**Arrependimento do Comprador: Gigantes dos Aplicativos Colhem o Que Plantaram na Europa**

**Ora, ora, ora, como o ditado diz ... se arrependimento matasse....** À medida que os planos de compliance são implementados sob o Ato de Mercados Digitais (DMA) na Europa, defensores conscientes do DMA devem estar se lastimando em pensamentos. No entanto, esta não é uma impressão que alguém aponta em público sem certa ironia. As maiores empresas do mundo que distribuem aplicativos por meio das principais lojas de aplicativos (Big Apps) certamente não querem admitir que cometeram um grande erro.

Em vez disso, estão criticando fortemente o plano de compliance da Apple, fingindo(?) surpresa pela Apple continuaria a cobrar pela distribuição de aplicativos. A ironia aqui deriva parcialmente do fato de que isso é exatamente o que eles estavam pedindo—uma transferência dos custos de si mesmos para o restante da economia de aplicativos. O restante advém da uma crença, seja sincera ou dissimulada, de que os custos podem ser dissipados por decreto governamental, de que o “almoço pode ser grátis". Grandes empresas de aplicativos podem ter o luxo de não aprender nada com o experimento do DMA, mas não é tarde demais—e é vitalmente importante—para outros governos e formuladores de políticas públicas em todo o mundo que estão sendo instados a intervir no estilo do DMA, incluindo propostas como o American Innovation and Choice Online Act (AICOA) e o Open App Markets Act (OAMA).

Algumas das lições aprendidas da experiência do DMA:

*Lição 1: A intervenção no estilo do DMA inevitavelmente introduzirá vulnerabilidades de privacidade e segurança.*O Artigo 6, parágrafo 4, do DMA exige que as sistemas operacionais **atribuídos como gatekeepers** permitam lojas de aplicativos de terceiros. Como [apontamos](https://actonline.org/wp-content/uploads/European-Style-Online-Marketplace-Regulation-v1-1-2.pdf), se os reguladores aplicassem estritamente as diretrizes do DMA, isso eliminaria a maioria das medidas comuns e proativas de cibersegurança e privacidade que atualmente protegem os consumidores em seus dispositivos inteligentes. As exceções às diretrizes do DMA são estreitas, permitindo apenas medidas que abordem ameaças que “ponham em perigo a integridade do hardware ou sistema operacional”. Os reguladores europeus esperançosamente veem os problemas com uma interpretação rigorosa dessa passagem, já que o plano de conformidade da Apple mantém a capacidade de usar a notarização para autenticar que os aplicativos são o que afirmam ser e não são falsificações. Isso é uma vitória especialmente importante para os consumidores no processo de compliance. No entanto, a notarização é apenas um dos meios básicos de garantia contra ameaças de privacidade e segurança. Por exemplo, a notarização por si só não permitiria uso ou acesso a controles parentais (mais sobre isso abaixo) e não aborda necessariamente a verificação de permissões. Como discutimos anteriormente, [a verificação de permissões](https://actonline.org/2023/11/06/event-recap-mobile-security-and-the-app-ecosystem/) é o que garante à loja de aplicativos que as categorias de dados solicitadas por um aplicativo correspondam ao seu propósito. A verificação de permissões consegue impedir uma porcentagem significativa das tentativas de comprometer os dispositivos das pessoas, roubar suas informações, identidade ou dinheiro. Alguns podem dizer que abrir essa camada de segurança para concorrentes é positivo. Mas lembre-se de que a competição em si é o que produziu uma solução verticalmente integrada que os consumidores aparentemente preferem e escolheram em relação às alternativas. Vale a lembrança de que a competição neste aspecto específico, entre outras, sob o DMA, é um simulacro de competição impulsionado pelo regulador que ocorre em cima das plataformas individuais das empresas.

Notadamente, é improvável que o OAMA permita um plano de conformidade que inclua a notarização, uma vez que proibir o acesso a sistemas operacionais, hardware e software presume a ilegalidade. A autorização do OAMA para fornecer ao “usuário final os meios técnicos para verificar a autenticidade e origem de aplicativos ou lojas de terceiros” está disponível apenas por meio da chamada defesa afirmativa. Essa defesa afirmativa, por sua vez, só está disponível se a plataforma puder estabelecer que a notarização não é usada como pretexto “para excluir ou impor termos desnecessários ou discriminatórios” a terceiros (entre outras coisas que devem ser demonstradas). Essa linguagem parece deixar a notarização fora do alcance das plataformas de software, a menos que, ou até que, estejam dispostas a gastar dezenas de milhões em litígios para defendê-la. Seria, afinal, manter uma pequena parte das medidas de segurança e privacidade nos dispositivos inteligentes fabricados pela Apple, e tanto o AICOA quanto o OAMA foram redigidos com a suposição fundamental de que essas medidas são pretextos para prejudicar a concorrência.

