Analys · 25 maj 2026

← Föregående·Nästa →

Self-hosting som professionell praxis

En server är inget annat än en dator. Frågan är inte om man ska ha en, utan var kundernas data bor, vem som underhåller dem och vem som bär ansvaret när något brister.

Kort sagt: Dina data bor alltid på någons dator: på en jättes, som du anförtror allt till, på en hyrd som du själv administrerar, eller på din egen. Ju mer kontroll du vill ha, desto mer ansvar tar du på dig. Att delegera till en stor tredje part lugnar, men fritar inte: informationen är din —och dina kunders—, och den ansvariga är du.

Frågan mellan molnet och källaren

Det är bra att börja med att avmystifiera ett ord som skrämmer utan anledning: server. En server är inte en mystisk maskin i ett kylt rum. Det är helt enkelt någon annans dator —eller din egen— som lagrar information och levererar den till den som ber om det. I decennier förvarade vi våra kunders information i en mapp, i ett arkivskåp, på skrivbordet, och ingen låg sömnlös över det. Information var inte skrämmande för att den var på papper; den behöver inte vara det bara för att den är på en disk heller.

«Molnet» är inte heller eteriskt. Det är ett företags dator, nästan alltid långt borta och nästan alltid någon annans. Jag lärde mig det oavsiktligt den dagen då jag, i förlitan på att mina filer var i säkert förvar i Google Drive, upptäckte att mappen på min dator inte innehöll mina dokument, utan genvägar till dokument som bodde någon annanstans. Om det andra stället bestämde sig för att stänga, ändra priset eller säga upp tjänsten, skulle mitt lugn ha försvunnit med det. Jag ägde inte mina saker; jag hade tillstånd att få åtkomst till dem.

Därifrån föds frågan i detta Häfte, enklare att formulera än att besvara: var bör dina klienters data bo? Och dina egna? Den offentliga samtalet framställer den som om det bara fanns två motstridiga svar — de stora plattformarnas moln eller att sätta upp det själv —, nästan en fråga om vilket läger man tillhör. Men det är inte två vägar: det är tre, och ingen av dem är en trosakt. Lästa i lugn och ro har de fler nyanser och kräver mer än det verkar.

Detta angår dig, oavsett vad du säljer

Det är lätt att tro att konfidentialitet är en sak för advokater, läkare eller journalister, och att resten inte har något att dölja. Det är ett fel, och ett dyrt sådant. Nästan varje verksamhet lagrar data om sina kunder som lyder under lagen, och många lagrar, utan att veta om det, information som är långt mer känslig än den verkar.

En soffaffär antecknar namnet, adressen och telefonnumret på den som köper; finns det finansiering, även dennes ekonomiska uppgifter. Ett renoverings- eller inredningsföretag bevarar foton av insidan av sina klienters hem och de fullständiga ritningarna över deras bostäder. Ett städföretag hanterar ritningarna över de kontor det städar, ofta markerade med färger och siffror som anger vilken anställd som går in var, vid vilken tid och med vilken nyckel. Inget av detta verkar vara mycket förrän man frågar sig för vem annars det skulle ha värde: dessa städritningar är, sedda med andra ögon, den perfekta kartan för den som vill ta sig in för att stjäla.

Att en verksamhet är liten, eller att den säljer soffor istället för att föra rättsprocesser, gör inte dess data värdelösa eller att lagen slutar gälla för den. Det gör bara att ägaren tenderar att tänka mindre på det. Och att tänka lite på

något som är ditt ansvar är precis där problemen börjar.

Var bor dina data?

På den frågan finns det i grund och botten tre svar. Och det är värt att minnas att »datan« inte bara är en klients dossier eller bunten av fakturor och offerter: det är också dina samtal med honom — via WhatsApp, via en professionell chattjänst, via Solo2. De tre svaren som följer är inte renhetsgrader eller en stege från goda till onda: de är tre sätt att fördela samma sak, kontrollen och ansvaret.

