**Protecció dels clients de serveis** al  **núvol del govern** **estranger**

AWS està plenament compromès amb la protecció de les dades dels seus clients i el compliment de les lleis aplicables a cada país on opera. Críticament, ens comprometem a treballar estretament amb clients governamentals estrangers per garantir que el seu contingut al núvol continuï sent segur i segur als centres de dades d'AWS ubicats a qualsevol lloc de el món. Malgrat alguns informes inicials que pretenien despertar temors sobre l'aplicació als Estats Units de la Llei d'aclariment de l'ús legal a l'estranger de dades (CLOUD Act), la la llei ha creat garanties additional per al contingut al núvol, a més de les proteccions existents. Més important encara, no creiem que la Llei CLOUD permeti als EUA. govern per accedir al contingut del núvol del govern estranger. Confiem en la nostra capacitat per protegir el contingut clou d del govern estranger utilitzant els mitjans legals disponibles als EUA. llei, inclosa l'aplicació de la immunitat sobirana i les defenses de la comitiva. I com a capa addicional de seguretat, els clients governamentals estrangers també poden aplicar xifratge fort al contingut del núvol als serveis D'AWS, que actua com un complet salvaguarda contra qualsevol accés no autoritzat pel client. A continuació, proporcionem les nostres idees i aclariments sobre les proteccions legals, estructurals i pràctiques disponibles per als governs estrangers.

# Resumint la Llei CLOUD

Anem a l'art amb el que ha canviat. La Llei CLOUD va crear un mecanisme judicial específic que els EUA les forces de l'ordre poden utilitzar-la d'acord amb la Llei de comunicacions emmagatzemades (SCA) per buscar accés a la informació que es conserva fora dels Estats Units si aquesta informació s'ha utilitzat per ometre un crim sota els EUA llei. És important destacar que la Llei CLOUD reconeix explícitament el dret dels proveïdors de serveis en el núvol a desafiar la divulgació d'informació si fer-ho entraria en conflicte amb les lleis d'un altre país o nacionals interessos. Abans de la Llei CLOUD, aquest dret era una disputa en virtut de la SCA, tot i que no hem vist cap evidència dels EUA. les forces de l'ordre que utilitzen el SCA per buscar informació propietat d'un govern estranger, ara està clar que AWS pot desafiar la divulgació de contingut al núvol del govern estranger si la divulgació vulneraria la llei o la sobirania estrangera. Treballarem amb els clients governamentals estrangers per ajudar a garantir que tant AWS com els nostres clients estiguin millor posicionats per obtenir aquests avantatges.

A més, la Llei CLOUD contempla que els EUA el govern signarà nous "acords executius" amb governs estrangers. Aquests acords executius serviran per simplificar i regular les sol· licituds bilaterals d'informació policial estrangera en termes i condicions mútuament acordables que poden ser addicionals motius per resistir-se a la divulgació i garantir que totes les divulgacions estiguin plenament autoritzades per ambdós governs. A través d'aquests acords executius, els governs estrangers podran ajudar a donar forma a l'aplicació de la Llei CLOUD a través de la diplomàcia dels EUA. govern. Estem encantats de treballar directament amb clients governamentals estrangers i els EUA. Departament de Justícia (DOJ) per ajudar a agilitzar l'entrada en acords executius.

Què no ha canviat? La Llei CLOUD no dóna eua. les forces de l'ordre noli limiten o no tenen accés a la informació dels clients emmagatzemada dins o fora dels Estats Units. Per protegir els drets individuals, EUA la llei aplica garanties processals a les sol·licituds d'informació de les forces de l'ordre, i la Llei CLOUD no canvia aquestes proteccions. En casos de delictes, com ara terrorisme, la Llei CLOUD permet als EUA. aplicació de la llei per sol·licitar-se a un EUA independent tribunal per obtenir una ordre o ordre. Aquesta sol·licitud ha d'especificar les proves buscades i proporcionar fets suficients per demostrar als EUA. tribunal que hi ha una causa probable per creure que s'ha produït un delicte i les proves estan directament relacionades amb aquest delicte. Un jutge independent decideix si els EUA l'aplicació de la llei ha complert amb la seva càrrega, i la decisió d'aquest jutge està subjecta a apel·lació i revifada per tribunals d'apel·lació independents. Es tracta d'un procediment molt més rigorós i independent del que existeix per a les sol·licituds d'informació policial en altres països.

