

## כש'אין אף אחד באמצע

הצפנת מה שעובר דרך שרת מגינה על התוכן. אי-קיום שרת באמצע מבטל את השאלה. אלו אינם דברים זהים.

**במילים פשוטות:** כשאתה מדבר פנים אל פנים עם מישהו, אף אחד אחר לא צריך להבטיח לך שהוא לא הקשיב. הוא לא הקשיב כי הוא לא היה שם. זו הגרסה החזקה ביותר של פרטיות: לא ההבטחה של מתווך להתנהג יפה — אלא היעדר המתווך.

### שני אנשים, שיחה אחת

כששני אנשים מדברים פנים אל פנים בחדר, אף אחד אחר לא צריך להבטיח שהוא לא שמע כלום. הוא לא שמע כי הוא לא היה שם. כששני אנשים מעבירים פיסת נייר מיד ליד, אף אחד באמצע לא צריך להישבע שהוא לא קרא אותה. אין אף אחד באמצע.

רוב הדברים בחיי היומיום פועלים כך. איננו חותמים על הסכמי סודיות עם האוויר המעביר את קולנו, ולא עם הנייר שאנו מחזיקים. פרטיות השיחה אינה נשענת על הבטחה של מתווך, כי אין מתווך. זוהי אחת הצורות החזקות ביותר של פרטיות הקיימות: לא בגלל שמהו או מיישהו מתנהג יפה, אלא בגלל שאין משהו או מיישהו.

כאשר השיחה עוברת לערוץ דיגיטלי, זה משתנה כביררת מחדל. המודל הרגיל הוא הבא: שני אנשים מתחברים לשרת, השרת מקבל את ההודעה, מצפין אותה או שומר אותה מוצפנת, ומוסר אותה לנמען. השרת נמצא באמצע. השרת יכול להיות ישר. ניתן לבצע בו ביקורת. הוא יכול לפעול בתחום שיפוט נוח ותחת מדיניות פרטיות קפדנית. כל זה יכול להיות נכון. אבל השרת נמצא באמצע.

### ההבדל בין הצפנה לבין אי-איסוף (חלק שני)

במאמר קודם בסדרה זו טענו שהצפנת התוכן ואי-איסוף מטא-נתונים אינם אותו דבר. ישנו צעד נוסף שכדאי לנסח בבירור: הצפנת מה שעובר דרך שרת ואי-קיום שרת אינם אותו דבר גם כן.

המודל הראשון — שרת באמצע, תוכן מוצפן — מגן על התוכן מפני מפעיל השרת, צוות התחזוקה שלו, או תוקף חיצוני שיפרוץ למערכת. וזה חשוב. אבל זה לא מבטל את השרת. השרת עדיין שם. הוא ממשיך לעבד מטא-נתונים. הוא נשאר נקודה שיכולה לקבל דרישה שיפוטית, התערבות משפטית, לחץ פוליטי או פרצת אבטחה. הוא נשאר נקודה שדורשת מתן אמון במישהו.

המודל השני — אי-קיום שרת בין שני הקצוות — אינו מגן טוב יותר על התוכן המוצפן: אם הקריפטוגרפיה חזקה, התוכן מוגן בשני המקרים. מה שמשתנה אינו התוכן. מה שמשתנה הוא שהשאלה "מה קורה עם השרת?" מפסיקה להיות רלוונטית, כי אין שרת לשאול עליו.

### אמון, היעדרות, וההבדל ביניהם

האמון יכול להיות מונח במקומו. חברות ישרות קיימות. מבקרים קפדניים קיימים. חקיקות לטובת המשתמש קיימות. שירותים רציניים הממלאים בקפידה אחר כל האמור לעיל קיימים. אמון, כאשר הוא ניתן למפעיל שראוי לו, אינו הסדר רע.



הערת עורך: כאשר Cuadernos אלו נוקבים בשמות של חברות או מוצרים, זה לא כדי להאשים. אלו שבונים אותם עושים עבודה שמיליוני אנשים משתמשים בה ומעריכים אותה. מה שאנחנו מצביעים עליו הוא מבני — המודל, לא המותג. המותגים מופיעים כדוגמה כי הם אלו שהקורא מזהה.

## מקורות וקריאה נוספת

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. טקסט מכוון של העיקרון לפיו הערביות של מערכת צריכות להיות מיושמות בקצוות, לא בערוץ הביניים.
- תקנה (איחוד אירופי) 2016/679, סעיף 25 — הגנת נתונים כבר מהעישוב וכברירת מחדל.
- תקנה (איחוד אירופי) 2016/679, סעיף c.5.1 — עקרון מזעור הנתונים.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. פרקים על ארכיטקטורות הממזערות את האיסוף על ידי בנייה.

[← הקודם GDPR ותקשורת מקצועית: מדוע הרוב מפרים את הכללים מבלי לדעת זאת? Schrems II → חמש שנים אחרי](#)

## קריאות אחרונות

- [ניתוח · 18 במאי 2026 פרטיות אמיתית מול מדומה: השאלות שכדאי לשאול את עצמך](#)
- [ניתוח · 18 במאי 2026 Self-hosting כפרקטיקה מקצועית](#)
- [מושג · 18 במאי 2026 24 המילים: מהי זהות קריפטוגרפית](#)

קחו את המאמר הזה אתכם לכל מקום שתצטרכו.

[PDF ↓ טקסט פשוט ↓ Markdown ↓](#)

הקובץ יורד למכשיר שלכם. משם תוכלו לשמור אותו, לייבא אותו ל-Solo2 או לשתף אותו היכן שתמצאו. Cuadernos לא מחליטה על היעד עבורכם.

חותם שעווה · SHA-256 1e5707aed818ddf029530cf22fdec5287cfd10bcf1695bdc80f391f964ccf0d

· Cuadernos Lacre · פרסום של [.Menzuri Gestión S.L](#) · נכתב על ידי R.Eugenio · נערך על ידי צוות [Solo2](#).

אתר זה אינו משתמש בעוגיות ואינו טוען משאבי צד שלישי. הוא משתמש במונה ביקורים אנונימי באירוח עצמי (Umami), בשרת האירופי שלנו) ובמינימום ה-JavaScript הדרוש לשני פקדי הכותרת: ערכת נושא בהירה או כהה, ובורר שפה. ללא עוקבים, ללא פרופילציה, ללא שיתוף נתונים. אם תרצו לעקוב אחרינו: [RSS](#).