*Lição 2: A intervenção no estilo do DMA mina o controle parental e a segurança online em um momento em que o Congresso está* [*dando prioridade polítca à esses temas*](https://www.judiciary.senate.gov/committee-activity/hearings/big-tech-and-the-online-child-sexual-exploitation-crisis) *.*

Outra limitação da notarização e à verificação de permissões de forma mais ampla sob o DMA é que ela não prevê a aplicação de controles parentais no mesmo nível das plataforma de softwares para aplicativos adquiridos em uma loja de terceiros. Em vez disso, o DMA parece exigir que para aplicativos baixados de lojas de aplicativos alternativas qualquer forma de controle parental possa ser usado. Isso torna muito mais difícil para os pais supervisionarem o que seus filhos podem baixar e adiciona atrito a uma função parental emergente que muitas vezes desmorona sob o peso da burocracia adicionada. De acordo com a legislação atual nos Estados Unidos, os pais podem configurar um dispositivo para o filho e [habilitar a capacidade de revisar qualquer download de aplicativo, compra ou uso de um aplicativo a partir de seus próprios dispositivos inteligentes](https://actonline.org/2024/01/31/developers-write-software-parents-parent-government-should-do-neither/). Na União Europeia, esse arranjo será muito mais complicado e não funcionará para aplicativos baixados por meio de lojas de terceiros. Isso é especialmente preocupante, pois sabemos que até mesmo alguns dos defensores mais estabelecidos e bem financiados de lojas de aplicativos alternativas [são violadores dedicados da privacidade infantil](https://actonline.org/wp-content/uploads/2023-02-15-ACT-FTC-Settlement-Letter-to-Senate-Commerce.pdf). Como resultado, sabemos que recursos serão empregados para criar lojas de aplicativos alternativas que pretendem contornar os controles e a supervisão parentais. Por fim, a compensação do DMA em grande parte renuncia a uma ferramenta poderosa que os pais têm para proteger seus filhos online em favor de modelos de negócios alternativos que intencionalmente—não incidentalmente—tornarão mais difícil do que é agora ser pai online.

*Lição 3: A intervenção no estilo do DMA transfere esses custos para desenvolvedores menores.*Há anos alertamos que projetos de lei no estilo do DMA, como o AICOA e o OAMA,  [transferirão os custos de distribuição](https://actonline.org/2021/11/12/antitrust-and-you-part-3-nondiscrimination-provides-a-platform-for-me-but-not-for-thee/)  para [desenvolvedores menores](https://actonline.org/wp-content/uploads/Platforms-and-Competition_web.pdf). Principalmente, esses custos se manifestarão de maneiras indiretas ainda não vistas, como exigir que os desenvolvedores ajustem seus e aplicativos e cumpram com termos de serviço de lojas de aplicativos diferentes, forçando os consumidores a adotar uma atitude mais cautelosa em relação aos seus dispositivos inteligentes em geral, e a lista continua. No entanto, de plano está claro que estávamos certos sobre os custos diretos. Durante audiências legislativas estaduais nos EUA sobre projetos de lei para impor mandatos de must-carry em lojas de aplicativos, destacamos que a eliminação da taxa de compra dentro do aplicativo imposta aos maiores fabricantes de aplicativos resultaria necessariamente na redistribuição dessas taxas para todos os fabricantes de aplicativos, elevando desproporcionalmente os custos e as barreiras de entrada para os pequenos fabricantes de aplicativos. A resposta de um legislador foi sugerir que as lojas de aplicativos deveriam cobrar vários milhares de dólares em taxas de registro para desenvolvedores, redistribuindo assim os custos para todos os desenvolvedores. Dessa forma, argumentou o legislador, as maiores empresas de aplicativos seriam aliviadas de arcar com grande parte do custo de manter a loja de aplicativos e distribuir aplicativos. Claro, isso é exatamente o oposto do que a política pública deveria buscar alcançar, já que a solução proposta aumentaria (de maneira bastante desigual) as taxas da loja de aplicativos para as menores empresas de aplicativos em mais de 100 vezes os custos atuais, enquanto virtualmente eliminaria todos os custos da loja de aplicativos que as maiores empresas suportam. Missão um tanto cumprida para os Big Apps nesse sentido, pois eles receberam pelo menos parte do que estavam desesperadamente buscando.

Muitos dos impactos que o DMA ainda estão por ser vistos. O que sabemos é que, com o recente lançamento do plano de compliance, os Big Apps estão conseguindo o que pediram, e é difícil ver melhoria para os consumidores e as pequenas empresas de aplicativos. Assim, agora é o momento para os governos ao redor do mundo enxergarem esse exercício pelo que é: uma vasta saída de capital político, proteções de privacidade e segurança, dólares dos contribuintes, valor do consumidor e valor de distribuição de aplicativos, em troca de pouco ou nenhum benefício discernível, exceto custos ligeiramente mais baixos para os Big Apps.