La màxima prioritat d'AWS és la seguretat del contingut en el núvol dels nostres clients. La Llei CLOUD no canvia això. Ens mantenim amb el nostre compromís de no divulgar contingut del núvol del client tret que estigui legalment obligat a fer-ho. També mantenim el nostre compromís que notificarem als clients abans de divulgar contingut al núvol. Finalment, la Llei CLOUD no impedirà que els US actuïn per protegir els nostres clients, de fet, ens proporciona mitjans addicionals per desafiar la divulgació. Hem desafiat els EUA. sol·licituds governamentals d'informació dels clients que crèiem que eren il·legals o exagerades, guanyant decisions que han servit per establir estàndards legals per protegir els interessos de privadesa dels clients , i seguim compromesos a fer-ho.[[1]](#footnote-1)

# Els governs es mouen al núvol

AWS ofereix els serveis en el núvol més complets i àmpliament adoptats del món, servint milions de customers actius cada mes i desenes de milers d'agències governamentals , institucions educatives , i organitzacions sense ànim de lucre de tot el món. Tot i que AWS s'ha convertit en el proveïdor de serveis al núvol escollit per a tot tipus de clients governamentals, inclosos els ministeris i les agències (per exemple, el Ministeri de Justícia del Regne Unit, UK Driver i Agència de Llicències de Vehicles, Autoritat de Transport Terrestre de Singapur i EUA Departaments d'Estat, Seguretat Nacional, Energia, Salut i Serveis Humans , i Agricultura), instrumentalitats (per exemple, Court italià d'auditors) i organitzacions relacionades (per exemple, Banc Mundial , Nacions Unides i Europol), tots els clients d'AWS es beneficien de la infraestructura que hem construït per satisfer els requisits de més cossos de seguretatsensibles. Fins i tot amb l'increïble ritme d'innovació i adopció de serveis en el núvol com una alternativa més segura, escalable i rendible que la tradicional Infraestructura de TI, creiem que estem just al principi del que és possible amb el núvol. Els nostres clients governamentals reconeixen aquest fet i estan adoptant solucions avançades al núvol per abordar el seu funcionament operatiu, social i més urgent necessitats econòmiques: des de la intel·ligència artificial fins a l'Internet de les coses, visió per computador, aplicacions habilitades per a la veu, processing i comprensió del llenguatge natural, grans dades, realitat virtual i molt més. Veiem un camí perquè els governs estrangers adoptin el futur de les tecnologies en el núvol per satisfer aquestes necessitats crítiques, alhora que gaudeixen de proteccions legals, estructurals i pràctiques per a les seves contingut al núvol.

# Proteccions Jurídiques: Sobirania i Interessos Nacionals

Els governs estrangers, inclosos els seus ministeris, agències i instrumentalitats, són únics, tant en els seus interessos com a clients com a entitats sobiranes sota els EUA. lleis. Aquest fet permet a AWS desafiar els EUA. sol·licituds d'informació de les forces de l'ordre que poden orientar-se al contingut al núvol de governs estrangers.

Tot i que la Llei CLOUD estableix que els proveïdors de serveis en el núvol han de complir amb les obligacions del SCA de divulgar informació relativa a un "client" o "subscriptor" en resposta a un EUA vàlid. sol·licitud d'informació policial (subjecte a les proteccions processals per a warrants i altres ordres descrites anteriorment), creiem que els termes "client" i " subscriptor" com s'utilitza en el NÚVOL Act no i no pot incloure governs estrangers. I estem en bona companyia: EUA. els tribunals fa temps que reconeixen que les paraules generals d'un estatut no inclouen els governs i no afecten els drets dels governs tret que aquesta interpretació sigui clara i indiscutible del text de l'estatut. Això és especialment així quan l'aplicació de l'estatut privaria un govern estranger sobirà d'interessos establerts o on els resultats d'aquests una aplicació seria absurda. Creiem que la nostra perspicàcia sobre la Llei CLOUD compleix aquestes dues condicions a la llum dels interessos sobirans únics que un govern estranger té en el seu propi contingut al núvol.