Att delegera allt till en leverantör. Det är det vanligaste, och för de flesta är det det enda de känner till. Jag lägger allt i Google Workspace eller Microsoft 365 och anförtror det helt och hållet åt leverantören. Jag betalar min avgift och slutar tänka på det. Den mest extrema formen av detta är de tjänster där du inte ens kommer åt att ha dina egna data: vissa faktureringsprogram i molnet sparar till exempel dina fakturor och offerter — och fungerar mycket bra —, men informationen lever i deras system, inte i ditt. Så länge du betalar har du tillgång; den dag du lämnar upptäcker du att det är svårt eller omöjligt att ta med dig din egen historik. Att hålla dina data halvt som gisslan är för mer än en leverantör just det som hindrar dig från att gå till konkurrenten. I utbyte mot bekvämlighet lämnar jag ifrån mig kontrollen och — utan att säga det högt — känslan av att ansvaret inte längre är mitt. Här ryms en nyans som nästan aldrig görs: att delegera är inte synonymt med amerikanskt. Jag kan delegera allt lika bekvämt till en europeisk leverantör — Infomaniak, till exempel — och med ett enda slag lösa en stor del av tvivlen kring internationella överföringar som vi såg i »Schrems II«, utan att hosta något själv. Det är inte USA mot resten av universum: inom den rena delegeringen finns det redan beslut som har betydelse.

Hyra och hantera din egen server. Jag har samma sak som Microsoft eller Google skulle ge mig, men jag sätter upp det själv. Jag hyr en server hos en europeisk leverantör —Hetzner, OVH, Scaleway—, installerar fri programvara (Nextcloud för filer, till exempel) och administrerar resultatet själv. Jag får reell kontroll: jag vet vad som körs, var och varför. Men maskinen befinner sig fortfarande i datasentret hos en tredje part och framför allt ändras det vem som bär konsekvenserna. Genom att delegera har du någon att klandra om något går fel. Genom att hantera det själv är det högst troligt att felet är ditt.

Ha det på din egen dator. Detta är alternativet som nästan ingen berättar om, och det är hjärtat i detta häfte. Man behöver inte en enorm server som står på dygnet runt inuti ett makrodatalager för att hosta sina saker. Din kontorsdator är redan en server: den tjänar dig. Du låter den stå på på kontoret och kopplar upp dig till den från din bärbara dator hos en kund, eller från mobilen när du är hemma. Vi kallar den «kontorsdatorn», inte «servern», men den gör exakt samma sak som de två föregående alternativen. Kontrollen är maximal och närheten likaså: dina data är där du är. Baksidan, sagt utan omsvep, är att ansvaret också är maximalt. Om strömmen går finns det ingen tekniker i tjänst i Nürnberg: det är ditt jobb att fälla upp säkringen. Och för att den datorn ska vara tillgänglig utifrån behövs något som bygger bro mellan din bärbara dator och den. Det är inte magi, och det är bra att veta innan man väljer denna väg.

Och du behöver inte ens återanvända kontorsdatorn: det finns en enhet utformad just för detta, NAS:en (tillverkad av Synology, QNAP och andra). Liksom nästan allt vi har sett i dessa Cuadernos finns det ingen magi inuti: det är en specialiserad dator, samma typ av maskin som du skulle hyra i ett datacenter, fast byggd för att lagra data och servera den över nätverket, utan bildskärm eller tangentbord emellan. Anslut en skärm och ett tangentbord och du har en vanlig dator; installera rätt programvara på din dator och du har en NAS. Skillnaden är att NAS:en kommer klar att användas. Du köper den, du ansluter den hemma eller på kontoret, och den är din. Du betalar ingen månadsavgift; du betalar en gång och den är din, som vilket annat verktyg i din verksamhet som helst. Du sätter på den, stänger av den, tar med dig den någon annanstans om du vill. Och eftersom den är din finns det inget som hindrar dig från att ha två —en hemma, en på kontoret— eller tre, genom att lägga till en på en säker plats, synkroniserade med varandra: din egen redundans, utan att vara beroende av att en tredje part underhåller den. Egen drift är i slutändan inte en enda sak: det är en kombination av maskiner, av ägande, av platser och av programvara.

Här är det oundvikligt att nämna det vi gör, och vi gör det utan förklädnad: hos Solo2 är det applikationen själv som slår den bron. Datorn på ditt kontor förblir åtkomlig endast för dina betrodda enheter, och alltid under

kryptering, och dina övriga apparater återansluter till den av sig själva. När en klient talar med dig är det din dator — inte en tredje parts — som talar med klienten. Vi löser inte strömavbrottet; vi löser bron. Och vi är inte ensamma: för nästan varje behov finns det i dag program — fria eller proprietära — som möjliggör just detta, att ha datan på din egen utrustning och nå den utifrån. Vårt är ett exempel; det viktiga är idén, inte varumärket.

