**El remordimiento de los compradores: los gigantes de aplicaciones recogen lo que siembran en Europa**

Vaya, vaya, vaya… Como se suele decir: si parece que son las consecuencias de mis propios actos. A medida que se implementan los planes de cumplimiento de la Ley de Mercados Digitales (DMA) en Europa, estos son los sentimientos de arrepentimiento que deben de estar experimentando los defensores de la DMA más conscientes de la realidad. Pero nunca es una emoción que se quiera expresar en público de un modo no irónico. Las mayores empresas del mundo que distribuyen aplicaciones a través de las principales tiendas de aplicaciones, desde luego, no están admitiendo haber cometido ningún error. En su lugar, están teniendo una pataleta ante el plan de cumplimiento de Apple, fingiendo (¿?) sorpresa por el hecho de que Apple vaya a continuar cobrando por la distribución. La ironía del asunto solo procede parcialmente del hecho de que esto es exactamente lo que habían estado pidiendo: un traspaso de los costes desde ellos mismos hacia el resto de la economía de aplicaciones. Su equilibrio procede de una creencia, ya sea sincera o no, de que los costes podrían ser eliminados por decreto gubernamental, que les diesen la comida "gratis". Los gigantes de las aplicaciones quizá tengan el lujo de no aprender nada del experimento de la DMA, pero no es demasiado tarde para que otros Gobiernos tomen notas del asunto; y es de vital importancia que lo hagan. Hay varias lecciones que podemos sacar ya mismo de esta experiencia a medida que se solicita a los formuladores de políticas de todo el mundo que intervengan al estilo de la DMA, incluyendo propuestas como la *American Innovation and Choice Online Act* (AICOA) y la *Open App Markets Act* (OAMA):

*Lección 1: Una intervención al estilo de la DMA introduciría, inevitablemente, vulnerabilidades de privacidad y seguridad.*El artículo 6, párrafo 4 de la DMA requiere que las plataformas de software cubiertas permitan las tiendas de aplicaciones de terceros. Como [hemos señalado](https://actonline.org/wp-content/uploads/European-Style-Online-Marketplace-Regulation-v1-1-2.pdf), si los reguladores ejecutaran el mandato estrictamente, esto eliminaría la mayoría de medidas de ciberseguridad y privacidad proactivas y de sentido común que actualmente protegen a los consumidores en sus dispositivos inteligentes. Las excepciones al mandato son limitadas, y permiten únicamente medidas que aborden amenazas que "ponen en peligro la integridad del hardware o el sistema operativo". Esperemos que los reguladores europeos vean los problemas que conlleva una lectura estricta de este pasaje, a medida que el programa de cumplimiento de Apple retiene su habilidad para utilizar la certificación notarial con el fin de certificar que las aplicaciones son lo que dicen ser y no son falsificaciones. Esto es una victoria especialmente importante para los consumidores en el proceso de cumplimiento. Sin embargo, la certificación notarial solo es una de las garantías básicas frente a las amenazas de privacidad y seguridad. Por ejemplo, la certificación notarial por sí sola no permitiría imponer controles parentales (más al respecto a continuación) y no tiene por qué abordar la comprobación de permisos. Como ya hemos comentado antes, [comprobar los permisos](https://actonline.org/2023/11/06/event-recap-mobile-security-and-the-app-ecosystem/) es lo que permite a las tiendas de aplicaciones garantizar que las categorías de datos que una aplicación solicita coinciden con su propósito. La comprobación de permisos cubre un sorprendente porcentaje de intentos de comprometer los dispositivos de los usuarios o robar su información, identidad o dinero. Hay quien podría decir que es bueno abrir esta capa de seguridad a los competidores, pero hemos de recordar que es la propia competencia la que ha producido una solución integrada verticalmente que los consumidores parecen preferir y han seleccionado frente a otras alternativas. No nos conviene olvidar que, bajo la DMA, la competición respecto a esta característica en particular, entre otras, es un simulacro de competición impulsado por los reguladores que se desarrolla por encima de las plataformas de las empresas individuales.

Es improbable que la OAMA en particular permita un plan de cumplimiento que incluya la certificación notarial, dado que presupone la ilegalidad de desautorizar el acceso a sistemas operativos, hardware y software. La permisión de la OAMA de proporcionar a un "usuario final los medios técnicos necesarios para verificar la autenticidad y el origen de las tiendas de aplicaciones o aplicaciones de terceros" sólo está disponible mediante la defensa afirmativa. La defensa afirmativa, por su parte, sólo está disponible si la plataforma puede establecer que la certificación notarial no se ha usado como un pretexto "para excluir o imponer términos innecesarios o discriminatorios" sobre terceros (entre otras cosas que se deben demostrar). Este lenguaje parece situar la certificación notarial fuera del alcance de las plataformas de software, a no ser que y hasta que estén dispuestas a gastar enormes sumas de dinero en pleitos para defenderla. Al fin y al cabo, supondría la retención de una pequeña medida de control sobre la seguridad y privacidad en los dispositivos inteligentes que Apple ha manufacturado, y tanto la AICOA como la OAMA se han basado en las suposiciones fundamentales de que dichas medidas son pretextos para dañar a la competencia.

