

PROTECT
THE
STACK

Infrastructure Providers Should Not Be Content Police

(The Stack): מגינים על ארסנל הכלים הטכנולוגי

ספקי תשתיות לא אמורים להיות משטרת התוכן

כיום מופעל לחץ גדול על ספקים של שירותי תשתיות אינטרנט 'להגדיל ראש' בשיטור על תכנים מקוונים ועל השתתפות המשתמשים ברשת. יש ספקים שכבר החליטו להתערב מיוזמתם. מדובר כאן במגמה מסוכנת שחייבת להיפסק כאן ועכשיו.

למרות שבנסיבות מסוימות אפשר להבין את הקריאה לספקי שירות להשתמש במלוא ארסנל הכלים שברשותם כדי לחסל שיה פוגעני ברשת, שימוש כזה יגרום למגוון תוצאות לא רצויות, במיוחד עבור המשתמשים המוחלשים ביותר. למעט בנסיבות חריגות ונדירות, אסור לממשלות לדרוש התערבויות כאלו, וספקי תשתיות אינם צריכים להתערב מיוזמתם.

רקע

המשתמשים וקובעי המדיניות מכירים היטב פלטפורמות כגון פייסבוק, טוויטר או YouTube. אך השירותים האלה אינם האינטרנט למעשה, התקשורת והמסחר המקוונים ברשת תלויים גם [במגוון רחב של ספקי שירותים](#), כולל ספקיות אינטרנט וחברות טלפון, כגון פרטנר, בזק בינלאומי, סלקום ו-Vodafone; סוכנויות לרישום שמות דומיינים כגון Namecheap או GoDaddy; שירותי תמיכה כגון Amazon Web Services (AWS), רשויות למתן תעודות (כגון [Let's Encrypt](#)); מעבדי תשלומים כגון PayPal ו-M-Pesa; שירותי דוא"ל, שירותי מסרים ועוד. כל הגורמים האלה ביחד מכונים לפעמים 'ארסנל הכלים הטכנולוגי' (Tech stack).

רוב המשתמשים באינטרנט אינם עוצרים לחשוב על שירותי התשתיות הנמצאים בבסיס השימוש הזה. אך השירותים האלה חיוניים עבור יכולת הביטוי, הפרטיות והאבטחה ברשת. וכאשר ספקי השירותים האלה – שלרבים מהם אין כמעט קשר עם המשתמשים – מתערבים באינטרנט על בסיס תוכן, לבהירות שלהם יכולות להיות השפעות עצומות בנוגע לזכויות אדם, השפעות שקשה מאוד או בלתי אפשרי לתקן אותן.

המלכודת והסיכונים הספציפיים לחופש הביטוי ולפרטיות עשויים להשתנות על פי אופי השירות המדובר. אבל על כל ספק תשתיות יחול שילוב כלשהו של החששות הבאים. כשמצרפים חששות אלה זה לזה, הם מדגימים מדוע, למעט במקרים חריגים נדירים, אסור לספקי תשתיות להתערב באכיפה ובשיטור של תכנים באינטרנט.

הערה בנוגע ל'ארסנל הכלים הטכנולוגי'

'ארסנל הכלים הטכנולוגי' (The Stack) הוא מונח מתחום מדעי המחשב והנדסת תוכנה שמתאר שילוב של כלים, תהליכים, שפות תכנות ומנגנונים המשמשים ביחד לבניית אפליקציה או מוצר. בהקשר הנוכחי, אנחנו משתמשים בביטוי זה כדי לתאר את האינטרנט כפי שאנו מכירים אותו, ואת ספקי השירות, הפלטפורמות, התהליכים וכל השחקנים האחרים שמאפשרים את קיומו של האינטרנט המודרני.

ספקי תשתיות לא אמורים להיות משטרת התוכן (The Stack): מגינים על ארסנל הכלים הטכנולוגי

‘ארסנל הכלים הטכנולוגי’ כולל פלטפורמות של תוכן שיוצרים המשתמשים כגון פייסבוק וטוויטר, וכן את מגוון ספקי התשתיות המתוארים למעלה. פלטפורמות מדיה חברתית שוכנות בחלקו העליון של ארסנל הכלים הזה, בעוד שספקי תשתיות ליבה, כגון ספק האינטרנט שלכם, נמצאים בתחתיתו. ביניהם יש מבחר רחב של מתווכים – כולל מעבדי תשלומים וסוכנויות רישום דומיינים.