Redundans är ingen superkraft

Här uppstår den omedelbara invändningen, och den är rimlig: om jag har allt på kontorsdatoren, vad händer om den går sönder? Frågan är god. Svaret är att det säkerhetsnät vi föreställer oss hos de stora leverantörerna är mer blygsamt —och lättare att efterlikna— än det verkar.

När jag lämnar mina data i datacentret hos ett multinationellt företag litar jag på att de har kopior på flera ställen. Och troligtvis har de det: på en andra plats, kanske på en tredje. Men den redundansen är inte oändlig och framför allt är den inte min: det förblir en hårddisk som jag inte äger, hanterad av någon som jag visar ett förtroende jag nästan aldrig verifierar.

Samma nät kan jag väva själv, och med en avgörande fördel. Min dagliga tjänst bor på kontorsdatoren. Därifrån lagrar jag en krypterad kopia på ett vänligt företags dator —en kollega i yrket, ett annat betrott kontor— och en annan krypterad kopia, om jag vill, hos samma europeiska leverantör som vi pratade om. Skillnaden är allt: det jag lämnar ute är inte min tjänst eller mina data i klartext, utan en krypterad kopia som bara jag kan öppna. Den externa leverantören förvarar en låst kista som vederbörande inte har nyckeln till. Jag anförtror honom inte min information: jag anförtror honom några bytes som utan mig inte betyder någonting.

Det var säkert tills det inte var det längre

Låt mig berätta en personlig historia, för den illustrerar detta bättre än något argument. I mer än tio år var jag en trogen kund hos CrashPlan, en tekniskt sett extraordinär säkerhetskopieringstjänst. Jag säkerhetskopierade alla mina datorer och min familjs datorer —företagets och hemmets, allt— i deras moln, med versioner som jag kunde återställa med den frekvens jag önskade, och resa tillbaka i tiden till en specifik fil från månader tidigare. Efter den första kopian överförde den bara skillnaderna, krypterat och komprimerat, så att jag höll en enorm säkerhetskopia uppdaterad med nästan ingen ansträngning. Det räddade mig många gånger, från ett obetydligt dokument till en hel disk. Priset steg under åren och jag brydde mig inte: jag betalade med glädje.

Vad jag inte visste var att CrashPlan hade gjort ett räknefel: de hade lovat obegränsat lagringsutrymme genom kontrakt, både i utrymme och tid. Och utrymme multiplicerat med tid —år av historik, versioner var femte minut — växer tills det blir ohållbart. En dag meddelade de oss alla att tjänsten upphörde. De gjorde det med elegans och med en generös tidsfrist, nästan ett år, och gav oss medel att ladda ner vårt eget. Men vart går man med mer än tio år av versionerade kopior av alla sina diskar? Där upptäcker man att man varken har ett sätt att ladda ner allt eller någonstans att göra av det, och att även om man kunde, skulle det nya lagret kosta en förmögenhet.

Jag räddade fyra oumbärliga saker. Resten försvann när de slog av strömbrytaren. Jag var lugn, min information var i säkerhet... tills den slutade vara det. Och inte på grund av ett svek: CrashPlan uppförde sig oklanderligt — till skillnad från Evernote, som år senare uppförde sig skamligt —; helt enkelt beslutade min skyddsängel i molnet, med all rätt, att sluta vara det. Resultatet var för mig identiskt: det jag trodde var säkert försvann.

Det denna historia verkligen lär oss har mer med mänsklig natur att göra än med teknik. När man känner att något är ens eget ansvar agerar man förebyggande: man tar kopior, säkrar ryggen, är misstänksam med gott omdöme. När man —felaktigt— tror att ansvaret bärs av en stor och solid tredje part, slappnar man av och låter det bero. Det delegerade lugnet är inte försiktighet: det är, utan smink, en form av oansvarighet.

