com foco em registro de usuários de SIM cards pré-pagos

Todas essas questões, que têm importantes repercussões para os governos, para as empresas e demais partes interessadas, serão aprofundadas neste capítulo.

Manutenção da segurança pública

Para cumprir as leis e obrigações regulatórias, incluindo as relativas às licenças de operação, as operadoras móveis são obrigadas a assumir a tarefa de cooperar com órgãos de segurança pública em sua missão de zelar pela proteção ao público. Os governos devem garantir que o marco regulatório seja proporcional, indicando claramente quais são os poderes dos órgãos de segurança pública no país. O marco regulatório também deve garantir que os pedidos de assistência sejam: necessários; proporcionais às necessidades de cada caso; dirigidos ao serviço de comunicações ou provedor de tecnologia mais apropriado; e compatíveis com os direitos humanos. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

Ao lidar com questões envolvendo sigilo ou segurança pública nos países onde atuam, as operadoras cumprirão todas as obrigações perante a lei ou impostas como condicionamento de licença de prestação de serviço e, ao mesmo tempo, apoiarão questões relacionadas a direitos humanos. Colaboraremos com os órgãos competentes para proteger a segurança pública adotando as seguintes medidas:

- **Trabalhar junto aos órgãos competentes quando necessário, desenvolver e adotar soluções apropriadas para atingir o objetivo com transtornos mínimos para consumidores e serviços essenciais**
- **Desenvolver redes com funcionalidades para situações de emergência e risco à segurança**
- **Expor claramente os limites da nossa atuação dentro da cadeia de valor, destacando os pontos em que outros agentes podem atuar**

Pedidos de assistência de órgãos de segurança pública

Atendendo a pedidos de assistência de órgãos de segurança pública

As operadoras móveis possuem licenças que geralmente preveem a obrigação de colaborar com os órgãos de segurança pública e de segurança nacional em cada país onde atuam. Tais leis e condições de licenciamento geralmente exigem que as operadoras armazenem dados[47] sobre a utilização de redes móveis por seus clientes e os revelem a órgãos de segurança pública mediante ordem judicial; permitem ainda, também com ordem judicial, a interceptação em tempo real de comunicações entre os consumidores.

A lei normalmente define as situações, e às vezes os procedimentos, pelos quais órgãos de segurança pública podem solicitar às operadoras móveis acesso direto ou informações sobre comunicações realizadas em suas redes. Essas leis criam um marco legal que orienta as operadoras sobre como responder a esses pedidos. Em novembro de 2016, o Reino Unido aprovou novas leis[48] que esclarecem esses limites. Embora nem todos concordem sobre se os órgãos de segurança pública do Reino Unido devem ter esses poderes, é importante que as regras sejam debatidas e promulgadas publicamente. Em alguns países, as leis que regulam a quebra de sigilo ou a interceptação legal das comunicações de consumidores são pouco claras. Isso cria dificuldades para o setor, que procura manter a privacidade das informações de seus clientes e, ao mesmo tempo, acatar as obrigações decorrentes do licenciamento para colaborar com órgãos de segurança pública.

Nos últimos anos, tem havido um importante debate global sobre a abrangência, necessidade e legitimidade dos poderes do governo de acessar comunicações privadas entre indivíduos. Também surgiram dúvidas sobre como os prestadores de serviços de rede e telecomunicações devem proceder em relação a esse tipo de acesso. Para discutir essas questões, em 2011 um grupo de operadoras móveis formou o Telecommunications Industry Dialogue (ID) para trabalhar conjuntamente em temas relacionados à privacidade e liberdade de expressão, e definir princípios que destacassem a responsabilidade das empresas de telecomunicações de proteger a liberdade de expressão e a privacidade. Um dos resultados do trabalho da ID foi que algumas empresas decidiram, sempre que possível e em cada país onde atuam, revelar de forma proativa informações sobre a natureza e o volume de pedidos de quebra de sigilo feito pelos governos.[49]

A legislação nem sempre acompanha o desenvolvimento tecnológico[50], e pode haver mal-entendidos sobre a capacidade técnica das operadoras móveis de interceptar comunicações. A interceptação de telefonemas comuns ou mensagens de SMS de ou para usuários específicos é tecnicamente possível, e os requisitos e recursos para interceptação dentro da lei foram definidos há décadas nos padrões globais do setor. Entretanto, as operadoras geralmente não conseguem impedir a comunicação entre usuários que utilizam uma plataforma de internet, mesmo quando o tráfego passa por suas redes. Alguns serviços muito difundidos como o WhatsApp, WeChat e Signal são criptografados, e as operadoras das redes não têm acesso ao conteúdo das mensagens nem às chaves de criptografia. Isso significa que, mesmo quando um determinado pedido está dentro da lei, as operadoras não têm acesso aos dados, e, portanto, não podem fornecer o conteúdo das mensagens. A próxima seção apresenta, como exemplo, o caso do WhatsApp no Brasil.

As operadoras móveis reconhecem a importância, a soberania e a legitimidade dos governos, que precisam manter seus cidadãos em segurança. Para cumprir esse objetivo, a interceptação de comunicações para fins de policiamento ou segurança deve ser realizada sempre sob um marco legal claro, observando-se os princípios de direitos humanos, necessidade e proporcionalidade, e com a devida autorização legal.

Finalmente, a responsabilidade e, em muitos casos, os custos incorridos pelas operadoras para atender às necessidades de segurança pública vêm sendo absorvidos pelas operadoras. Um exemplo extremo ocorreu em El Salvador em novembro de 2015. O governo aprovou um imposto de 5% sobre serviços de telecomunicação para financiar planos de segurança.[51] Embora caiba aos governos definir a política fiscal, tributar as operadoras da infraestrutura de redes móveis que contribuem para a segurança é contraproducente, pois retira recursos de uma das entidades que já investe em segurança pública.

47. Ao anular a Diretiva em 2014, a Corte Europeia de Justiça (CEJ) decidiu que "a retenção generalizada de dados pessoais" prevista na Diretiva de Retenção de Dados da UE violava o direito à privacidade previsto no Estatuto de Direitos Fundamentais da União Europeia. Em dezembro de 2016, a CEJ confirmou essa decisão e decidiu que as legislações de países que produzem os mesmos efeitos que a Diretiva de Retenção de Dados também violam a legislação (acquis) da UE.
48. Para saber mais, acesse http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
49. Entretanto, muitos países proíbem expressamente as operadoras de publicar até mesmo detalhes gerais sobre a natureza ou o volume de solicitações de interceptação que recebem.
50. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Acesso de Governos"
51. Telecompaper, 2016. "El Salvador introduces 5% telecoms tax"

Principais implicações para governos, entidades do setor e demais partes interessadas

As operadoras móveis são responsáveis por atender apenas a solicitações feitas dentro da lei (ordens judiciais) de órgãos do governo devidamente autorizados, que seguiram o devido processo legal e com os mecanismos de salvaguarda necessários. Portanto, os governos devem garantir uma estrutura legal proporcional, que indique claramente quais são os poderes de monitoramento dos órgãos de segurança pública.[52]

- Toda interferência no direito à privacidade deve ocorrer de acordo com a lei, ou seja, a retenção de dados, a quebra de sigilo e a interceptação de comunicações para fins de policiamento ou segurança deve ser realizada sempre com o devido processo e autorização prescritos pela legislação.[53]
- Os prestadores de serviços de telecomunicação devem dispor de procedimento legal para contestar solicitações que acreditem não ser devidas nos termos da legislação em vigor.
- A legislação deve ser transparente, proporcional, justa e compatível com princípios de direitos humanos e com as obrigações contraídas em virtude de convenções internacionais de direitos humanos, como a Convenção Internacional sobre Direitos Civis e Políticos.
- Como os serviços de comunicações vêm se expandindo, a legislação deve tecnologicamente neutra.[54]
- Os governos devem limitar a responsabilidade ou indenizar as prestadoras de serviços de telecomunicações em caso de disputas legais decorrentes do cumprimento de solicitações de obrigações de quebra de sigilo, retenção ou interceptação de dados e comunicações, e interrupção do acesso a redes e serviços[55]
- Os governos também devem arcar com os custos de cumprir a legislação pertinente à interceptação de telecomunicações, retenção e dados, quebra de sigilo e restrições de acesso a redes ou serviços, como já ocorre em alguns países. Tais custos e suas bases de cálculo devem ser definidos com antecedência.[56]

A GSMA e seus membros apoiam iniciativas que procuram tornar os governos mais transparentes, e, sempre que possível, a publicação, pelos governos, de estatísticas relacionadas aos pedidos de acesso a dados de consumidores[57].

52. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Acesso de Governos"
53. Ibid.
54. Ibid.
55. Ibid.
56. Ibid.
57. Ibid.

