Análise de Conjuntura (Working Paper), no. 2, junho de 2017.
ISSN 2359-1706



# ESTADOS x EMPRESAS DE TECNOLOGIA

Rodolpho Barnabel – Analista Pleno RAIA-ESPM

Maria Antônia Santiago– Analista Junior RAIA-ESPM

Esther Fuentes – Analista Junior RAIA-ESPM

**Estados x Empresas de Tecnologia: O dilema entre segurança e privacidade**

O terrorismo é um dos assuntos mais debatidos atualmente e seus métodos de atuação estão sempre se adaptando com as novas tecnologias, o que coloca empresas como Apple e WhatsApp no centro do debate e muitas vezes em rota de colisão com os Estados.

Recentes atentados terroristas como San Bernardino (2015) e Londres (2017) reacenderam o debate entre garantir a segurança nacional ou preservar a privacidade dos cidadãos. A preferência entre um ou outro não é fixa, mas fluida e a opinião pública é fator de alta influência para tal escolha.

O trade-off entre segurança e privacidade é um problema que remonta à origem da teoria política moderna. De tempos em tempos este debate volta à tona devido a eventos que causam grande comoção pública.

O terrorismo é um dos assuntos mais debatidos atualmente, seja pelo número de vítimas, o clima de terror que propaga nas sociedades ou as suas consequências posteriores que afetam as esferas política, econômica e social.

Um ponto particularmente preocupante quanto ao terrorismo é a sua facilidade de adaptação às novas circunstâncias do ambiente, não sendo diferente quanto às inovações tecnológicas, que influenciam o *modus-operandi* dos agentes.

Dois casos recentes reacenderam o debate entre segurança e privacidade demonstram o problema: o atentado perpetrado em San Bernardino nos EUA em dezembro de 2015 e o atentado de Londres em março de 2017. Enquanto no primeiro o iPhone de um dos atiradores foi recuperado pelo FBI, no segundo a polícia descobriu que o autor do atentado utilizara a plataforma de mensagens

WhatsApp apenas alguns minutos antes de realizar o ataque. Em ambos os casos as autoridades ficaram impedidas de prosseguir com as investigações devido aos esquemas de segurança e à criptografia dos aparelhos e seus softwares.

A partir daí os governos afetados se voltaram para as empresas de tecnologia como Apple e Facebook (detentora da plataforma WhastApp) de modo que elas fornecessem um meio de acesso aos dados destes aparelhos para continuar a investigação. O impasse entre ambos ocorreu quando tais empresas se recusaram a quebrar os esquemas de segurança dos aparelhos, alegando que isto geraria um risco futuro que afetaria a privacidade dos demais usuários. Enquanto isso, os governos afirmaram que deveria haver uma cooperação entre as empresas e os mesmos, dizendo que o monitoramento e análise de dados dos indivíduos serviriam unicamente para garantir a segurança nacional e seriam usados como parte de investigações contra atos criminosos, como o terrorismo

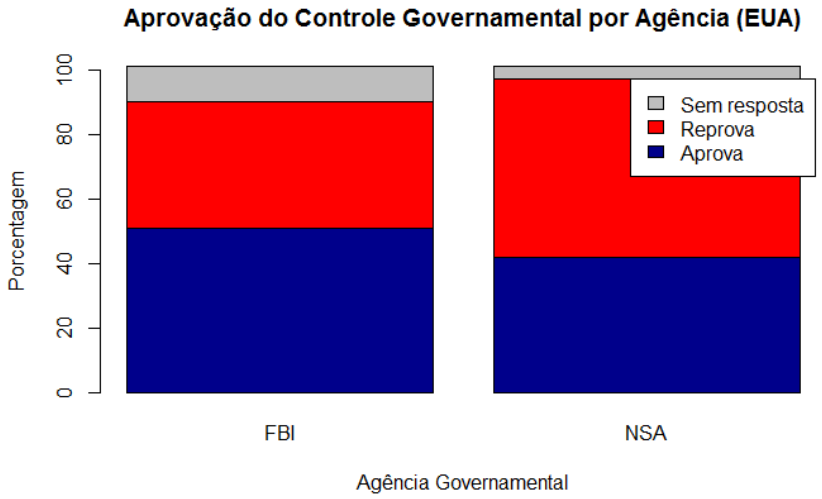
**Como a opinião pública se comporta tendo como referência o tema que mais pesa na balança: segurança nacional ou privacidade?**

Quais são os possíveis impactos desse novo cenário para as empresas de tecnologia e os seus usuários? Como a opinião pública afeta as decisões dessas companhias? Este artigo busca analisar o desenvolvimento dessa conjuntura, as suas oportunidades e probabilidades.