Att betala är inte samma sak som att följa regler

Den tysta oansvarigheten liknar mycket den hos föräldrar som skriver in sin son på den dyraste skolan, betalar för en masterutbildning efteråt, och med det tror att de har uppfyllt sin plikt. De har inte uppfyllt sin plikt. Att vara förälder är att oroa sig för vad han lärt sig idag, om det han inte förstår, om hans värderingar, om hans självförtroende. Om den sonen vid tjugofem års ålder inte vet hur man arbetar eller beter sig, är felet inte skolans som tog emot pengarna: det ligger hos den som delegerade och betalade i tron att det räckte. Att betala en tredje part befriar inte från ansvar. Det har det aldrig gjort.

Med data är det likadant, och den nutida historien bekräftar det. För femtio eller hundra år sedan förvarade en yrkesperson sina klienters saker i mappar, på sitt kontor eller hemma, och kände sig ansvarig för dem. Sällan gick något förlorat. Vi har gått över till den digitala världen och laddar, med häpnadsväckande lätthet, upp allt till »molnet« — som inte är något annat än ett multinationellt företags dator — och slutar bekymra oss. Och ofta inträffar olyckor, och det finns företag som förlorar allt, och då säger man: det var Googles fel, det var Microsofts fel. Nej. Informationen är din, eller dina klienters, men den ansvarige är du.

Att hosta sina egna saker är inget tekniskt infall: det är att återfå det lugn som fanns för decennier sedan, det att veta var varje sak är och varför. Dataskydd har under tiden upplevt en tvär pendelrörelse —från frånvaron av alla regler, när vem som helst utan eftertanke visade upp en kunds data, till ett krav som faller med oproportionerlig hårdhet på den minsta, frilansaren som ger en kunds telefonnummer till budet. Jag diskuterar inte målet; jag observerar missförhållandet. Men missförhållandet fritar oss inte: den dag myndigheterna har medel att spåra och sanktionera i stor skala, kommer storlek att sluta skydda någon, och det är klokt att inte vänta på den dagen med ett oorganiserat hus. Att ha data under egen kontroll hjälper till att följa regler och hjälper till att bevisa det. Och framför allt sätter det tillbaka saker på sin plats: när informationen är din, är ansvaret helt och hållet ditt —det finns ingen tredje part att skylla på, inte heller en tredje part vars misslyckande exponerar dig—.

Ansvaret skyddar också

Det vore ohederligt att måla detta utan skuggor. Att inta mellanhandens plats innebär att bära dess börda: att hålla säkerhetskopior uppdaterade, att tillämpa uppdateringar och ett juridiskt ansvar — RGPD:s — som i själva verket aldrig helt upphörde att vara ditt (fotnotsreferenserna anger artiklarna i detalj). Det finns arbete, och det finns en dag då något brister vid en olämplig tidpunkt. Vi döljer det inte.

Men rädslan som omger det ordet, ansvar, är felkalibrerad. Det är mycket lättare att förlora dina filer i en molntjänst som stänger, eller dina foton i Google Foto, än att förlora den mapp med viktiga dokument du har på din egen dator: den du vet var den finns och vars frånvaro du skulle märka så snart den försvann. Det du känner som ditt vårdar du; det du tror är i säkerhet i någon annans händer försummar du.

Tänk på forna tiders fotoalbum, de av framkallat papper förvarade i en låda. Har du någonsin hört någon säga att de »förlorade« sitt familjealbum? Man hör talas om huset som brann med albumet inuti; att bara förlora det, nej. Och däremot, folk som hade alla sina foton i Google Foto eller i Apple Foton och blev kvar med ingenting: den historien återkommer med några månaders mellanrum, eftersom de trodde att det var i säkerhet. Google Foto vårdar dina foton, javisst; men det vårdar dem inte som föräldrar vårdar albumet där deras barn och barnbarn finns. Den skillnaden åtgärdas inte av något datacenter: ansvar, när det är ditt, är inte bara en börda; det är också den bästa garantin.