הסיכונים לזכויות אדם

1. רוב שירותי התשתיות אינם מסוגלים להתאים את פרקטיקות ההתערבות שלהם כך שתהיינה חיוניות ופרופורציונליות.

לפלטפורמות יש לרוב מגוון רחב של [אפשרויות ניהול תוכן \(מודרציה\)](#). לעומת זאת, שירותי תשתיות רבים אינם מסוגלים למקד את התגובה שלהם באופן מדויק על פי סטנדרטים מדויקים של זכויות אדם. טוויטר חוסמת ציורים ספציפיים; Amazon Web Services מונעת שירותים מאתרים או מחשבונות שלמים, מה שאומר שההתערבויות שלה משפיעות בסופו של דבר על הרבה יותר מאשר התוכן הלא רצוי שגרם לה להגיב מלכתחילה. חטיפת שירותי תקשורת על ידי ממשלה כזו או אחרת במטרה להפריע לרשת האינטרנט של מדינה שלמה היא צעד גס במיוחד.

פעולות גסות מתרחשות גם ברמת הדומיין, כאשר סוכנויות רישום דומיינים שמתנגדות להתבטאות מסוימת באתר כלשהו אינן מתמקדות רק בהתבטאות הזו, אלא משעות ו/או מסירות את רישום האתר כולו. למשל, ארגון ARTICLE 19 תיעד מקרים רבים של [‘שימוש לרעה ב-DNS’](#): ההשעיה והסרת הרישום של שמות דומיינים כאמצעי להשתקת מחאה.

אנחנו גם יכולים ללמוד לקח מתחום זכויות היוצרים, שם ראינו כיצד סוכנויות רישום דומיינים וספקי אירוח אתרים [סוגרים](#) אתרים שלמים בתגובה להתראות בדבר הפרת זכויות יוצרים שכוונו רק למסמך בודד. יש אולי אפשרות ששירותים מסוימים יוכלו לתקשר ישירות עם לקוחות, כאשר הם מודאגים מפיסת תוכן ספציפית ומבקשים להוריד אותה. אך במקרה שהבקשה הזו תידחה, לרשות השירות עומד רק הכלי הקהה-מאוד של הסרה מלאה של האתר כולו. ויש שירותים שבכלל אין להם דרך לתקשר ישירות עם מקור התוכן.

2. רק לעתים נדירות קיימים תהליכים אפקטיביים של שליחת התראות וערעור על התראות, במיוחד כשמדובר באנשים מוחלשים יותר.

הסטנדרטים בנושא זכויות אדם ועקרונות ההליך המשפטי הנאות דורשים מספקי שירות להודיע למשתמשים על כך שהתבטאות ו/או החשבון שלהם הורדו – או יורדו – מהרשת, ולהציע למשתמשים אלה הזדמנות לערער על החלטה זו. ברמת התשתית, התראות ואפשרויות ערעור כאלה עשויות להיות בלתי אפשריות. לעתים קרובות, אין ביכולתם של שירותי תשתית לתקשר ישירות עם משתמשי האינטרנט, כי לרוב אין לשירותים האלה מערכת יחסים ישירה עם הדובר או עם קהל היעד בהקשר להתבטאות הבעייתית. ולעומת מארחי תוכן ברמת-הפלטפורמה, שיכולים להשאיר הודעת הסבר במיקום המקורי של הפוסט שהוסר, לספקי תשתית אין לרוב את היכולת להודיע למשתמשים עתידיים על הדרכים שבהן חסם ספק התשתית את הגישה לתוכן.

וכך, לדוגמה, אם משתמש כלשהו יגלה שקישור ששלח לו ידיד אינו עובד, הוא לא יהיה מסוגל לדעת בקלות אם הבעיה הייתה טמונה בקישור, אם הבעלים הורידו את האתר מרצונו החופשי, או אם האתר נחסם. גם משתמשים של שירות התלוי בחברה לעיבוד תשלומים עשויים להיות מופתעים מהיעלמותו של השירות, זאת כי, שלא בידיעתם, החברה הזו סגרה את התשלום לאותו שירות.

ספקי תשתיות לא אמורים להיות משטרת התוכן: (The Stack) מגינים על ארסנל הכלים הטכנולוגי

למשל, בארגנטינה נסגרו התשלומים ל-Uber בין לילה, זאת עקב [צו בית משפט](#) שדרש ממעבד התשלומים לחסום את התשלומים עבור שירות Uber.