A més, perquè la Llei CLOUD no esmenta específicament els governs estrangers com entre aquells el contingut cloud dels quals està subjecte als EUA. sol·licituds d'informació policial, creiem que la Llei CLOUD no s'hauria d'aplicar al contingut al núvol d'un govern estranger. Interpretació de la Llei CLOUD per permetre als EUA l'aplicació de la llei per accedir al contingut al núvol dels governments estrangers conduiria a un resultat absurd, ja que permetria posar fi a les proteccions de la immunitat sobirana en virtut de la Llei d'immunitats sobiranes estrangeres (FSIA) mitjançant l'habilitació dels EUA. govern per obtenir la informació d'un govern estranger sense haver d'escometre el govern estranger a la jurisdicció federal (discutim la immunitat sobirana amb més detall a continuació). No creiem que la Llei CLOUD ampliï la capacitat dels EUA. funcionaris policials per arribar al contingut al núvol de governs estrangers. A més, we creuen que el llenguatge planer de la Llei CLOUD, i en particular el seu respecte a la comitiva, impediria qualsevol divulgació d'estrangers contingut del núvol governamental.

El FSIA protegeix explícitament la immunitat sobirana dels governs estrangers, i la Llei CLOUD no fa res per canviar aquest fet perquè la Llei CLOUD no conté renúncies al sobirà immunitat. El FSIA s'erigeix com el marc exclusiu per obtenir (o derrotar) jurisdicció sobre un govern estranger als EUA. tribunals, una posició confirmada de manera inequívoca i reiterada pels EUA. Tribunal Suprem. [[2]](#footnote-2) De fet, els EUA El Tribunal Suprem ha afirmat sovint que "interpretarà els estatuts per evitar interferències no raonables amb l'autoritat sobirana d'altres nacions sempre que sigui possible". [[3]](#footnote-3) La immunitat sobirana lim estrictament la seva jurisdicció d'un tribunal i, un cop establerta la immunitat sobirana, el tribunal no té jurisdicció personal i temàtica . La jurisdicció és essencial perquè els tribunals no poden fer complir una sol·licitud d'informació segons la Llei CLOUD (ni obligar cap acte) sense jurisdicció, i el poder d'un tribunal per emetre ordres o altres ordres d'informació no pot ser més extens que la seva jurisdicció. Com a qüestió de referència, no hi ha dubte que els governs estrangers gaudeixen d'immunitat sobirana davant de qualsevol tribunal dels Estats Units.

Tot i que AWS no té dret a la immunitat sobirana, creiem que AWS pot afirmar efectivament la immunitat sobirana derivada en resposta als EUA. sol·licituds d'informació policial en virtut de la Llei CLOUD. De fet, eua courts han reconegut les proteccions de la immunitat sobirana derivada per als EUA privats. empreses que actuen sota la direcció de governs estrangers (a *Butters v.*  *Vance Int'l, Inc.* i *Alicog v.*  *Regne d'Aràbia Saudita*). La immunitat sobirana derivada s'aplicaria sempre que AWS actuï sota la direcció d'un govern estranger i que l'ús que el govern estranger faci dels serveis al núvol s'alineï amb les activitats que són peculiar dels sobirans (per exemple, executar funcions governamentals o mantenir secrets d'estat ). Un pilar clau per a l'aplicació del principi d'immunitat sobirana derivada és la nostra creença que els clients d'AWS, i no la pròpia AWS, han completat control sobre el seu contingut en el núvol. Tenim molt clar que AWS actua sobre el contingut en el núvol emmagatzemat en els serveis d'AWS només sota la direcció dels nostres clients, tal com es materialitza en els nostres compromisos sota els nostres contractes de serveis en el núvol i el compliment dels règims globals de privacitat i protecció de dades, com ara la Llei de portabilitat i rendició de comptes de l'assegurança mèdica (HIPAA) a els Estats Units i el Reglament General de Protecció de Dades (RGPD) a la UE. Els governs estrangers emeten els seus propis judicis sobre quina informació posaran a disposició i, en quins termes, a altres governs, sovint a través de diplomàcia d'alt nivell i avarícia internacional. L'ús que un govern estranger fa dels serveis al núvol no hauria d'alterar aquest principi fundacional.