No momento de insegurança atual, no qual os países mais desenvolvidos, e tecnicamente mais seguros estão sendo alvos fáceis de atentados, há o crescimento do terror generalizado. Com tal crescimento, ocorre uma desvalorização rápida da privacidade: diante da sensação de insegurança nacional imediata, as pessoas recorrem ao governo, mesmo que isso signifique a perda de controle em determinadas áreas de suas vidas. Dessa forma, conseguimos perceber como a opinião pública se comporta tendo como referência o tema que mais pesa na balança na ocasião, segurança nacional ou privacidade

Isso fica explícito em dados retirados de determinadas pesquisas, como em um estudo realizado pela Pew Research, em dezembro de 2015, logo após o atentado de San Bernardino.

Segundo a análise, 51% dos americanos posicionavam-se do lado do FBI, isto é, preferiam que a Apple desbloqueasse o aparelho do terrorista, contra 38% que não concordavam, pois acreditavam que isto poderia gerar o risco de uma invasão à privacidade dos demais usuários futuramente. Entretanto, antes do atentado, a maioria dos americanos (54%) discordava das ações do governo de coletar dados de telefones e internet para ações de contraterrorismo, ao contrário de 42% deles que aprovavam a medida. Esses dados sugerem que as pessoas ficam muito mais suscetíveis a uma intervenção por parte do governo logo após alguma fatalidade.




Outra pesquisa que demonstra um posicionamento semelhante é a da empresa de eletrônicos Cable Co. De acordo com o estudo realizado logo após o atentando de Londres, de duas mil pessoas entrevistadas na cidade, 66% eram a favor de que as autoridades tivessem um acesso mais fácil às comunicações, mesmo que isso significasse perda de privacidade. Apenas 25% dessas pessoas disseram que a remoção da criptografia ou a instalação de outros acessos para as autoridades lhes faria sentir menos seguras.

Portanto, primeiramente, há um risco de maior intervenção estatal, a qual é fomentada principalmente pela resistência das empresas de comunicação em auxiliar nas investigações governamentais. Dessa forma, haveria o perigo do aumento de controle da indústria por parte do Estado, o qual assim poderia criar ou aumentar regulamentações que facilitariam a obtenção de dados de usuários em assuntos de segurança nacional.

Tal intervenção do governo em um momento de insegurança poderia gerar impactos para a empresa, como a perda do valor da mesma e a diminuição dos números de usuários. Todavia, os últimos poderiam ser recuperados facilmente, visto que nesse cenário a atuação do governo e a aplicação de certas normas seriam pontuais, e não necessariamente institucionalizadas.

Além disso, no caso da Apple, por exemplo, o perigo de que outros usuários tivessem seus dados vulneráveis a monitoramento e vigilância do próprio governo ou de hackers, por meio da criação de um software demandado pelo governo, faria com que houvesse uma perda de confiança em relação a empresa. Isso traria o risco de que não só a Apple, mas todas as empresas de tecnologia que asseguram a privacidade de seus consumidores, perdessem contratos lucrativos com seus clientes corporativos, uma vez que os mesmos não se sentiriam mais seguros em confiar suas informações confidenciais nos produtos de tais empresas.

A mesma situação pode ocorrer na Inglaterra, visto que Amber Rudd, secretária de Estado britânica, está trazendo para discussão os planos antigos da gestão de David Cameron, os quais envolvem um maior poder das agências de inteligência em relação a obtenção das informações e de conhecimento sobre criptografias. Além disso, tanto políticos britânicos como americanos já estão sugerindo que as empresas como Whatsapp e Telegram criem redes e serviços como os dos seus aplicativos para as agências quando estas estiverem investigando atividades terroristas.

Contudo, passando o momento de insegurança e toda a comoção referente aos ataques, haveria o aumento da preocupação com a privacidade e com a intromissão do governo, que passaria a incomodar a sociedade com seu controle excessivo. Há, portanto, o risco de uma armadilha legislativa, que dificulta a diminuição do domínio do Estado sobre a indústria num momento de maior tranquilidade. Uma vez que o terror gera uma comoção e mobilização muito maior que a privacidade, esta não seria fator suficiente para fazer com que o governo desfizesse a armadilha. Essa armadilha também traria consequências para a indústria de telecomunicações, visto que com a perda de credibilidade e confiança, as empresas enfrentariam uma queda no número de usuários.