המשתמשים כפופים למעשה לתנאים ולמגבלות של כל אחד מהשירותים בשרשרת, החל מהדובר וכלה בקהל היעד, למרות שברוב המקרים אין להם מושג מהם השירותים האלה או איך יוצרים איתם קשר. בהינתן ההשלכות הפוטנציאליות של הפרות, והקושי לנווט בין תהליכי הגשת הערעור נגד שירותים שפתאום נעלמו (בהנחה שיש בכלל תהליך כזה), משתמשים רבים פשוט יפסיקו לשתף דעות מעוררות-מחלוקת באופן גורף. בהמשך לכך, כאשר אין לספק השירות קשר ישיר עם הדובר או עם קהל היעד, הפתרון של הורדת האתר כולו תהיה הרבה יותר קלה וזולה עבורו כעסק מאשר ניתוח של הניואנסים בהתבטאותו הבעייתית של כל משתמש נתון.

3. התערבויות מבוססות-תוכן ברמת התשתית גורמות לנזק היקפי שיפגע באופן לא פרופורציונלי בקבוצות מוחלשות יותר.

בעלי כוח והשפעה ינצלו ללא ספק את כל מערכות הצנזורה שעומדות לרשותם כדי לדכא דעות ורעיונות לא פופולריים. ואכן, חסימת תשתיות היא כלי מועדף על ממשלות דיקטטוריות. במהלך חוסר השקט החברתי המתמשך באוקטובר 2019, משתמשי האינטרנט באקוואדור חוו [חסימות רשת תכופות](#). ניגריה דרשה מספקי אינטרנט [לחסום את טוויטר](#) במשך חודשים. הודות ליישום הרחב מאוד של סנקציות אמריקאיות, AWS [חסמה את שירותיה בפני משתמשים איראניים](#). Cloudflare [מנעה שירות](#) מאירוע של Mastodon שאירח קולקטיבי של עובדות מין מאוסטרליה, וציטטה תקנות אמריקאיות כהצדקה לכך. וכמובן שמדינות מסוימות סגרו את האינטרנט לגמרי.

יתרה מכך, גם מקבלי החלטות בעלי כוונות טובות לעתים קרובות אינם מעריכים היטב את זכות הדיבור של אנשי השוליים. ברמת הפלטפורמה, חברות העוסקות בניהול תוכן משקפות ומחזקות את ההטיה שלהן נגד קהילות מוחלשות. יש לכך דוגמאות רבות: [פייסבוק החליטה](#) באמצע תנועת #MeToo שהצהרה 'גברים הם זבל' מהווה שיח שנאה; [טוויטר החליטה להשתמש בתנאים במדיניות העוסקים בהטרדה](#) כדי לסגור את חשבונות המאומת של פעיל מצרי בולט נגד עינויים; החלטות רבות בנושא ניהול תוכן [מנעו מנשים לא לבנות](#) לשתף עם חבריהן ועוקביהן סיפורים של הטרדה שאותם חוו; טוויטר החליטה [לסמן ציוצים שכללו את המילה 'queer' כפוגעניים](#), ללא קשר להקשר שלהם.

גם חולים שאינם יכולים להרשות לעצמם תרופות מרשם מושפעים מכך. במאמץ [למשטר את השימוש במילה 'אופיואידים'](#) ובמילים קשורות בצירוף להאשטגים, אינסטגרם סגרה וחסמה חשבונות 'שנראה כאילו' מכרו אופיואידים. השלכה אחת הייתה סגירת החשבון של [PharmacyChecker](#), שירות שסיפק אימות ומידע על מחירים של בתי מרקחת מקוונים [שעזרו למטופלים ולאלה המטפלים בהם לקנות תרופות זולות יותר באמצעות ייבוא](#) אך שלא מכר תרופות בעצמו.

אין סיבה להניח שחברות תשתית יתנהגו טוב יותר מאשר פלטפורמות בקבלת החלטות כאלו, ויש סיבות רבות להניח שהן תהיינה אף גרועות יותר.

ספקי תשתיות לא אמורים להיות משטרת התוכן: (The Stack) מגינים על ארסנל הכלים הטכנולוגי

4. שחקנים מטעם המדינה או מהמגזר הפרטי עשויים לנסות לחטוף מסלולי התעבורה מבוססי-תוכן כדי להרחיב את שליטתם על התוכן.