Estudo de caso

Telecommunications Industry Dialogue: relatórios de transparência (publicação de pedidos de autoridades)

Por que um relatório?
O Telecommunications Industry Dialogue (ID) foi lançado oficialmente em 2013 e é um grupo de operadoras e fornecedores que se uniram para promover a liberdade de expressão e o direito à privacidade no setor de telecomunicações no âmbito dos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos. Essas empresas têm presença global, prestando serviços de telecomunicação e fornecendo equipamentos a consumidores, empresas e governos em quase 100 países no mundo inteiro.

Um dos principais objetivos do ID é o aprendizado conjunto. Para promover a transparência, as operadoras do ID (AT&T, Millicom, Orange, Telenor Group, Telia Company e Vodafone Group) publicam regularmente relatórios que revelam informações sobre pedidos de órgãos de segurança pública encaminhados a elas, na esperança de que os relatórios ajudem o público a entender o contexto em que as empresas operam e interagem com os órgãos de segurança pública.

Qual o conteúdo dos relatórios?
Os relatórios geralmente buscam atingir os seguintes objetivos:

- **Explicar os marcos legais e a capacidade de atuação dos órgãos de segurança pública nos mercados onde as empresas atuam**
- **Explicar as políticas e procedimentos adotados para responder a pedidos de órgãos e autoridades do governo**
- **Sempre que possível, publicar estatísticas sobre o número de pedidos de acesso a dados de consumidores em determinados países ou regiões.**

Quais são os limites?
A legislação sobre órgãos de segurança pública e segurança nacional muitas vezes prevê severas restrições, o que impede que as operadoras revelem informações sobre pedidos da polícia e de outros órgãos do governo, incluindo a publicação de estatísticas sobre os pedidos. Em muitos países, as operadoras também são proibidas de revelar ao púbico qualquer informação sobre como essas demandas são atendidas. Restrições como essas podem impedir as operadoras de responder às demandas do público por mais transparência.

Entretanto, essas operadoras acreditam que cabe aos Estados a responsabilidade de ser transparente. A métrica mais sensata, embora imperfeita, é o número de solicitações recebidas das autoridades. Assim, evita-se complexidade excessiva. Também cabe destacar que apenas os governos que fazem os pedidos às empresas de telecomunicações podem explicar completamente a natureza desses pedidos. (Telecommunications Industry Dialogue, consulte https://www.telecomindustrydialogue.org/)

Ordens de restrição de serviço e bloqueadores de sinal

Ordens de restrição de serviço

Além de solicitações de interceptação de comunicações, as operadoras móveis às vezes recebem ordens de órgãos do governo para restringir serviços em suas redes. São as chamadas ordens de restrição de serviço. Essas ordens exigem o desligamento ou restrição de acesso a uma rede móvel, um serviço específico da rede ou um serviço fornecido por um terceiro e acessado através da rede. As ordens podem exigir o bloqueio de determinados serviços ou conteúdos, restrição da largura de banda de dados ou degradação da qualidade de serviços de SMS ou de voz. Além de serem obrigadas por lei a cumprir essas ordens, em alguns casos, as operadoras podem sofrer processos criminais, incluindo prisão de diretores, ou perder suas licenças de operação se revelarem que receberam uma ordem de restrição de serviço ou se recusaram a cumprir tal ordem.

Esse tipo de restrição pode ter graves consequências. O uso indevido desses poderes pode até prejudicar a segurança nacional (por exemplo, restringir a rede para impedir ataques terroristas também impede que os cidadãos e órgãos de segurança pública se comuniquem para combater o terrorismo) e a segurança pública pode ser posta em risco se serviços de emergência e cidadãos não puderem se comunicar. Direitos humanos como liberdade de expressão, liberdade de associação e liberdade de empreender também podem ser prejudicados. As operadoras móveis também podem ser prejudicadas. Além de perda de receita e danos à reputação causados pela suspensão dos serviços, os funcionários também podem ser pressionados pelas autoridades ou até sofrer retaliação do público.

Um exemplo recente aconteceu no Brasil, onde o serviço de mensagens WhatsApp não deu suporte adequado a uma série de investigações criminais.[58] O governo reagiu exigindo que as operadoras móveis no Brasil restringissem o acesso aos serviços do WhatsApp em três ocasiões diferentes desde dezembro de 2015.[59] O principal efeito dessa medida foi impedir que mais de 100 milhões de usuários no Brasil usassem o aplicativo de mensagens mais popular do país. As decisões foram reformadas após apelos a tribunais superiores porque geraram um impacto desproporcional. O WhatsApp e sua controladora, o Facebook, afirmaram que a cooperação seria tecnicamente impossível porque as mensagens não são armazenadas; mesmo que fossem, não seria possível acessá-las porque o sistema possui criptografia ponto-a-ponto. Entretanto, muitos dos usuários afetados culparam suas operadoras de celular pela interrupção do serviço.

Houve exemplos mais extremos de desligamentos de redes em outros países. Em alguns casos, a rede foi desligada para impedir que a oposição a um governo se organizasse.[60] As operadoras móveis acreditam que os governos devem ser transparentes junto a seus cidadãos e explicar que possuem autoridade para desligar ou restringir o acesso a redes, assim como as bases legais das restrições. As empresas também devem ter permissão para revelar oportunamente a seus clientes que os serviços foram restritos por ordem do governo.[61]

58. The Financial Times, 2016. "WhatsApp ban ignites Brazil censorship fears"
59. The Guardian, 2016. "WhatsApp officially un-banned in Brazil after third block in eight months"
60. A Internet & Jurisdiction Retrospective Database menciona alguns exemplos de desligamentos. Consulte também http://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTYtMTEifQ
61. Para saber mais sobre a declaração conjunta do Telecommunications Industry Dialogue e do Global Network Initiative, acesse http://www.telecomindustrydialogue.org/global-network-initiative-telecommunications-industry-dialogue-joint-statement-network-service-shutdowns/

Uso de bloqueadores de sinal

Outra forma de restringir a comunicação móvel é usando bloqueadores de sinal, também conhecidos como jammers. Esses equipamentos geram interferências para impedir comunicações via rádio e bloqueiam a comunicação entre o terminal móvel e a estação base. Esses equipamentos são simples e costumam ser usados para bloquear a comunicação em penitenciárias ou entre terroristas ou grupos considerados subversivos, muitas vezes em locais onde há grandes aglomerações públicas. Os bloqueadores de sinal também são usados para evitar o uso de dispositivos móveis em áreas proibidas. Por exemplo, na América Latina os bloqueadores de sinal são usados para evitar o uso indevido de dispositivos móveis em locais sensíveis como penitenciárias. Entretanto, o bloqueio do sinal não resolve a causa básica do problema, que é a chegada de dispositivos móveis às mãos de criminosos. Outro problema é que as características dos sinais de rádio praticamente impossibilitam que a interferência gerada pelos bloqueadores fique restrita a uma área específica. Consequentemente, a interferência gerada por bloqueadores de sinal afeta cidadãos, serviços e órgãos segurança pública. Seus efeitos se estendem a diversos outros usuários, como, por exemplo, as pessoas que moram ou trabalham perto de prisões, que ficam impossibilitadas de usar serviços móveis. Existe ainda um efeito negativo para as operadoras devido ao custo dos bloqueadores, perda de receitas e, muitas vezes, danos à reputação causados pelas interrupções do serviço.

Interrupções nas redes de comunicação, serviços de rede ou de internet (por exemplo, mídias sociais, sites de busca ou de notícias) podem prejudicar a segurança pública e impedir o acesso a serviços vitais como serviços de emergência, de pagamentos e de saúde. Por exemplo, uma restrição de serviço pode impedir que usuários de serviços móveis liguem para números de emergência como '190' ou '192' ou interferir na operação de alarmes ou equipamentos médicos conectados à rede móvel. Por essas razões, as restrições de serviço devem ser utilizadas o mínimo possível, observando sempre que existem consequências negativas para todos os usuários.

5

Principais implicações para governos, entidades do setor e demais partes interessadas

A GSMA compreende a necessidade e apoia o uso de inteceptações dentro da lei para promover a segurança pública, mas acredita que as ordens de restrição de serviço e o uso de bloqueadores de sinal devem ser evitados.