Fyra frågor innan du bestämmer dig

Om du överväger att ta steget, i vilken form som helst, är det bra att först svara på fyra frågor med nykter ärlighet:

1. Vilken del av dina data skulle det göra ont att förlora, eller att inte kunna ta med dig? Och akta dig för att avfärda det »rutinmässiga«: fakturahistoriken verkar vara det mest prosaiska i världen tills du byter program och upptäcker att de fakturorna tillhörde leverantören, inte dig — att du i bästa fall kan skriva ut

dem till PDF, utan att längre kunna söka i dem. Det är inte bara en fråga om känslighet: det handlar om vem det du behöver bevara i själva verket tillhör.
2. Vilket alternativ står i proportion till din verkliga tekniska förmåga? En välskött egen dator är inom räckhåll för vem som helst; att administrera en hel server, inte lika mycket. Var ärlig om vad du kan och vad du inte kan. Och kom ihåg att mellan att sätta upp en hel server och att delegera allt finns det ett mycket rimligt mellanläge: program — fria eller proprietära — som sparar dina data på din egen utrustning och låter dig nå dem utifrån. För många människor är det den bästa balansen.
3. Vilken plan har du för den värsta dagen? Ett dataintrång, en disk som dör, en leverantör som stänger, teknikern är sjukskriven. Om planen börjar med «det borde inte hända», är det ingen plan.
4. Skulle du veta hur du bevisar att du följer reglerna om du blev inspekterad imorgon? Att göra det bra och att kunna bevisa att man gör det bra, är inte samma sak. Lagen kräver det senare.

Det finns inget universellt svar. Det finns ett proportionerligt svar, antaget med ärlighet om vad som vinns och vad som ärvs. Och höjt över tekniken, en enkel visshet: dina data bor i någons dator. Den enda frågan som verkligen betyder något är vem du vill ska äga den datorn.

Självhosting är varken en dygd eller en last: det är ett verktyg med ett konkret avtryck av förmågor och ansvar. Frågan var aldrig om du skulle hosta dina egna data, utan vilka data, hur och med vilket stödnätverk. Att återfå kontrollen över data är inte att återvända till källaren eller att misstro allt: det är att återgå till att känna sig ansvarig för det som är vårt, precis som när dessa data bodde i en mapp på skrivbordet. Det ansvaret, rätt förstått, är den verkliga tjänst som en professionell person utför åt sina kunder.

Källor och vidare läsning

- Förordning (EU) 2016/679 — artikel 28 (personuppgiftsbiträde), artikel 32 (säkerhet vid behandling), artikel 33 (anmälan om personuppgiftsincident), artikel 37 (utnämning av dataskyddsombud).
- Den spanska datainspektionen (AEPD) — *Praktisk guide för riskanalys vid behandling av personuppgifter* (nuvarande version). Ramverk för personuppgiftsansvariga som åtar sig egna tekniska funktioner.
- Europeiska dataskyddsstyrelsen — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Tillämplig även för proportionalitetsbedömning vid beslut om egen infrastruktur.
- Europeiska kommissionen — offentlig förteckning över leverantörer av informationstjänster etablerade inom europeisk jurisdiktion. Administrativ utgångspunkt för att identifiera europeiska hanterade hosting-möjligheter.
- Nextcloud GmbH (Tyskland) — *Nextcloud Enterprise architecture and compliance documentation*. Dokumenterat fall av fri programvara med självhostade och hanterade lösningar via europeisk leverantör; användbart som teknisk referens för ett projekt som stöttats inom europeisk jurisdiktion sedan 2016.

← FöregåendeDe 24 orden: vad en kryptografisk identitet ärNästa →Verklig vs skenbar integritet: Frågorna man bör ställa sig

Senaste läsning

- Reflektion · 29 juni 2026 Du är inte anonym
- Reflektion · 27 maj 2026 Det en signatur inte kan fixa
- Analys · 26 maj 2026 Verklig vs skenbar integritet: Frågorna man bör ställa sig

Ta med dig den här artikeln dit du behöver den.

↓ Markdown ↓ Klartext ↓ PDF

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 ae0f013f75b224c24117029a0ea2edbd12aa4838a327a698961867fbdefd3333

Cuadernos Lacre · En utgåva från Menzuri Gestión S.L. ·
skriven av R.Eugenio · redigerad av teamet bakom Solo2.

Denna webbplats använder inte cookies. Allt som din webbläsare laddar är skrivet eller övervakat av oss och placerat på våra europeiska servrar: den anonyma besöksräknaren (Umami, självhostad) och det minimala JavaScript som krävs för språkväljaren och din inställning för ljust eller mörkt tema, som sparas på din egen enhet. Inga resurser från externa företag, inga trackers, ingen profilering, ingen datadelning. Om du vill följa oss: RSS.