Kill switch et capture institutionnelle

Une promesse de protection qui conserve la possibilité de la retirer. Quand l'interrupteur existe, quelqu'un finit par appuyer dessus.

Pour faire simple : Par exemple, WhatsApp peut effacer vos messages quand il veut. Le contrat ne l'empêche pas aujourd'hui, et demain ils le changent. Une décision de justice, une nouvelle règle, un gouvernement qui le demande — et vous découvrez qu'ils n'ont jamais été à vous.

La promesse qui repose sur la possibilité de la retirer

En 2017, pendant l'ouragan Irma, plusieurs propriétaires de Tesla en Floride ont découvert que leur voiture, en recevant une mise à jour à distance du fabricant, gagnait soudainement des kilomètres d'autonomie supplémentaires. Ils n'avaient pas payé pour cela. La batterie avait toujours été capable de les fournir ; le fabricant avait décidé, afin de segmenter le marché, de ne pas le permettre au client. Pendant l'urgence, Tesla a activé la capacité totale de manière temporaire. Une fois l'urgence passée, il l'a désactivée.

Ce que les informations décrivaient comme un geste de générosité était, à bien y regarder, autre chose. Le propriétaire n'avait jamais été propriétaire du produit entier qu'il avait payé. Le fabricant conservait une capacité technique — étendre ou réduire les prestations à distance — et a choisi de l'exercer en faveur du client dans ce cas précis. Il aurait pu choisir le contraire. L'histoire ne raconte pas un acte de bonté ; elle raconte une architecture de pouvoir.

Cet article traite de cette architecture. Nous l'appelons, par convention du secteur, *kill switch* : l'interrupteur à distance qui permet à l'opérateur de désactiver, modifier ou retirer les capacités d'un produit, d'un service ou d'un appareil que l'utilisateur croyait déjà sien. La question n'est pas de savoir si l'opérateur est honnête. La question est de savoir ce qui se passe quand il cesse de l'être, ou quand quelqu'un l'oblige à utiliser l'interrupteur dans une autre direction.

Qu'est-ce qu'un kill switch exactement

Le terme vient de l'anglais et se traduit avec difficulté : *interruptor de muerte* est dramatique ; *interruptor remoto* est trop neutre. Ce qui définit le kill switch n'est pas le caractère dramatique, mais une propriété simple : la capacité technique de désactiver quelque chose à distance, aux mains de quelqu'un d'autre que l'utilisateur. Il peut s'agir d'une fermeture complète —la voiture qui ne démarre pas, le fichier qui s'efface, le compte qui est suspendu— ou d'une fermeture partielle —la fonction qui disparaît, la batterie qui perd de l'autonomie, l'abonnement qui s'interrompt.

Tout contrôle à distance n'est pas un kill switch. Une mise à jour de sécurité routinière, autorisée par l'utilisateur lors de l'installation du produit, n'en est pas un. Pas plus qu'un système antivol activable par le propriétaire lui-même en cas de vol de son téléphone. Le kill switch, au sens propre, présente trois traits : son utilisation est une décision de l'opérateur, non de l'utilisateur ; il ne nécessite pas le consentement ponctuel de la personne concernée pour être activé ; et il s'exerce sur un produit ou un service que l'utilisateur considérait déjà comme le sien à part entière.

La galerie européenne des interrupteurs en activité

Tesla répète souvent ce schéma, de manière documentée dans son cas : dégradations contractuelles d'autonomie appliquées à des véhicules d'occasion ayant changé de propriétaire, retraits de fonctions de conduite assistée après révocation de licence, modifications unilatérales du comportement du produit entre deux versions de firmware. John Deere est depuis des années au centre du débat européen et américain sur le droit à la réparation : l'achat d'un tracteur inclut une couche logicielle dont le service dépend du réseau officiel du fabricant ; lorsque ce réseau refuse l'accès, le tracteur réduit ses fonctions essentielles. BMW a proposé en 2022 un abonnement mensuel pour activer le chauffage des sièges sur des voitures qui en étaient déjà équipées physiquement ; la pression publique a forcé le retrait du modèle, mais la capacité technique demeure.

Dans le domaine du logiciel, le schéma est structurel. Adobe Creative Cloud révoque les licences mensuelles lorsque l'abonnement n'est pas renouvelé, rendant inutilisables les fichiers que l'utilisateur a créés avec ces outils. Microsoft peut désactiver les copies de Windows qu'il considère comme non authentiques, sans recours pratique. Google retire des applications du Play Store pour se conformer à des décisions de justice ou à des décisions internes ; l'application désinstallée l'est également sur les téléphones où elle se trouvait. Apple Pay a été désactivé en Russie en mars 2022, Apple se conformant aux sanctions internationales : légitime dans le contexte, mais la procédure était toujours disponible.