As ordens de restrição devem ser usadas apenas em casos excepcionais, como último recurso, e quando absolutamente necessárias para atingir um objetivo específico, permitido por lei e compatível com direitos humanos internacionalmente reconhecidos.[62] Outros aspectos também devem ser observados:

- Para promover a transparência, os governos devem emitir todas as ordens de restrição de serviço por escrito, citando a base legal da ordem e mantendo uma trilha de auditoria até o indivíduo que autorizou a ordem. Os cidadãos devem ser informados que o acesso ao serviço foi restrito por ordem do governo com aprovação do judiciário ou de outra autoridade competente e de acordo com procedimentos previstos em lei. As redes móveis devem poder investigar os efeitos sobre suas redes e sobre seus clientes, além de comunicar livremente acerca da ordem para seus consumidores. Se esse tipo de comunicação puder comprometer a segurança nacional ao ser realizada com a restrição ainda em vigor, os cidadãos devem ser informados assim que possível após o evento[63]
- Os governos devem tentar evitar ou reduzir os possíveis efeitos prejudiciais das ordens de bloqueio limitando o número de ordens, a área abrangida, o número de indivíduos e empresas afetados, o escopo funcional e a duração da restrição. Por exemplo, em vez de bloquear toda uma rede inteira ou toda uma plataforma de mídia social, a ordem pode ser específica para determinados conteúdos ou usuários. Em todos os casos, a ordem deve sempre especificar uma data fim para a restrição. Para garantir que esses princípios sejam observados, é essencial que sejam estabelecidos mecanismos independentes de supervisão[64]
- As operadoras móveis podem buscar conscientizar os governos sobre os possíveis impactos das ordens de restrição. Elas também podem se preparar para agir com rapidez e eficiência, verificando se a ordem foi aprovada judicialmente, se é válida e legítima e se cabe apelação. Assim, elas podem trabalhar junto aos governos para limitar o escopo e as repercussões da ordem. Procedimentos devem incluir orientações sobre como as equipes locais devem lidar com as ordens (por exemplo, escalando o nível de tomada de decisão na empresa)[65]
- Em todas as decisões, a maior prioridade deve ser a segurança e o sigilo dos clientes, das redes e dos funcionários das operadoras. Também é preciso se preparar para restabelecer os serviços o mais rapidamente possível[66]

A GSMA e seus membros estão comprometidos em trabalhar junto a governos para usar a tecnologia de modo a manter os dispositivos móveis longe de áreas indevidas, além de colaborar em iniciativas que procuram detectar, rastrear e evitar o uso de dispositivos contrabandeados. Entretanto, é essencial encontrar uma solução prática, eficaz e de longo prazo que não prejudique os usuários legítimos nem os grandes investimentos que as operadoras precisam realizar para melhorar a cobertura.[67]

- Bloqueadores de sinal devem ser usados apenas como último recurso e apenas em coordenação com operadoras móveis licenciadas. Essa coordenação deve durar enquanto os dispositivos estiverem em funcionamento, a fim de minimizar a interferência em áreas adjacentes e não afetar outros usuários legítimos de dispositivos móveis.[68]
- Os reguladores também devem proibir o uso de bloqueadores de sinal por particulares e impor penalidades pelo seu uso ou comercialização sem permissão das autoridades competentes[69]
- A importação e a venda de bloqueadores ou equipamentos de interferência devem ser permitidas apenas a entidades devidamente qualificadas, autorizadas e reguladas pela agência regulatória de telecomunicações do país.
- A medida mais eficaz para reforçar a segurança e impedir que dispositivos de comunicação sem fios sejam introduzidos em locais indevidos (por exemplo, penitenciárias) é fortalecer a segurança, pois assim os direitos de usuários legítimos na região ao redor não são afetados.[70]

62. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Ordens de restrição de serviço"
63. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Ordens de restrição de serviço
64. Ibid.
65. Ibid.
66. Ibid.
67. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Bloqueadores de sinal"
68. Ibid.
69. Ibid.
70. Ibid.

Tema em foco

Reduzindo os impactos de ordens de restrição de serviço

Em situações de emergência, autoridades dos governos de alguns países têm o poder de exigir medidas extremas das operadoras, tais como desligar total ou parcialmente as redes e serviços por qualquer período de tempo. Quando esses pedidos são feitos por motivos de segurança nacional, o descumprimento pode acarretar graves penalidades. Mesmo quando recebem tais pedidos de governos, algumas operadoras procuram minimizar os possíveis efeitos sobre a liberdade de expressão e a privacidade. Apresentamos a seguir três exemplos:

1) Em 1º de junho de 2014, autoridades do governo de um país africano contataram a Orange por telefone e pediram que a empresa suspendesse os serviços de SMS em todo o país. Para verificar a base legal do pedido, a Orange pediu que a ordem fosse encaminhada por escrito. No dia seguinte, as quatro operadoras de telecomunicações do país receberam uma ordem por escrito, que citava a base legal, vinha assinada pelo órgão competente responsável e detalhava as sanções que o descumprimento poderia acarretar. Em seguida, a ordem foi publicada em um jornal pan-africano. As empresas cumpriram a ordem e suspenderam os serviços de SMS até o dia 24 de julho. A empresa aprendeu várias importantes lições com esse evento, como a importância de cooperar com outras empresas ao atender demandas governamentais que pareçam irregulares, e que a transparência facilita o cumprimento das ordens pelas empresas. (Telecommunications Industry Dialogue, 2016. "Input to UN Rapporteur David Kaye")

2) Na AT&T, pedidos como esses são avaliados por funcionários (incluindo o jurídico da empresa e, quando necessário, advogados locais que conhecem a legislação pertinente) devidamente treinados para confirmar que os pedidos são legítimos, foram emitidos por uma autoridade competente e estão de acordo com o marco regulatório local. A empresa rejeita pedidos de governos que não atendam a esses critérios. Sempre que apropriado, a empresa busca esclarecimentos, solicita modificações aos pedidos ou contesta as exigências perante o governo ou judicialmente na instância apropriada. Esses esforços ajudam a reduzir possíveis repercussões de pedidos de governos sobre a privacidade dos clientes da AT&T e sobre a capacidade dos mesmos de se comunicar e de acessar informações. (Telecommunications Industry Dialogue, 2016. "Input to UN Rapporteur David Kaye")

3) A Millicom encontrou dificuldades relacionadas à segurança na América Central em 2015. No ano anterior, autoridades da Guatemala, El Salvador e Honduras haviam adotado leis que obrigavam as operadoras de telecomunicações a desligar ou reduzir a capacidade de seus serviços dentro e em torno de penitenciárias, pois as autoridades suspeitavam que quadrilhas operavam de dentro dos presídios usando dispositivos móveis contrabandeados. Inicialmente, as operadoras foram solicitadas a desligar as torres que cobriam grandes áreas. Isso afetaria populações que viviam nas adjacências das penitenciárias e prejudicaria outras atividades que elas realizavam no dia a dia, como o uso de caixas eletrônicos.

   A empresa dialogou ativamente com as autoridades e outras entidades do setor para encontrar outras soluções que resolvessem o problema de uma forma que não afetasse as pessoas que viviam em áreas próximas aos presídios. A cobertura em torno dos presídios foi modificada, foram adotadas outras soluções que interferiam nos sinais de modo a restringir o sinal apenas em determinadas áreas e alguns presídios foram movidos para locais mais afastados de áreas densamente povoadas.

   Com isso, Guatemala e Honduras conseguiram, ao final de 2015, restringir o sinal de celular de maneira mais seletiva, afetando apenas o interior dos presídios. (Millicom, 2016. "Law Enforcement Disclosure Report 2016")

Registro obrigatório de SIM cards pré-pagos

A terceira área de segurança pública que foi amplamente debatida em anos recentes é o registro obrigatório de SIM cards pré-pagos. Esse é requerimento para que os usuários comprovem sua identidade no ponto de venda de um SIM card pré-pago para utilizar serviços de redes móveis.

Já foi prática comum para muitas operadoras móveis,[71] especialmente as que haviam acabado de entrar em um mercado, a distribuição de SIM cards gratuitos para clientes em potencial. Algumas distribuíam cartões em cada esquina — literalmente. Em seguida, os clientes adquiriam crédito por um cupom pré-pago e podiam usar o SIM card e o número de telefone.

Alguns governos acreditam que isso permitiria que criminosos se aproveitassem desse anonimato para praticar atividades ilegais como pedir resgate por pessoas sequestradas ou planejar ataques terroristas. Esse anonimato foi visto como sendo capaz de reduzir a capacidade de atrelar um SIM card ao real usuário. Muitos governos reagiram exigindo que as operadoras móveis registrem os dados de todos os seus clientes (atuais e futuros).

Quando se tentou adotar essa medida, ela produziu diversos efeitos não intencionais:

- Pessoas que não possuíam documentos, muitas vezes as mais pobres e mais vulneráveis da sociedade, ficaram excluídas do acesso a serviços móveis. Dependendo do país e da disponibilidade de documentos de identidade, isso pode ser uma barreira significativa[72]
- O furto de dispositivos móveis aumentou. Surgiu um mercado negro de SIM cards[73] roubados ou adulterados para alguns usuários, inclusive criminosos, que buscavam permanecer anônimos.
- Preocupações crescentes dos usuários com acesso, segurança e armazenamento de dados pessoais, principalmente se não houver leis de proteção da privacidade e da liberdade de expressão[74]

Estudo de caso

Colaboração no setor

Em 2012, a Comissão de Comunicações de Uganda anunciou que as operadoras móveis deveriam bloquear todos os SIM cards não registrados até o dia 31 de agosto de 2013 (prazo final).