A més de les defenses sobiranes d'immunitat descrites anteriorment, la Llei CLOUD confirma que els principis de comitat permeten als proveïdors de serveis en el núvol divulgar informació als EUA. l'aplicació de la llei si ho fes entraria en conflicte amb les lleis o els interessos nacionals d'un país estranger. Tot i que l'anàlisi de la comitat implica múltiples consideracions, el factor més important són els interessos nacionals relatius en joc. La immunitat sobirana, i el reconeixement exprés dels Estats Units, també pesa molt en l'anàlisi de la comitat, i creiem que els EUA. els tribunals donaran un pes important a la comitiva (reforçada per una base sobirana d'immunitat) per a la simple reafirmaciósobre això si un EUA. els tribunals havien de fer el contrari, s'arriscaria a soscavar la pròpia immunitat sobirana dels Estats Units en els procediments dels tribunals estrangers. Els Estats Units els interessos del govern per fer complir un EUA la sol·licitud d'informació de les forces de l'ordre es veuria disminuïda si el compliment exposés els EUA. el propi govern a demandes d'informació similars de governs estrangers sense l'acord explícit dels EUA. govern. De fet, eua els tribunals tenen un historial demostrat de rebutjar les sol·licituds d'informació contra governs estrangers.

# Proteccions estructurals: acords executius, lleis estrangeres i condicions de contractació

La Llei CLOUD crea incentius positius perquè els governs estrangers negociïn acords executius recíprocs amb els EUA. anara vernment i a promulgar proteccions sota les seves pròpies lleis per obtenir informació vital per als seus interessos nacionals. En fer-ho, els governs estrangers poden prendre la iniciativa per donar forma encara més a l'aplicació de la Llei CLOUD al contingut al núvol. Segons els acords executius, els proveïdors de serveis al núvol no només tindran el dret independent de desafiar els EUA. sol·licituds d'informació policial quan la sol·licitud entra en conflicte amb les lleis d'una nació estrangera, però també poden informar els governs estrangers dels objectius de la información sol·licituds. Els acords executius en virtut de la Llei CLOUD permetran encara més als EUA. govern i governs estrangers per establir les condicions en què s'han de reconèixer els seus interessos nacionals sobirans. AWS està preparada per ajudar a donar suport als esforços per establir un acord executiu entre els Estats Units i els governs estrangers que utilitzen o busquen adoptar el núvol serveis.

Per ajudar a adonar-se dels avantatges de la immunitat sobirana i la comitat descrits anteriorment, AWS treballarà amb clients governamentals estrangers per afegir proteccions contractuals als acords que regulen el seu ús de serveis AWS. Per exemple, els nostres contractes es poden adaptar a: (1) reconèixer expressament, i no renunciar, a la immunitat sobirana d'un govern estranger i a la immunitat derivada d'AWS (encluding reconeixent que els termes "client" i "subscriptor" utilitzats a la Llei CLOUD no s'apliquen a un govern estranger); (2) afirmar el dret d'un govern estranger a dirigir la gestió del seu contingut al núvol; (3) definir l'abast de les activitats d'AWS al servei de les directives del govern estranger i dels drets i interessos sobirans particulars; (4) afirmar l'objecció del govern estranger a qualsevol divulgació del seu contingut al núvol; (5) prohibir a AWS divulgar contingut al núvol del govern estranger; i (6) reconèixer lleis estrangeres específiques que serien violades per la divulgació de contingut al núvol del govern estranger.