**O terror gera uma comoção e mobilização muito maior que a privacidade**

É a partir desse cenário que propostas como a de Amber Rudd em banir totalmente o uso de criptografia podem ser aprovadas. Leis tão rígidas e extremas como esta podem gerar impactos em setores como no comércio online, nas transações financeiras e até mesmo no crescimento da própria indústria digital. Além disso, no caso da ausência da criptografia, muitos programas e softwares ficariam vulneráveis à pirataria.

Vale ressaltar que ambos os riscos, a maior intervenção estatal e a armadilha legislativa, parecem ter uma probabilidade semelhante de ocorrer, uma vez que a *driving force* dos dois é a mesma, qual seja, o nível da atividade terrorista. Esses cenários mencionados parecem, portanto, mais prováveis a um médio prazo, pois observamos uma tendência de aumento das atividades terroristas. Também é relevante notar como os riscos ocorrem de acordo com a opinião pública, a qual muda em relação as novas incertezas e preocupações referentes à segurança.

Apesar dos riscos apresentados, existem oportunidades dentro dessa nova configuração da relação entre empresas e Estados. A primeira seria a cooperação entre ambos, que poderia partir da própria indústria por meio de uma iniciativa própria, o nos parece ter uma chance média de acontecer. Essa contribuição mútua

poderia se dar com a criação de uma solução que auxiliasse o monitoramento das atividades dos usuários de forma detalhada, observando o conteúdo das comunicações, e ajudando o governo ao fornecer dados de atividades suspeitas.

Entretanto, apesar de tal solução beneficiar a segurança, ela ocasionaria um impacto para o setor, principalmente referente à perda de usuários. Se as empresas de tecnologia colaborarem abertamente com programas de monitoramento governamental, criar-se-á uma suspeição entre os clientes, que não gostarão de ter sua comunicação monitorada e possivelmente repassada ao Estado. Além disso, haveria o risco de que a imagem destas empresas sofresse um impacto muito negativo, e isto abalaria a credibilidade das mesmas no mercado internacional, impactando nas vendas e consequentemente na participação de mercado destas empresas no exterior, o que evidentemente afetaria seu lucro, bem como o do setor de tecnologia como um todo.

Já a segunda oportunidade é referente à busca por inovações que possivelmente tornem o conflito entre empresas e Estados um problema obsoleto. Para isso, a indústria poderia trazer novos produtos e serviços, que atrairiam novos clientes e manteriam os já conquistados, gerando como impacto um aumento do número de usuários. Mas a chance de isso acontecer no curto prazo é pequena, uma vez que *breakthroughs* são difíceis e, além disso, os terroristas tentariam novamente ter acesso à essas novas tecnologias, reiniciando o ciclo de embates.

Para que a indústria de tecnologia possa evitar o pior cenário, existem algumas medidas que podem ser aplicadas. Primeiramente, estas empresas podem tomar a frente e ensejar a cooperação com o Estado, visando a minimização de suas perdas. Além disso, para maximizar ganhos, elas podem investir em inovações como novos produtos e novas tecnologias de criptografia que, de certa forma, diminuam os conflitos com o poder nacional.

Também seria de extrema importância que novas formas de relacionamento com os usuários fossem exploradas. Lembre-se que o conjunto de usuários intersecta o de eleitores, e estes influenciam nas decisões das firmas e governos por meio de sua opinião, que deve ser sempre observada, já que é inconstante. Um exemplo dessa medida, foi a ação da empresa Facebook ao convidar os seus usuários a reportarem as fake news, encorajando a formação de um espaço mais seguro e confiável, além de promover uma aproximação do cliente com plataforma.

Por fim, é possível também que o setor de tecnologia se faça escutar junto às esferas legislativas e decisórias, expondo sua situação e suas demandas.

O RAIA É UM NÚCLEO DE ANÁLISE DE RISCO E CENÁRIOS INTERNACIONAIS COMPOSTO DE PROFESSORES E ESTUDANTES DO CURSO DE RELAÇÕES INTERNACIONAIS DA ESPM-SP.

Análise de Conjuntura (Working Paper), no. 2, junho de 2017. ISSN 2359-1706

**Expediente**