Para cumprir esse prazo, as operadoras móveis Airtel e Warid lançaram campanhas inovadoras para incentivar mais pessoas a se registrarem. Além de enviar lembretes por SMS a informando o prazo final a seus clientes, elas ofereceram minutos e mensagens de texto de graça a quem se registrasse antes do prazo. Os consumidores também tiveram a opção de fazer um registro parcial, registrando o número de seu celular por meio de uma ligação gratuita e, assim, evitar que o SIM card fosse desativado no prazo previsto. Essa opção de registro parcial permitia que os clientes informassem que seus SIM cards estavam ativos e, com isso, eles ganhavam mais tempo para fazer o registro pessoalmente, mesmo que perdessem o prazo.
(GSMA, 2013. "Registro obrigatório de usuários de SIM cards pré-pagos: White Paper")

71. O registro de usuários de operadoras inclui também operadoras que prestam serviços de comunicação mas não são proprietárias da rede, como as operadoras de redes móveis virtuais (MVNO) e outras operadoras móveis licenciadas (MOLO)
72. GSMA, 2016. "Registro obrigatório de SIM cards pré-pagos: Desafios e melhores práticas"
73. GSMA, 2013. "Registro obrigatório de usuários de SIM cards pré-pagos"
74. Ibid.

Cada vez mais governos vêm introduzindo o registro obrigatório de SIM cards pré-pagos. Os principais objetivos são combater o terrorismo e aumentar a eficiência das atividades policiais.[75] Entretanto, até agora não há nenhuma evidência empírica de que o cadastro obrigatório de SIM card pré-pago ajude a reduzir a criminalidade.[76] Embora não haja evidência empírica, muitos governos acreditam que o registro obrigatório de SIM cards ajuda no combate ao crime e ao terrorismo. Geralmente, os custos de adotar o registro obrigatório de usuários SIM cards pré-pagos recaem sobre as operadoras. Esses custos podem ser significativos, o que pode afetar a capacidade das operadoras móveis de investir em atender usuários com menor perfil de consumo. Alguns países como o Reino Unido[77] analisaram esses programas e concluíram que os custos à sociedade (em burocracia e bancos de dados de registro) superam os benefícios e, portanto, optaram por não adotar essa política. Decisões como essa dependem tanto da situação de cada país como dos problemas que se deseja enfrentar com o registro.[78]

Uma vantagem do registro de SIM card é que ele permite que os consumidores acessem serviços móveis e digitais que não estão disponíveis para usuários não registrados, como serviços financeiros, identificação digital e serviços de governo digital (e-government). Para disseminar esses benefícios e levar valor aos consumidores, as operadoras móveis e governos precisam oferecer serviços que incentivem os consumidores a se cadastrarem voluntariamente.

Políticas de registro obrigatório podem ter consequências não intencionais e negativas, mas o registro voluntário de SIM cards pode ajudar a trazer mais benefícios para o consumidor. Nenhum desses benefícios e resultados depende de que o registro de SIM cards seja obrigatório. Ao contrário: é possível obter esses benefícios por meio do registro voluntário de usuários que escolhem registrar seus SIM cards pré-pagos para obter acesso a serviços que consideram úteis, como dinheiro móvel, comércio eletrônico ou serviços de governo. Ainda assim, o registro voluntário requer que os consumidores tenham acesso a documentos que comprovem sua identidade.

Estudo de caso

Alternativas ao registro: o caso do México

Em 2009, o México introduziu um programa de registro obrigatório de SIM card, chamado RENAUT, para combater atividades criminosas.

Quando as regras do RENAUT entraram em vigor, surgiram muitas preocupações sobre privacidade e segurança de dados. Além disso, muitas pessoas não podiam ser registradas porque não possuíam documentos de identidade e os prazos eram curtos demais. A solução não só não resolveu os problemas de criminalidade, mas aumentou os furtos de dispositivos móveis.

Após discutir a questão com empresas do setor, academia e ONGs, o programa RENAUT foi interrompido em 2012. O banco de dados foi desativado, e os vultosos investimentos das operadoras móveis e das autoridades foram relegados a fundo perdido. Uma alternativa foi adotada na Lei de Telecomunicações e Radioteledifusão, promulgada em 2014, de forma mais apropriada à situação do mercado mexicano.

A nova Lei de Telecomunicações e Radioteledifusão e outros dispositivos regulatórios não exigem que os usuários forneçam informações para registro antes de usar serviços pré-pagos. Em vez disso, a lei utiliza as várias obrigações das operadoras móveis (por exemplo, interceptação por ordem judicial) para ajudar o governo em atividades de segurança e combate à criminalidade.

(GSMA, 2016. "Registro obrigatório de SIM cards pré-pagos: Desafios e melhores práticas")

5

75. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Registro obrigatório de SIM cards pré-pagos"
76. GSMA, 2016. "Registro obrigatório de SIM cards pré-pagos: Desafios e melhores práticas"
77. Lord West de Spithead, no Parlamento, respondendo à pergunta do Visconde Waverley sobre o registro obrigatório de usuários de SIM cards: https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones
78. GSMA, 2016. "Registro obrigatório de SIM cards pré-pagos: Desafios e melhores práticas"

Quando o registro obrigatório é adotado, os clientes precisam ser informados de que precisam registrar seus SIM cards, o que precisam fazer e quais as consequências do descumprimento (por exemplo, desativação do SIM card). Nesse caso, o registro de SIM card deve ser implementado de forma pragmática e apropriada para a situação do mercado local, observando aspectos como o acesso a documentos de identidade oficiais, a qualidade e disponibilidade dos registros civis de identidade e a capacidade das operadoras de verificar os documentos de identidade dos consumidores.

Principais implicações para governos, entidades do setor e demais partes interessadas

O registro de SIM cards pré-pagos pode oferecer valiosos benefícios para os consumidores e para os cidadãos em geral, mas não deve ser tornado obrigatório. Os governos que optarem pelo registro obrigatório de usuários de SIM cards pré-pagos devem considerar as melhores práticas globais e criar mecanismos flexíveis, proporcionais e relevantes para o mercado em que serão usados, incluindo o nível de penetração de documentos de identidade oficiais.[79]

Quando essas condições são atendidas, o registro de SIM card tem mais chances de ser eficaz e de produzir dados mais precisos sobre os consumidores. Além disso, um sistema robusto de verificação e autenticação do consumidor pode permitir que as operadoras móveis facilitem a criação de soluções de identidade digital, ajudando os consumidores a ter acesso a diversos serviços, baseados em redes móveis ou não. Como o volume de usuários é grande em todos os países, deve-se analisar cuidadosamente a magnitude dessa tarefa e o tempo necessário para registrar os usuários, a fim de minimizar o impacto sobre os consumidores e possíveis interrupções do serviço.

A GSMA acredita que os governos que vêm pensando em introduzir ou rever suas políticas de registro obrigatório de SIM card devem tomar as seguintes medidas antes de finalizar seus planos:

- Discutir, colaborar e se comunicar com as operadoras móveis antes, durante e depois da implementação
- Considerar tanto as necessidades de segurança do país como os direitos dos cidadãos, sobretudo quando o governo deseja exigir o registro de SIM cards por motivos de segurança
- Garantir que existam salvaguardas e um marco legal apropriado para proteger os dados e a privacidade dos clientes
- Definir cronogramas exequíveis para o planejamento, teste e implementação de processos de registro
- Dar clareza e segurança sobre as necessidades de registro antes de qualquer implementação
- Permitir e/ou incentivar a armazenagem de registros eletrônicos e desenvolver processos de registro fáceis de usar
- Permitir e incentivar que usuários com SIM card registrado possam ter acesso a outros serviços digitais
- Apoiar as operadoras móveis na implementação de programas de registro de SIM card, contribuindo em campanhas conjuntas de comunicação e reduzindo custos operacionais

79. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Registro obrigatório de SIM cards pré-pagos"

Tema em foco

Parcerias público-privadas para implementar o registro de Sim cards na América Latina

Em 2009 no Equador e em dezembro de 2016 na Argentina, as agências regulatórias (CONATEL e ENACOM, respectivamente) solicitaram verificação cruzada e validação dos procedimentos de registro de SIM de todos os clientes junto a um órgão de registro público ou privado. Nesses dois casos, a Telefónica trabalhou junto ao governo para instalar uma solução apropriada para os consumidores que atendesse às necessidades do governo.

No Equador, a Telefónica instalou um processo de registro através de um sistema automático chamado Unidade de Resposta Audível (URA). O serviço de voz era melhor que o procedimento anterior, no qual a identidade do consumidor era verificada no Registro Civil.

Na Argentina, a Telefónica desenvolveu um aplicativo que era ativado assim que um SIM card era introduzido no dispositivo móvel. O aplicativo coleta informações sobre o SIM card e a identidade do usuário. Esse sistema digital vem sendo usado para criar um banco de dados com informações que identificam o proprietário de cada SIM card.