# Proteccions pràctiques: respectar els governs estrangers i el xifratge

Cal destacar que els EUA el govern generalment no busca enformació propietat de governs estrangers a través de la SCA. De fet, no coneixem cap EUA. sol·licituds d'informació de les forces de l'ordre segons el SCA que busquen informació propietat d'un govern estranger. Això no és d'estranyar, ja que les directrius internes tant del DOJ com de l'Oficina Federal d'Investigació (FBI) es dirigeixen a fer aquestes sol·licituds. El desembre de 2017, el DOJ va emetre una guia disponible públicament que desaconsella als fiscals buscar informació dels proveïdors de serveis al núvol i, en canvi, aconsella als fiscals, sempre que sigui possible, que buscar informació directament del client propietari de la informació. 4 Per la seva banda, la Guia d'Investigacions i Operacions Domèstiques de l'FBI preveu restriccions específiques contra l'ús de l'SCA per sol·licitar informació r elating a les capacitats, intencions i activitats dels governs estrangers, tret que ho facin , entrarien dins de la missió bàsica de seguretat nacional de l'FBI. 5è.

Finalment, sabem que la millor manera de protegir el contingut, tant si s'emmagatzema al núvol com en qualsevol altre lloc, és fer-lo inaccessible per a tercers no autoritzats. És per això que proporcionem eines i serveis avançats d'encriptació que els clients poden utilitzar per protegir el seu contingut en el núvol i per què els clients poden triar entre una sèrie de ions soluts de xifrat compatibles amb tercers quan utilitzen serveis AWS. El contingut del núvol que s'ha xifrat es deixa inútil sense les claus de desxifrat aplicables. A més, la Llei CLOUD prohibeix expressament als acords executius crear qualsevol obligació que els proveïdors de serveis en el núvol be siguin capaços de desxifrar contingut.

# Proteccions per a governs estrangers

En conjunt, creiem que l'abast circumscrit de la Llei CLOUD, combinat amb les proteccions legals, estructurals i pràctiques disponibles per la llei, pot salvaguardar la contingut al núvol dels governs estrangers sobirans, alhora que s'estableix un marck per a la cooperació internacional en la lluita contra la delinqüència.

1. Guia DOJ disponible a [https://www.justice.gov/criminal-ccips/file/1017511/download.](https://www.justice.gov/criminal-ccips/file/1017511/download)
2. Extracte de la Guia d'Investigacions i Operacions Domèstiques de l'FBI 2013:

9.9 (U) MÈTODES D'INVESTIGACIÓ NO AUTORITZATS DURANT UNA INVESTIGACIÓ D'INTEL·LIGÈNCIA ESTRANGERA POSITIVA COMPLETA [*Èmfasi en l'original*]

No es permeten els següents mètodes d'investigació a be utilitzats amb la finalitat de recollir intel·ligència estrangera positiva d'acord amb els requisits de recollida de PFI:

. . .

H) (U//FOUO) *Comunicacions bancàries i electròniques*  emmagatzemades  *i* registres  *transaccionals.* (Article 18.6.8) [*Referit a la SCA*]

1. Veureper exemple, [https://www.aclu.org/sites/default/files/field\_document/2010-10-25-AmazonvLay-Comanda.pdf](https://www.aclu.org/sites/default/files/field_document/2010-10-25-AmazonvLay-Order.pdf) Un[d http://www.wiwd.uscourts.gov/opinions/pdfs/2006-2009/07-GJ-04-11-23-07.PDF](http://www.wiwd.uscourts.gov/opinions/pdfs/2006-2009/07-GJ-04-11-23-07.PDF)  [↑](#footnote-ref-1)
2. Veure Per exemple,., Permanent Missió de L'Índia a el Regne Nacions v. Ciutat de Nova York. aNd Argentí República v. Amerada Hess Navili Corp. [↑](#footnote-ref-2)
3. RJR Nabisco, Inc. v. Europeu Cmty. [↑](#footnote-ref-3)