L'argument légitime du côté du fabricant

Celui qui conçoit l'un de ces systèmes avance généralement des arguments parfaitement valables :

1. **Prévention du vol.** Si on me vole ma voiture ou mon téléphone, j'apprécie que le fabricant puisse le rendre inutilisable à distance.
2. **Prévention de la fraude.** Les abonnements impayés nécessitent un mécanisme de coupure ; sans ce mécanisme, le modèle économique s'effondre.
3. **Prévention de l'usage abusif.** Un outil dangereux entre de mauvaises mains peut bénéficier de la possibilité d'être révoqué.
4. **Conformité réglementaire.** Certaines ordonnances juridiques obligent l'opérateur à retirer du contenu, désactiver des fonctions ou suspendre des comptes, et un système sans interrupteur est un système qui ne peut pas s'y conformer.

Les quatre arguments sont vrais. Aucun ne change la nature de la question. Il est vrai qu'un kill switch facilite la prévention du vol ; il est également vrai que cette même capacité sert à contraindre le client vivant, et pas seulement à nuire au voleur. Il est vrai que le modèle d'abonnement nécessite une coupure ; il est également vrai que la coupure peut être exécutée demain sur un client actuel pour une raison différente de celle prévue au contrat. La question n'est pas de savoir si le kill switch a des usages légitimes. La question est qu'une fois qu'il existe, ses usages ne se limitent pas à ceux prévus dans la documentation initiale.

La capture institutionnelle

C'est ici qu'entre en jeu le concept qui donne son titre à l'article. La capture institutionnelle est la situation dans laquelle un acteur — une entreprise privée, une administration, un organisme de régulation — finit par exercer des capacités qu'il a acquises ou qui lui ont été concédées à des fins limitées à des fins plus larges, différentes, ou franchement opposées aux originales. L'économie politique connaît le phénomène depuis des décennies dans la régulation financière. L'industrie technologique le découvre de sa propre main.

Le mécanisme est le suivant. L'entreprise conçoit le kill switch à des fins légitimes : antivol, gestion d'abonnement, conformité. L'entreprise documente ces fins dans ses conditions d'utilisation, dans sa politique de confidentialité, dans ses messages publics. Les années passent. Un gouvernement émet un ordre en vertu d'une nouvelle législation ; l'entreprise se voit obligée d'utiliser l'interrupteur dans une direction non décrite dans sa

documentation originale. Un actionnaire activiste entre au conseil d'administration et modifie la politique commerciale ; les interrupteurs existent, et ils sont appliqués selon la nouvelle politique. L'entreprise est acquise par une autre plus grande ; les conditions de service sont réécrites unilatéralement avec un préavis de trente jours. Dans chaque cas, le client qui a fait confiance à l'interrupteur pour les fins documentées se retrouve avec un interrupteur toujours présent, mais qui répond à d'autres intérêts.

Le cas paradigmatique pour le lecteur européen : l'affaire Apple contre le FBI à San Bernardino, en 2016. Après un attentat en Californie, le FBI a exigé d'Apple qu'elle déverrouille un iPhone de l'auteur. Apple a refusé, soutenant en partie des arguments de principe et en partie un argument technique : le système, tel qu'il était conçu, ne permettait pas à l'entreprise elle-même de déverrouiller l'appareil sans réécrire le logiciel de base. La défense la plus solide n'était pas morale ; elle était architecturale. Apple ne s'est pas appuyée sur la promesse de ne pas appuyer sur l'interrupteur ; elle s'est appuyée sur l'absence de l'interrupteur. D'autres entreprises, avec des interrupteurs présents dans leur architecture, n'ont pas pu maintenir la même position face à des pressions équivalentes.

La trajectoire normative européenne

Le droit européen, lors de la dernière législature, a poussé vers davantage de capacités de contrôle à distance, et non moins. Le Règlement sur les Services Numériques (DSA), pleinement applicable depuis février 2024, oblige les plateformes à activer des mécanismes rapides de retrait de contenu sur ordre d'une autorité compétente ; des mécanismes qui n'existeraient pas sans la capacité technique sous-jacente. Le Règlement sur l'Intelligence Artificielle (AI Act), en vigueur de manière échelonnée depuis août 2024, exige des fournisseurs de certains systèmes d'IA à haut risque de disposer de mesures permettant leur désactivation ou une surveillance humaine significative : une forme normative de kill switch obligatoire. Le Règlement sur les Marchés Numériques (DMA) introduit, en revanche, des obligations d'interopérabilité : un courant opposé qui limite les effets de verrouillage.

Pour le professionnel européen, la lecture honnête est la suivante : la question « l'opérateur peut-il désactiver ce service pour moi ? » reçoit chaque année davantage de réponses affirmatives par exigence légale, et non moins. Cela ne remet pas en question la légitimité de la réglementation — le DSA répond à de vrais problèmes —, mais cela renforce une chose : faire confiance à l'opérateur pour qu'il n'utilise pas l'interrupteur exige de faire confiance, en plus, au fait qu'aucune obligation légale future ne l'obligera à l'utiliser dans une direction non envisagée aujourd'hui. C'est une confiance qui ne repose pas seulement sur l'entreprise ; elle repose sur l'ensemble de l'environnement normatif.