Dessas experiências de trabalho conjunto com órgãos de governos, a Telefónica aprendeu três importantes lições:

1. O registro de SIM card pode ser validado de diversas maneiras diferentes. As operadoras móveis devem usar a solução que considerarem mais apropriada.
2. Toda implementação de sucesso depende de um cronograma bem planejado. Por exemplo, no Equador as operadoras móveis e o regulador trabalharam em conjunto para implementar uma "fase de estatística", que permitiu avaliar as reais necessidades e evitar a regulamentação excessiva
3. Apenas uma estreita parceria público-privada entre operadoras e governos pode analisar corretamente as alternativas de implementação e desenvolver aquela que melhor atende às necessidades de todos os envolvidos de forma equilibrada.

5

6 Segurança de rede e integridade dos dispositivos

O uso seguro de dispositivos móveis requer uma rede com infraestrutura segura. Em sua forma mais simples, isso significa que as operadoras precisam cuidar da integridade das comunicações que passam por suas redes. Para isso, é preciso manter a segurança de elementos críticos (hardware, software e dados) e evitar o acesso não autorizado ou invasão dos nós que formam as redes. Para o usuário, o dispositivo móvel é o principal ponto de acesso à rede. Assim, tornou-se essencial proteger também a integridade dos dispositivos móveis. Por princípio, as redes móveis precisam ficar acessíveis a uma ampla gama de usuários, que usam os mais diversos dispositivos e protocolos de conexão. Elas também precisam se interconectar com diversas outras redes de comunicação no mundo inteiro — fixas, móveis, provedores de internet e redes corporativas — para oferecer conectividade a toda hora e em todos os lugares. Em resumo, proteger uma rede é muito complexo na prática.

A infraestrutura de redes de telecomunicação foi concebida originalmente como um sistema fechado e seguro. Onde havia interconexão entre as redes, o que geralmente ocorria em fronteiras (na maioria dos países, as primeiras operadoras eram monopólios estatais), isso era feito de forma transparente, bilateral e com base na confiança mútua. Desde então, a tecnologia avançou, o mundo se tornou muito mais conectado e as redes se multiplicaram. Hoje em dia, qualquer telefonema pode passar por várias redes, e muitas transmissões de dados passam por diversos trajetos em uma única comunicação. Isso criou várias vulnerabilidades em potencial. Dessa forma, todas as operadoras e o ecossistema amplo ecossistema precisam se manter vigilantes para enfrentar essas ameaças.

A Figura 6 resume diversas ameaças à integridade das redes, as quais poderiam permitir interceptação não autorizada, falsificação de identidade ou interrupção do serviço. A indústria móvel vem respondendo a essas novas ameaças. As principais medidas são promover a segurança da rede, incentivar um debate transparente sobre o equilíbrio entre conveniência e segurança e criar recursos e protocolos de segurança cada vez mais sofisticados à medida que cada nova geração de redes móveis é desenvolvida e instalada.

Esta seção do relatório trata de diversos problemas de segurança que afetam redes e dispositivos e podem comprometer a segurança necessária para manter o sigilo e a segurança das comunicações dos clientes.

- Segurança de redes
- Integridade dos dispositivos móveis
- A evolução futura das redes

Todas essas questões, que têm importantes repercussões para os governos, para as empresas e demais partes interessadas, serão aprofundadas neste capítulo.

Segurança de rede e integridade dos dispositivos

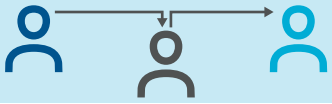
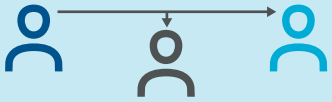
Os membros do ecossistema precisam colaborar entre si e também com órgãos de segurança pública no mundo inteiro para compartilhar informações sobre ameaças e responder a ataques a redes e dispositivos móveis, além de identificar os autores. Isso requer tanto o engajamento das grupos já existentes de resposta a incidentes como a criação de novos grupos, conforme necessário, para cobrir lacunas existentes. Quando necessária, a regulamentação deve ser aplicada de forma consistente a todos as empresas da cadeia de valor, de forma consistente e neutra em termos de tecnologia e serviço, e sem prejudicar o modelo multistakeholder de governança e inovação na internet. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras se esforçarão para proteger a infraestrutura para garantir que os consumidores recebam os serviços de comunicação mais seguros e confiáveis. Para isso, serão adotadas as seguintes medidas:

- **Adotar providências para garantir a segurança da infraestrutura de rede que operamos e controlamos**
- **Promover parcerias público-privadas para minimizar os riscos de ataques de hackers ou de uso da rede para fins mal-intencionados por meio de abordagens coordenadas em nível global**
- **Definir claramente por quais elementos da infraestrutura as operadoras são responsáveis e os limites de atuação das mesmas em relação a outros elementos da infraestrutura ou da prestação de serviços**

Figura 6

Proteção das redes

OBJETIVO DE SEGURANÇA	DESCRIÇÃO DA AMEAÇA	EXEMPLO DE ATAQUE
INTEGRIDADE — EVITAR ADULTERAÇÃO DOS DADOS	ADULTERAÇÃO NÃO AUTORIZADA	INTERMEDIÁRIO 
CONFIDENCIALIDADE — PRIVACIDADE DE DADOS	ACESSO NÃO AUTORIZADO	ESCUTA 
DISPONIBILIDADE — MANTER A REDE SEMPRE DISPONÍVEL PARA OS USUÁRIOS LEGÍTIMOS	DESTRUIÇÃO, FURTO, RETIRADA OU PERDA DE DADOS E INDISPONIBILIDADE DA REDE	NEGAÇÃO DE SERVIÇO (DoS) 

Segurança de rede

Infraestrutura física da rede

A segurança das redes móveis deve começar pela estrutura física, como torres, backhaul e os componentes básicos da estrutura da rede. Por exemplo, as redes possuem algumas funções-chave, como o registro de usuários autorizados, as quais precisam ser protegidas porque seu comprometimento, tanto por ataques maliciosos como por falhas técnicas, prejudicaria toda a rede. As operadoras móveis e fornecedores de equipamentos continuam desenvolvendo e instalando novas soluções para tornar os sistemas mais robustos. Esses esforços vêm sendo bem-sucedidos, mas eles requerem investimentos constantes no desenvolvimento e instalação de novas funções e recursos.

O uso de estações radiobase falsas, também chamadas IMSI (international mobile subscriber identity) catchers, é uma vulnerabilidade baseada na ausência de autenticação mútua de tecnologias 2G e em funções que fazem com que aparelhos 3G ou 4G se conectem automaticamente a redes 2G. Estações radiobase falsas induzem dispositivos móveis em sua área de alcance a se conectarem a elas e não à rede legítima. Após a conexão, o operador da estação falsa roteia a chamada. Esses ataques com "intermediário" criam diversas possibilidades de interceptação, rastreamento do local, fraude e negação de serviço. Legisladores como o Comitê de Supervisão e Reforma Governamental dos EUA estão elaborando recomendações sobre como se proteger contra o uso não autorizado desses dispositivos.[80] As operadoras móveis podem utilizar as medidas padronizadas de segurança de rede para ajudar a reduzir os riscos, e a GSMA criou orientações para ajudar as operadoras.

Comunicações pelas redes

A tecnologia empregada em redes móveis é atualizada regularmente, e a introdução de melhorias é planejada com antecedência. A infraestrutura recebeu investimentos elevados e frequentes, que contribuíram significativamente para tornar a infraestrutura da rede bastante robusta. É essencial manter a capacidade de investimento em face de mudanças na legislação ou regulamentação, as quais mudam para responder às diferentes ameaças.

Em 1991, o lançamento das redes de segunda geração (2G) introduziu o uso de modulação digital, que proporciona proteção robusta e segurança. O padrão GSM, que é usado em muitas redes 2G, emprega a tecnologia SIM (Subscriber Identity Module) para autenticar os usuários e administrar o faturamento, além de implementar criptografia no nível dos dispositivos para proteger os usuários contra interceptação e outros ataques. O conceito físico do SIM, baseado na tecnologia de smart cards, mostrou-se bastante robusto, e continua sendo um componente essencial das redes 4G. No futuro, surgirão outras inovações como o SIM embarcado.[81]

As redes 2G foram projetadas principalmente para suportar comunicações de voz, mas possuíam recursos básicos de transmissão de dados e introduziram o serviço de mensagens SMS, que se tornou bastante popular. No início dos anos 2000, foram lançadas as redes 3G, que foram as primeiras em que a transmissão de dados era um dos principais recursos. Foram introduzidos navegação na web em banda larga, integração multimídia e diversos recursos de segurança.

