Reflektion · 16 maj 2026

← Föregående·Nästa →

Tystnadsplikten i den digitala tidsåldern

När kommunikationen mellan yrkesutövaren och klienten sker via en tekniskt olämplig kanal bryts inte hemligheten den dag läckan sker. Den bröts långt tidigare, i det ögonblick verktyget valdes.

Ett problem som nästan ingen ser

En advokat tar emot ett känsligt dokument från en klient på sin telefon. En läkare diskuterar en känslig diagnos med en kollega. En psykolog samordnar en patients behandling med en psykiater. En skatterådgivare skickar uppgifter för en deklaration som ska granskas. Alla gör det via snabbmeddelanden. Och nästan ingen stannar upp för att tänka på var dessa meddelanden egentligen hamnar.

Svaret är i de flesta fall detsamma: på en server som yrkesutövaren inte kontrollerar, i ett land vars lagstiftning denne inte nödvändigtvis känner till, hanterad av ett företag vars affärsmodell är – i direkta ekonomiska termer – att samla in data. Meddelandet kan vara krypterat under transport. Men när det väl når servern är det en kopia lagrad i en tredje parts infrastruktur, underkastad denna tredje parts operativa, juridiska och kommersiella beslut. Inte yrkesutövarens.

Vad lagstiftningen säger

Den europeiska dataskyddsförordningen är entydig i sin artikel 32: den som behandlar personuppgifter måste vidta "lämpliga" tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Åtgärdernas lämplighet bedöms inte mot "vad appen säger att den gör", utan mot den faktiska risken. Om en klients uppgifter hamnar på en server vars jurisdiktion inte garanterar en skyddsnivå som motsvarar den inom Europeiska ekonomiska samarbetsområdet, tar den personuppgiftsansvarige – det vill säga yrkesutövaren – en risk som denne sannolikt inte är helt medveten om.

Och det är inte bara GDPR. Tystnadsplikten, som är specifikt reglerad för advokater, läkare, psykologer, revisorer, journalister med flera, kräver att kommunikationen med klienten är konfidentiell. Inte "konfidentiell så långt det är möjligt". Konfidentiell utan förbehåll. Om den tekniska kanal som används inte kan garantera detta, tar yrkesutövaren en risk som dennes yrkesetik inte tillåter.

Paradoxen är att risken är osynlig. Ingen granskar kontorets meddelandehantering. Ingen ber om personuppgiftsbiträdesavtalet från chattjänsten. Risken framträder först när det är för sent: en läcka, ett publicerat intrång, ett domstolsbeslut som verkställts på en annan kontinent utan att användaren meddelats.

Vad en yrkesutövare behöver tekniskt

Vad en person med tystnadsplikt behöver är egentligen förvånansvärt enkelt ur kravsynpunkt:

- En kanal där meddelandena går direkt från sändarens enhet till mottagarens, utan att passera en mellanliggande server som lagrar kopior.

- En infrastruktur vars jurisdiktion och policyer är anpassade till GDPR genom konstruktion, inte genom deklaration.
- Ett sätt att identifiera sig för samtalspartneren utan att behöva lämna ut yrkesmässiga kontakter (klientnamn, telefonnummer, kontaktbok) till tredje part.
- Ett verifierbart system – inte baserat på leverantörens ord – för att bekräfta att meddelandet nådde rätt person.

Det är ingen krävande lista. Det är i själva verket det som togs för givet i den fördigitala yrkeskommunikationen. Ett rekommenderat brev uppfyllde alla dessa kriterier. Ett telefonsamtal från kontorets växel till klientens likaså. Det märkliga är inte att dessa garantier krävs idag: det märkliga är att de har gått förlorade i övergången till den digitala kanalen, utan att någon märkte det.

Skillnaden mellan att kryptera och att inte lagra

Det finns en användbar metafor. Att kryptera ett meddelande och spara det på en server motsvarar att lägga ett dokument i ett kassaskåp och lämna kassaskåpet hemma hos en främling. Kassaskåpet är bra. Dokumentet kan i princip inte läsas. Men dokumentet *finns fortfarande kvar hemma hos någon annan*. Och denne andre kan få ett domstolsbeslut, utsättas för en IT-attack, ändra sina användarvillkor, köpas upp av ett annat företag med annan etik, eller försvinna imorgon.

Det strukturella alternativet – inte procedurellt, inte genom förtroende – är att dokumentet aldrig lämnar kontoret. Att det färdas direkt från yrkesutövarens bord till klientens bord, utan någon mellanhand. Det är vad punkt-till-punkt-kommunikation mellan enheter gör tekniskt: det eliminerar mellanhanden. Inte för att mellanhanden är ond. Utan för att mellanhanden är *onödig* när det gäller tystnadsplikt. Och det onödiga måste, i alla system som strävar efter att vara säkra, elimineras av princip.

Frågan om ansvar

I slutändan är frågan som varje yrkesutövare med tystnadsplikt bör kunna svara på med ett rungande ja följande:

> Om en konversation med en av mina klienter läcker ut imorgon och en domstol eller ett yrkesförbund frågar mig hur jag hanterar konfidentialitet, kan jag då tekniskt bevisa att den kanal jag använde inte lagrar kopior i tredje parts infrastruktur? Kan jag bevisa att data aldrig lämnade enheterna hos de två personer som deltog i konversationen? Kan jag bevisa, utan att förlita mig på ett företags ord från en annan kontinent, att konfidentialiteten garanterades av arkitekturen och inte av ett löfte?

Om svaret är nej är problemet inte det enskilda verktyget. Problemet är att man har delegerat ett ansvar till ett verktyg som verktyget inte var designat för att hantera. Det är som att lägga konfidentiella akter i ett genomskinligt kuvert och lita på att brevbäraren inte tittar.

Verktyget en yrkesutövare väljer för att kommunicera med sina klienter säger mycket om hur denne värderar deras förtroende. Det finns verktyg designade för att detta förtroende inte ska hänga på löften, utan på arkitekturen. Och så finns det verktyg som inte är det. Att känna till skillnaden är en del av arbetet.

Citerat regelverk

- Förordning (EU) 2016/679 (GDPR), särskilt art. 5, 25 (inbyggt dataskydd) och 32 (säkerhet vid behandling).
- Rättegångsbalken (1942:740) 36 kap. 5 § (Vittnesförbud för vissa yrkesutövare).
- Brottsbalken (1962:700) 20 kap. 3 § (Brott mot tystnadsplikt).
- Patientsäkerhetslagen (2010:659) 6 kap. 12 § (Tystnadsplikt för hälso- och sjukvårdspersonal).

← FöregåendeKryptering är inte integritet: vad metadata berättar om digNästa →GDPR och professionell messaging: varför de flesta bryter mot reglerna utan att veta om det

Senaste läsning

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 04aeb1c998921728b241ee8b86130949da3dedf148f75cf8fdc56f9b8170bf67

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