*Lección 2: Una intervención al estilo de la DMA socavaría el control parental y la seguridad en línea en un momento en el que el Congreso está*[*priorizando estos objetivos en materia de políticas*](https://www.judiciary.senate.gov/committee-activity/hearings/big-tech-and-the-online-child-sexual-exploitation-crisis)*.*Otro límite de la certificación notarial y los permisos más amplios bajo la DMA es que no permiten aplicar controles parentales a nivel de plataforma para las aplicaciones adquiridas en tiendas de terceros. En su lugar, la DMA parece requerir que cualquier control parental para aplicaciones descargadas a través de una tienda de aplicaciones alternativa sea facilitado por dicha tienda. Esto hace que sea mucho más difícil para los padres supervisar lo que sus hijos se pueden descargar, y complica una función parental emergente que suele colapsar bajo el peso del papeleo añadido. Bajo la legislación actual de los Estados Unidos, los progenitores pueden configurar un dispositivo para su hijo y [habilitar la supervisión de cualquier descarga, compra o uso de aplicaciones desde sus propios dispositivos inteligentes](https://actonline.org/2024/01/31/developers-write-software-parents-parent-government-should-do-neither/). En la UE, esto será muchísimo más complicado y no funcionará con las aplicaciones descargadas a través de tiendas de terceros. Esto es especialmente preocupante pues, como sabemos, incluso algunos de los defensores de las tiendas de aplicaciones alternativas mejor establecidos y con mejores recursos [están dedicados a vulnerar la privacidad de los niños](https://actonline.org/wp-content/uploads/2023-02-15-ACT-FTC-Settlement-Letter-to-Senate-Commerce.pdf). Por tanto, sabemos que se emplearán recursos para crear tiendas de aplicaciones alternativas que buscan evadir la supervisión y los controles parentales. Al fin y al cabo, el compromiso de la DMA invalida en gran medida una poderosa herramienta que tienen los padres para proteger a sus hijos en línea en favor de modelos de negocios alternativos que dificultarán deliberadamente, no por accidente, la tarea de ser padre en línea.

*Lección 3: Las intervenciones al estilo de la DMA trasladan los costes a los pequeños desarrolladores.*Llevamos ya años advirtiendo de que las leyes al estilo de la DMA, como la AICOA y la OAMA, [trasladarían los costes de distribución](https://actonline.org/2021/11/12/antitrust-and-you-part-3-nondiscrimination-provides-a-platform-for-me-but-not-for-thee/) a los [pequeños desarrolladores](https://actonline.org/wp-content/uploads/Platforms-and-Competition_web.pdf). Estos costes se manifestarán principalmente de formas indirectas que todavía están por verse, como requerir a los creadores de aplicaciones que desarrollen aplicaciones para más tiendas y cumplan con los diferentes términos del servicio de distintas tiendas de aplicaciones, forzando a los consumidores a adoptar una actitud más cauta como compradores en sus dispositivos inteligentes en general. Y la cosa no acaba ahí. Sin embargo, queda claro de inmediato que teníamos razón acerca de los costes directos. Durante las audiencias legislativas estatales sobre proyectos de ley para imponer mandatos de inclusión obligatoria de tiendas de aplicaciones, hemos señalado que, si se eliminara la tasa de compra dentro de la aplicación impuesta a los mayores creadores de aplicaciones, dichas tasas tendrían que redirigirse a todos los creadores de aplicaciones, lo cual elevaría los costes y las barreras de acceso de manera desproporcionada para los creadores de aplicaciones de pequeño tamaño. La respuesta de un legislador fue sugerir que las tiendas de aplicaciones cobraran varios miles de dólares en tasas de registro de los desarrolladores, distribuyendo así los costes entre todos los desarrolladores. De este modo, argumentó el legislador, las mayores empresas de aplicaciones ya no tendrían que cargar con una proporción tan grande del coste de mantener una tienda de aplicaciones y distribuir las aplicaciones. Por supuesto, esto es exactamente lo contrario de lo que las políticas públicas deberían tratar de conseguir, dado que la solución propuesta aumentaría (de manera muy poco equitativa) las tasas de las tiendas de aplicaciones para las empresas de menor tamaño, multiplicando hasta por 100 sus costes actuales, al tiempo que eliminaría prácticamente todos los costes de tiendas de aplicaciones en que incurrirían las mayores empresas. Se podría decir que los gigantes de las aplicaciones han cumplido su misión hasta cierto punto, pues al menos han obtenido algo de lo que tan desesperadamente estaba buscando.

Muchas de las consecuencias de la DMA todavía están por ver. Lo que sí sabemos es que, con la reciente implementación del plan de cumplimiento, los gigantes de las aplicaciones están consiguiendo lo que había pedido, y cuesta ver cómo han salido beneficiados los consumidores y las compañías de aplicaciones de pequeño tamaño. Ahora es el momento de que los Gobiernos de todo el mundo vean este ejercicio como lo que realmente es: una enorme salida de capital político, protecciones de privacidad y seguridad, dinero de los contribuyentes, valor del consumidor y valor de distribución de aplicaciones a cambio de un beneficio mínimo, si acaso discernible, más allá de unos costes ligeramente menores para los gigantes de las aplicaciones.