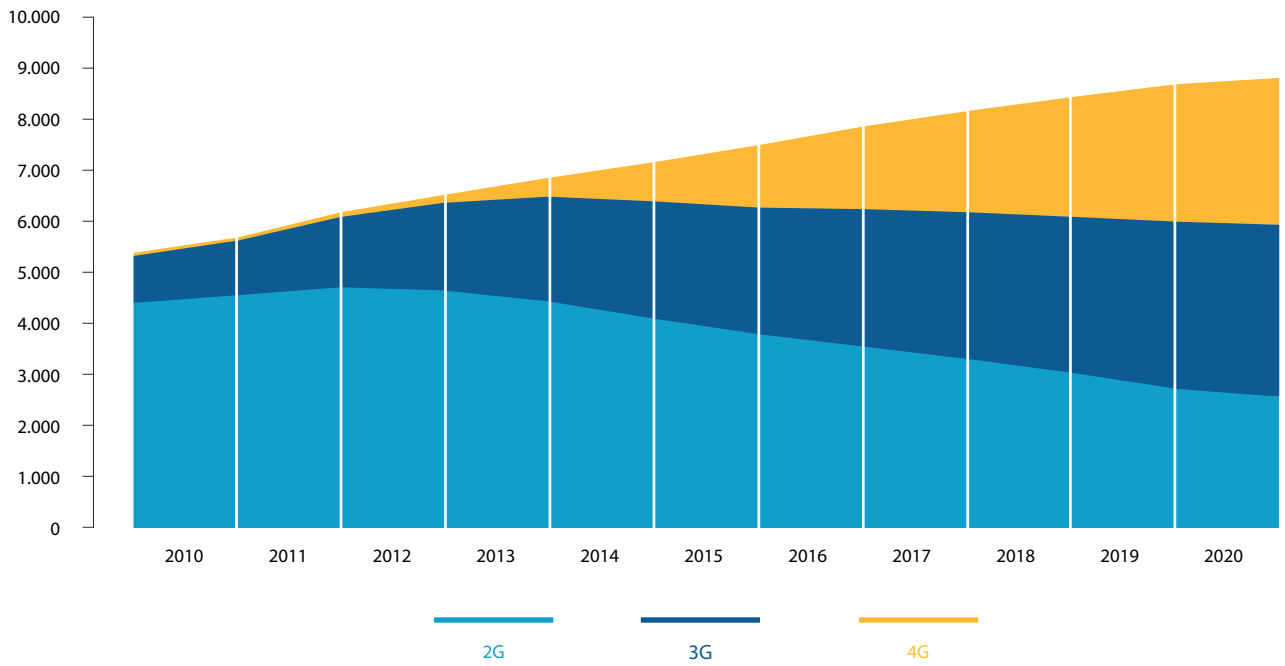
80. Committee on Oversight and Government Reform, 2016. "Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations"
81. O SIM embutido é um chip instalado em dispositivos móveis que proporciona o mesmo nível de segurança que a tecnologia SIM disponível atualmente. O novo chip é mais flexível porque permite baixar os perfis das operadoras, permitindo aos usuários mudar de operadora sem precisar trocar fisicamente o chip. Essa possibilidade é especialmente relevante para dispositivos que interagem com outras máquinas (interação máquina-máquina ou M2M). Consulte http://www.gsma.com/newsroom/press-release/leading-m2m-alliances-back-the-gsma-embedded-sim/

Contudo, foram encontradas falhas de segurança no protocolo Signalling System Number 7 (SS7) da UIT e em outros protocolos de interconexão usados para rotear chamadas de voz e suportar serviços entre e dentro de redes. Essas vulnerabilidades podem expor as redes móveis e seus clientes a diversas vulnerabilidades como escuta, identificação da localização ou interceptação de dados. Recursos de monitoramento, detecção e bloqueio existem para proteger os protocolos de interconexão e mensagem contra esses riscos. A GSMA reconhece que, para reduzir esses riscos, as operadoras móveis precisam se unir e agir de forma abrangente. O Grupo de Segurança e Fraude da GSMA vem trabalhando intensamente para orientar operadoras sobre como reduzir os riscos de segurança associados ao SS7.[82] As operadoras também precisam adotar todas as precauções necessárias para se proteger contra a interceptação de dados sensíveis, incluindo credenciais de acesso de assinantes.

Os padrões de comunicações móveis de quarta geração (4G) oferecem acesso móvel de banda larga através de smartphones e outros dispositivos. A adoção de redes 4G (Figura 7) introduziu um sistema baseado inteiramente no protocolo IP (Internet Protocol). Isso resolve a vulnerabilidade do SS7 quando implementado entre operadoras, mas a instalação de novos protocolos gera outros desafios de segurança. Para reduzir a vulnerabilidade dessas redes, é preciso garantir que os recursos de segurança previstos nos padrões sejam devidamente instalados e configurados. A GSMA oferece orientações sobre como fazê-lo.

Figura 7

Conexões globais por tipo de tecnologia (milhões, exceto M2M)



82. Para saber mais, acesse: http://www.gsma.com/newsroom/all-documents/ir-70-sms-ss7-fraud/

Outro desafio comum são os chamados gateways GSM, também chamados "SIM Boxes". Os gateways GSM podem permitir que terceiros não autorizados interfiram no roteamento de chamadas para usuários de redes móveis, o que gera preocupações com a segurança. Os gateways GSM normalmente não suportam identificação de chamada (CLI, ou calling line identity). Por isso, os serviços que dependem de CLI se tornam indisponíveis para usuários cujo tráfego é roteado por gateways GSM (por exemplo, um serviço pode ser negado a clientes com aparelhos pré-pagos que precisam adquirir mais créditos). A falta de identificação por CLI também pode dificultar a interceptação por ordem judicial e impedir que as operadoras cumpram suas obrigações legais nos mercados nos quais possuem licenças. Devido a seus efeitos sobre a disponibilidade do serviço e a segurança em geral, os gateways GSM são ilegais em alguns mercados. Quando permitido, as operadoras móveis são incentivadas a adotar medidas que evitem o uso de gateways por terceiros.

As operadoras móveis continuam enfrentando ameaças às suas redes e a seus consumidores, mas as operadoras de outras redes públicas (por exemplo, hotspots de WiFi em locais públicos) também devem estar preparadas para enfrentar essas ameaças. Operadoras e consumidores precisam adotar proteções apropriadas (como o VPN) para zelar pela segurança do ecossistema de comunicações.

Principais implicações para governos, entidades do setor e demais partes interessadas

Nenhuma tecnologia de segurança é absolutamente inviolável, mas as redes e serviços GSM não sofrem ataques com frequência. Ataques como esses exigem muitos recursos, como equipamentos especializados, capacidade de processamento e capacidade técnica de que a maioria dos indivíduos e organizações não possui.[83]

Superar a segurança de redes móveis é muito difícil. A GSMA considera que as pesquisas sobre possíveis vulnerabilidades geralmente são de natureza acadêmica.[84] Entretanto, mudanças na tecnologia e o surgimento de novas ameaças e fontes e ataques exigem que o setor adote uma abordagem ainda mais proativa para proteger as redes no futuro:

- A indústria móvel precisa manter mecanismos apropriados, oferecer ferramentas e oportunidades para facilitar o compartilhamento de informações sobre ataques e garantir a disseminação rápida de informações relacionadas a incidentes. Essas iniciativas podem contar com a participação de reguladores e órgãos do governo como os Grupo de Respostas a Incidentes de Segurança (CERTs).
- A indústria precisa agir coletivamente para proteger redes e os consumidores a elas conectadas. Para isso, é preciso desenvolver padrões consistentes e baseados em consenso, e utilizar de forma proporcional recursos como monitoramento, detecção e bloqueio.
- Manter a segurança de redes e serviços móveis é uma atividade complexa, que requer várias decisões de operadoras móveis e seus fornecedores para implementar corretamente os padrões de segurança, instalar e configurar diversos recursos. A GSMA orienta seus membros sobre como obter os melhores níveis de segurança e continua definindo os requisitos básicos de segurança a serem cumpridos por todas as operadoras móveis.
- A segurança é um desafio constante, que deverá crescer ainda mais com a evolução para tecnologia 5G, mas também cria oportunidades de repensar a segurança e encontrar maneiras de melhorá-la.

Quando necessária, a regulamentação deve ser aplicada de forma consistente a todos os membros da cadeia de valor, neutra em termos de serviço e tecnologia, e sem prejudicar o modelo em que vários participantes contribuem para a governança e a evolução da internet.