La question de conception qui est rarement posée

La majeure partie de la conception technique contemporaine suppose que l'interrupteur existera et promet ensuite de ne pas en abuser. Il existe une alternative, plus exigeante mais parfaitement réalisable : concevoir en supposant que l'interrupteur ne doit pas exister. Ce n'est pas un slogan. Cela implique des décisions concrètes : architecture distribuée plutôt que centralisée, droits sur l'appareil de l'utilisateur plutôt que dérivés du compte, contenu chiffré avec des clés que l'opérateur n'a pas plutôt que contenu chiffré avec des clés que l'opérateur conserve, identité cryptographique de l'utilisateur plutôt qu'identité gérée par l'opérateur. Chacune de ces décisions a un coût technique réel et des conséquences commerciales réelles. Mais toutes partagent une propriété : une fois prises, elles éliminent certaines injonctions légales en tant qu'objet possible. Ce qui ne peut être exécuté ne peut être ordonné d'être exécuté.

Pour le lecteur professionnel

Cinq questions qu'il convient de poser au fournisseur de tout service professionnel critique avant de l'adopter, formulées dans l'ordre où un inspecteur de continuité d'activité les poserait :

1. Existe-t-il une capacité technique du fournisseur pour suspendre, bloquer, supprimer ou dégrader mon service, mes données ou mon produit à distance ?
2. Dans quels cas contractuellement déclarés le fournisseur peut-il exercer cette capacité ?
3. Dans quels cas non déclarés — ordonnance judiciaire, sanction internationale, changement unilatéral de politique, acquisition d'entreprise — peut-il également l'exercer ?
4. Si elle est exercée, de quel temps de continuité de l'activité professionnelle disposé-je, et quel plan de sortie est disponible ?
5. Existe-t-il une alternative architecturale où la réponse à la question un serait « non » par construction, et non par promesse ?

La réponse à la question cinq n'est pas toujours disponible ou proportionnée. Un tableur personnel ne mérite probablement pas une telle exigence. Un dossier juridique actif, l'historique médical d'un patient, une comptabilité fiscale, une conversation déontologiquement protégée, si. La proportionnalité est une décision professionnelle ; la lecture honnête de la question un ne l'est pas : soit l'interrupteur existe, soit il n'existe pas.

La protection qui retient la possibilité de se retirer n'est pas une protection structurelle ; c'est de la confiance renommée. La confiance, nous l'avons dit dans un autre Cahier, est une solution sociale valide quand elle est accordée à qui la mérite, fragile au premier changement de mains. La défense structurelle la plus propre est celle qui ne peut être retirée parce qu'elle n'existe pas en premier lieu. Comme pour tout en architecture : un choix de conception, pas une décision de marketing.

Note éditoriale : quand ces Cuadernos nomment des entreprises ou des produits, ce n'est pas pour accuser. Ceux qui les construisent font un travail que des millions de personnes utilisent et apprécient. Ce que nous soulignons est structurel — le modèle, pas la marque. Les marques apparaissent comme exemples car ce sont celles que le lecteur reconnaît.

Sources et lectures complémentaires

- Tesla — mise à jour de septembre 2017 étendant temporairement l'autonomie des batteries des modèles S et X en Floride pendant l'ouragan Irma. Cas largement documenté dans la presse spécialisée et les rapports ultérieurs sur les révocations contractuelles d'autonomie.
- Règlement (UE) 2022/2065 relatif aux services numériques (DSA) — pleinement applicable depuis le 17 février 2024. Articles 16 et 9, sur les mécanismes de notification et d'action et les injonctions des autorités compétentes.
- Règlement (UE) 2024/1689 sur l'intelligence artificielle (AI Act) — en vigueur depuis le 1er août 2024, application échelonnée jusqu'en août 2026. Articles sur la surveillance humaine et les mesures d'atténuation obligatoires pour les systèmes à haut risque.
- United States District Court — Apple, Inc. (16 février 2016). Documentation du cas connu sous le nom de San Bernardino sur l'accès à l'iPhone dans le cadre d'une enquête pénale.
- U.S. Federal Trade Commission — mémorandums sur le droit à la réparation (2021-2024) avec des références spécifiques à John Deere et au secteur agricole ; complété par la directive (UE) 2024/1799 sur la promotion de la réparation des biens.

← PrécédentCe qu'est réellement SHA-256Suivant →Chiffrement de bout en bout, enfin expliqué

Lectures recentes

- Analyse · 18 mai 2026 Confidentialité réelle vs apparente : les questions à se poser
- Analyse · 18 mai 2026 Self-hosting comme pratique professionnelle
- Concept · 18 mai 2026 Les 24 mots : qu'est-ce qu'une identité cryptographique

Emportez cet article où vous en avez besoin.

↓ Markdown ↓ Texte brut ↓ PDF

Le fichier est téléchargé sur votre appareil. À partir de là, vous pouvez l'enregistrer, l'importer dans Solo2 ou le partager comme vous le souhaitez. Cuadernos ne décide pas de la destination pour vous.

Cachet de cire · SHA-256 4f4a11d5e8eee17d28ca52f377b6549df6ff1435bb2f8d57fe2d2000d991cd9e

Cuadernos Lacre · Une publication de Menzuri Gestión S.L. ·
écrite par R.Eugenio · éditée par l'équipe de Solo2.