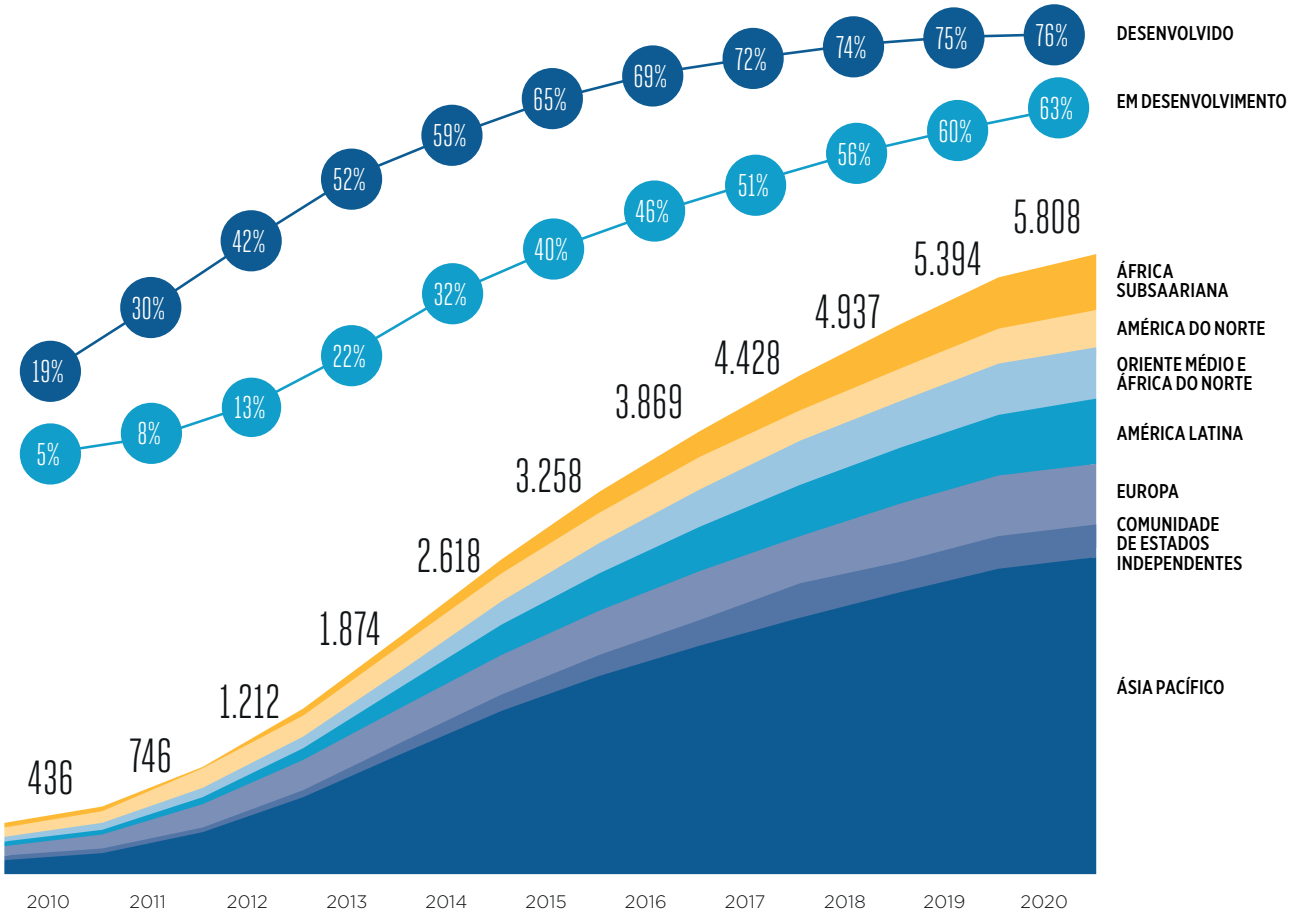
83. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Segurança de redes móveis"
84. Ibid.

Integridade dos dispositivos móveis

À medida que são instaladas redes 3G, 4G e, futuramente, 5G, cada vez mais smartphones e outros dispositivos móveis vêm sendo adquiridos. Até 2020, espera-se que 2 de cada 3 novas conexões em mercados emergentes e 3 de cada 4 quatro em mercados desenvolvidos sejam conexões de smartphone (ver Figura 8). Os fornecedores de aplicativos vêm analisando como os smartphones poderão, talvez por meio de módulos conectáveis, substituir dispositivos dedicados para uso em hotspots e outros ambientes sensíveis. Além disso, até 2020 haverá pelo menos um bilhão de conexões máquina-máquina (M2M) em lares, fábricas, transportes e outros setores, que corresponderão a pelo menos 10% do mercado global de redes móveis.[85]

Figura 8

Conexões e adoção de smartphones no mundo (em milhões)



85. GSMA, 2014. "Cellular M2M forecast and assumptions: 2010–2020"

Consumidores e empresas que utilizam esses serviços correm o risco de que redes mal gerenciadas se tornem mais vulneráveis, e a invasão dessas redes pode atingir grandes grupos de usuários.

Todas as tecnologias estão sujeitas a ameaças de segurança, incluindo as tecnologias móveis. Os dispositivos móveis são visados por diversos motivos. Como os dispositivos são valiosos para ladrões (pois têm preço relativamente alto e são pequenos), o crime organizado frequentemente buscar alterar o IMEI[86] de dispositivos roubados para reativá-los depois que o crime é comunicado. Outros criminosos usam malware para realizar atividades que podem prejudicar os usuários, geralmente por meio de furto de identidade e fraudes assemelhadas.[87]

Talvez a ameaça mais grave seja a de ataques premeditados e sistemáticos em grande escala para derrubar redes inteiras, prejudicando assim a todos os usuários. Existe ainda o risco de que invasões de dispositivos móveis (por exemplo, por malwares ou e-mails de phishing) sirvam como ponto de entrada para invadir outros dispositivos móveis, que são então explorados para atacar redes IP. Por exemplo, em 21 de outubro de 2016 houve um ataque contra a Dyn, um importante controlador da estrutura de nomes de domínio[88]. O ataque se originou de um malware em um computador, que se espalhou para outros dispositivos e criou uma rede de máquinas infectadas (botnet), que por sua vez foi usada para perpetrar um ataque distribuído de negação de serviço (DDoS).[89] Em uma escala ainda maior, uma abordagem semelhante pode inundar uma rede móvel baseada em IP com tráfego, sobrecarregando a rede e comprometendo sua estabilidade. Para evitar ataques como esses, operadoras móveis e órgãos de segurança pública precisam desenvolver conjuntamente um abrangente plano de segurança, pois as redes móveis não são o único ponto que um atacante pode explorar.

A GSMA ajudou a desenvolver mecanismos de proteção como os descritos nas GSMA IoT Connection Efficiency Guidelines[90] para proteger redes móveis contra a utilização em massa de dispositivos IoT ineficientes, inseguros ou defeituosos em suas redes. A GSMA também incentiva seus membros a disseminar atualizações de segurança críticas o mais rapidamente possível.

Principais implicações para governos, entidades do setor e demais partes interessadas

Todos os fornecedores do setor devem adotar boas práticas de segurança. Programas de certificação de fornecedores como o Security Accreditation Scheme[91] da GSMA garantem que o compromisso com a segurança seja incentivado e possa ser comprovado. A GSMA certifica a segurança de fornecedores e de seus produtos há bastante tempo por meio de iniciativas como o Security Accreditation Scheme (para mensagens SIM) e o programa para fabricantes originais de equipamento (OEMs) de infraestrutura.

A GSMA também procura ajudar provedores de internet e desenvolvedores de aplicativos que operam na rede, e que são responsáveis por impedir que sejam explorados como canal para violação da integridade de redes móveis.

A GSMA promove padrões globais de segurança para novos serviços e reconhece que sistemas de segurança baseados em SIM são uma alternativa válida a recursos de segurança embutidos em aparelhos ou instalados em cartões de memória externos (microSD), pois os SIM cards vêm se mostrando resistentes a ataques.[92]

6

86. O IMEI e outros tópicos relacionados ao furto de dispositivos móveis são discutidos mais detalhadamente na Seção 3. Proteção ao consumidor
87. Esses assuntos são discutidos mais detalhadamente no capítulo Proteção ao Consumidor
88. Dyn é o servidor de endereços de nomes de domínio (DNS) de fornecedores de serviços pela internet como Twitter, Amazon, AirBnB e Spotify. Após cada ataque, a Dyn conseguiu restaurar seus serviços e evitou uma queda de todo o sistema. Um terceiro ataque foi rechaçado e não afetou em nada os consumidores. A declaração pública está disponível em http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
89. USA Today, 2016. "Hacked home device caused massive Internet outage"
90. Para saber mais, acesse http://www.gsma.com/connectedliving/gsma-iot-device-connection-efficiency-guidelines/
91. Para saber mais, acesse http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
92. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: Segurança de redes móveis"

A evolução futura das redes

A internet das coisas (IoT) se refere a um conjunto de desenvolvimentos no qual diversos dispositivos são conectados à internet, desde carros a eletrodomésticos. Esses dispositivos se conectam a diversas redes, incluindo redes Wi-Fi, redes dedicadas de curto alcance e até redes móveis, usando faixas licenciadas ou não-licenciadas de espectro. Por exemplo, na próxima geração de tecnologia de redes móveis, a virtualização da função de rede e o 5G serão partes importantes da conectividade IoT, trazendo uma era de banda larga ainda mais rápida e abrindo caminho para serviços especialmente otimizados para redes 5G. Esses serviços otimizados podem incluir suporte para tecnologias de ponta, como internet por toque, realidade virtual e novos serviços de difusão.

Segurança na internet das coisas

A internet das coisas criou enormes oportunidades, tanto para o setor móvel como para muitos outros. Com o surgimento de novos parceiros empresariais e fornecedores de equipamentos, é essencial que a segurança tenha lugar de destaque nas mentes de quem entra nesse novo espaço comercial. Muitos dispositivos e equipamentos que antes não eram conectados a nenhuma rede agora precisam de proteções apropriadas, que devem ser embutidas no equipamento e nos serviços desde o início. Isso requer que fornecedores e desenvolvedores que nunca lidaram com essas questões introduzam rapidamente medidas de segurança poderosas e sofisticadas. A GSMA criou diretrizes de segurança para a internet das coisas[93] e um esquema de autoavaliação de segurança[94] para diversos membros do ecossistema.

Os padrões e protocolos 5G, inclusive os relacionados à segurança de rede, vêm sendo desenvolvidos de forma a incluir essa tecnologia. A GSMA vem liderando a iniciativa de identificar e priorizar os requerimentos, e de garantir que eles sejam considerados e embutidos nos novos padrões técnicos. Mas isso aborda apenas uma parte da internet das coisas. Será preciso muito esforço e atenção para garantir a segurança dos vários componentes em uma estrutura fortemente interconectada com vários componentes e serviços.

Principais implicações para governos, entidades do setor e demais partes interessadas

A GSMA busca ter uma atuação relevante no desenvolvimento estratégico, regulatório e comercial da internet das coisas e do ecossistema 5G.[95]

- A GSMA reconhece que deverá participar ativamente da coleta e priorização dos requerimentos de segurança padronização da segurança em redes 5G. O tema já está sendo discutido. A GSMA e seus membros convidaram outros especialistas da área e órgãos de segurança pública para participar e garantir que todas as necessidades sejam devidamente compreendidas.
- Os governos devem apoiar a natureza global das redes, em que uma variedade cada vez maior de dispositivos se conectará à internet. É preciso trabalhar em várias jurisdições para garantir consistência e clareza na regulação e nas obrigações de segurança de rede para todas as partes envolvidas nesse setor complexo.
- A indústria móvel continuará interagindo com o ecossistema como um todo e promoverá investimentos apropriados, tanto diretamente como por meio de fornecedores e parceiros no ecossistema, para manter a segurança de redes e dispositivos à medida que a tecnologia evolui, sobretudo em relação à transição para a virtualização de funções de rede e o 5G.

6

93. Para saber mais sobre as diretrizes de segurança para internet das coisas da GSMA, acesse http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
94. Para saber mais sobre a autoavaliação sobre segurança da internet das coisas da GSMA, acesse http://www.gsma.com/connectedliving/iot-security-self-assessment/
95. GSMA, 2016. "Manual de Políticas Públicas de Telecomunicações Móveis: 5G, a próxima geração"

6

7 Princípios de segurança e privacidade para a indústria móvel

Como parte de seu trabalho constante para promover a segurança, privacidade e sigilo, a GSMA e as operadoras membro reconhecem que é preciso adotar uma abordagem flexível e em constante evolução para encontrar o melhor equilíbrio entre os direitos de consumidores de cidadãos e as necessidades de segurança pública, assim como definir as responsabilidades das redes móveis para promover essas duas metas. As melhores respostas atendem às necessidades e particularidades do mercado local em vez de apenas copiar o que foi feito em outro lugar. Entretanto, é evidente que deve haver colaboração e aprendizado mútuo entre os vários grupos participantes do sistema.

A GSMA e suas organizações membro estabeleceram os seguintes princípios, que norteiam o desenvolvimento de soluções para os problemas detalhados neste relatório.

Proteção ao consumidor

Para incentivar o uso dos serviços e dispositivos móveis com segurança e responsabilidade, várias partes interessadas precisam contribuir. Governos e órgãos de segurança pública devem criar o ambiente apropriado, com marco regulatório, recursos e processos para deter, identificar e levar à justiça todas as práticas criminosas. Isso muitas vezes requer cooperação em escala global. Demais membros do ecossistema (por exemplo, fabricantes de aparelhos e fornecedores de aplicativos móveis) devem participar de iniciativas que ajudem a proteger os usuários e orientá-los sobre melhores práticas para que possam continuar se beneficiando desses serviços de forma segura. As operadoras móveis podem ajudar a lembrar seus clientes sobre a importância de permanecerem atentos e vigilantes, além de usar todos os recursos de segurança disponíveis. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras agirão de forma proativa para cuidar de problemas de proteção ao consumidor relacionados a atividades ilegais ou prejudiciais que utilizam ou que dependem de uso de celulares. Serão adotadas as seguintes medidas:

- **Trabalhar em parceria com outros órgãos para fornecer soluções multilaterais apropriadas.**
- **Adotar soluções projetadas para evitar que as redes sejam usadas para cometer fraudes ou outros crimes ou que os aparelhos sejam usados de forma lesiva ao consumidor.**
- **Orientar os consumidores sobre como agir com segurança para promover a confiança no uso de aplicativos e outros serviços móveis.**

Proteção à privacidade

O principal objetivo da proteção à privacidade é promover a confiança de que os dados pessoais serão devidamente protegidos, como previsto nas as leis e marcos regulatórios de cada país. Isso requer que todas as partes envolvidas nesse ecossistema sigam uma abordagem consistente e neutra em termos de tecnologia, serviço e região. Os governos podem ajudar a garantir esse resultado sem sacrificar a flexibilidade necessária para a inovação adotando regras baseadas em riscos para preservar dados pessoais e incentivando práticas de governança digital responsáveis e alinhadas com a regulamentação local. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras adotarão medidas proativas para proteger e respeitar a privacidade dos consumidores, permitindo que eles tomem decisões informadas sobre quais dados serão coletados e sobre como seus dados pessoais serão usados. Para isso, adotarão políticas que promovem:

- **Armazenamento e processamento de dados pessoais de forma segura e de acordo com o marco regulatório aplicável.**
- **Transparência junto aos consumidores sobre dados que são compartilhados de forma anonimizada, conforme determinado pelo marco regulatório local.**
- **Fornecimento de informações e ferramentas aos consumidores para que eles tomem decisões simples e importantes sobre a própria privacidade.**

Manutenção da segurança pública

Para cumprir as leis e obrigações regulatórias, incluindo as relativas às licenças de operação, as operadoras móveis são obrigadas a assumir a tarefa de cooperar com órgãos de segurança pública em sua missão de zelar pela proteção ao público. Os governos devem garantir que o marco regulatório seja proporcional, indicando claramente quais são os poderes dos órgãos de segurança pública no país. O marco regulatório também deve garantir que os pedidos de assistência sejam: necessários; proporcionais às necessidades de cada caso; dirigidos ao serviço de comunicações ou provedor de tecnologia mais apropriado; e compatíveis com os direitos humanos. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

Ao lidar com questões envolvendo sigilo ou segurança pública nos países onde atuam, as operadoras cumprirão todas as obrigações perante a lei ou impostas como condicionamento de licença de prestação de serviço e, ao mesmo tempo, apoiarão questões relacionadas a direitos humanos. Colaboraremos com os órgãos competentes para proteger a segurança pública adotando as seguintes medidas:

- **Trabalhar junto aos órgãos competentes quando necessário, desenvolver e adotar soluções apropriadas para atingir o objetivo com transtornos mínimos para consumidores e serviços essenciais**
- **Desenvolver redes com funcionalidades para situações de emergência e risco à segurança**
- **Expor claramente os limites da nossa atuação dentro da cadeia de valor, destacando os pontos em que outros agentes podem atuar**

Segurança de rede e integridade dos dispositivos

Os membros do ecossistema precisam colaborar entre si e também com órgãos de segurança pública no mundo inteiro para compartilhar informações sobre ameaças e responder a ataques a redes e dispositivos móveis, além de identificar os autores. Isso requer tanto o engajamento das grupos já existentes de resposta a incidentes como a criação de novos grupos, conforme necessário, para cobrir lacunas existentes. Quando necessária, a regulamentação deve ser aplicada de forma consistente a todos as empresas da cadeia de valor, de forma consistente e neutra em termos de tecnologia e serviço, e sem prejudicar o modelo multistakeholder de governança e inovação na internet. Tendo isso em mente, a GSMA e as operadoras móveis concordaram com o seguinte princípio:

As operadoras se esforçarão para proteger a infraestrutura para garantir que os consumidores recebam os serviços de comunicação mais seguros e confiáveis. Para isso, serão adotadas as seguintes medidas:

- **Adotar providências para garantir a segurança da infraestrutura de rede que operamos e controlamos**
- **Promover parcerias público-privadas para minimizar os riscos de ataques de hackers ou de uso da rede para fins mal-intencionados por meio de abordagens coordenadas em nível global**
- **Definir claramente por quais elementos da infraestrutura as operadoras são responsáveis e os limites de atuação das mesmas em relação a outros elementos da infraestrutura ou da prestação de serviços**

7

SEDE DA GSMA
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
Reino Unido
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601