מרגע שמסלולי התעבורה כאלה יזוהו וייחטפו, הם יספקו לשחקנים מטעם המדינה, לגורמים בחסות המדינה ולשחקנים פרטיים כלים נוספים לשליטה בשיח הציבורי. ומרגע שיפוחו או יורחבו תהליכים וכלים שנועדו לפגוע בחופש הביטוי, חברות יכולות לצפות למבול של דרישות להחיל אותם באופן מקיף יותר. ברמת הפלטפורמה, ייתכן ששחקנים של המדינה או בחסות המדינה כבר [פיתחו 'כלי נשק' המסוגלים להחריע על אי-הסכמה חברתית ולדאוג לסתימת פיות](#). חברת Cloudflare, המספקת מגוון שירותים, כולל הגנות מפני מתקפות DDOS, [מדווחת](#) שלאחר שהסירה שירותי אבטחה מאתר קונספירציות נאו-נאצי, היא החלה לזהות גידול במספר הבקשות מצד משטרים דיקטטוריים לעשות זאת גם עבורם בנוגע לארגוני זכויות אדם.

בהקשר של זכויות יוצרים, שחקנים פרטיים משתמשים באופן שוטף בתהליכים נוחים להורדת אתרים כדי להשתיק ביקורות. אין שום סיבה לצפות שדברים ישתנו כשמדובר ברמת התשתיות.

5. מחסור בתחרות, וכן עלויות המיתוג, מקשים ואף לא מאפשרים להטיל אחריות על חברות מסוימות בנוגע לשגיאות שאולי ביצעו או להשתדלות-יתר שלהן בנושא חסימות.

רוב חלקי העולם, כאשר ספק אינטרנט מחליט לסגור חשבון של משתמש ספציפי, אין בנמצא אף ספק אינטרנט חלופי: למעשה, משתמש כזה פשוט נבעט החוצה מהרשת. בכל השכבות האחרות של ארסנל הכלים הטכנולוגי (ה-Stack), למשל מערכת שמות הדומיינים (DNS), יש מספר ספקי שירות שניתן לבחור ביניהם – מי ששם הדומיין שלו הוקפא יכול לקחת את האתר שלו למקום אחר. אך אין די בקיומן של חלופות; צריך גם להכניס למשוואה את העלויות ואת מידת הקושי של החלפת ספקים. רק לעתים רחוקות יש חלופות זולות או קלות יותר. במספר אזורים עשוי להתקיים קשר הדוק בין שחקנים ברמת המדינה לבין חברות תשתית; למשל, ממשלת קניה מחזיקה ב-35% בעלות על חברת הטלקום Safaricom. ואפילו כאשר קל לבצע החלפת ספקים, זה לא יעזור אם כל הספקים ברמה מסוימת של ארסנל הכלים הטכנולוגי יחליטו, או שיופעל עליהם לחץ, לצנזר את אותו תוכן, את אותם דוברים ו/או את אותן נקודות מבט. לבסוף, הבעיה עלולה להחמיר אם ספקי השירות הם קטנים יותר, ועקב כך גם פגיעים יותר ללחץ מצד ממשלות ושחקנים פרטיים.

6. הדרישות להתעברות עשויות להיות לא מועילות.

התעברות שמטרתה היא השיח ברשת עשויה בפועל להזיק למטרות שהיא אמורה להשיג. למשל, מאמצים למשטר תכנים 'קיצוניים' הובילו בעבר לחסימה או למחיקה של תכנים של עיתונאים או פעילי זכויות אדם שעסקו בתיעוד טרור וזוועות אחרות. לחץ לחסום גישה לשירותי אינטרנט במדינות מסוימות [פגע במאמצים](#) לעזור לאנשים לעקוף צנזורה ממשלתית ולקבל גישה למידע מדויק.

7. התעברויות מבוססות-תוכן ברמת התשתית עשויות להזיק לפרוטוקולי אינטרנט בסיסיים ולפגוע באבטחה.

ספקי תשתיות לא אמורים להיות משטרת התוכן (The Stack): מגינים על ארסנל הכלים הטכנולוגי

התערבויות מבוססות-תוכן מסוימות מצד ספקי תשתית, למשל Deep Packet Inspection (או DPI) ברשת, או חסימת שאילתות DNS, עשויות לעצב-מחדש את ארכיטקטורת האינטרנט באופן שיפגע בפרטיות ובאבטחה. לדוגמה, אם מפעילי ציוד לפתירת כתובות DNS יתחילו להפנות שאילתות לדומיינים מסוימים רק בהתבסס על התוכן, זה עלול לסכך באופן מהותי את המאמצים להפוך את ה-DNS לחסין בפני 'התעסקות' זדונית – זאת עקב העובדה שמחשבים אינם מסוגלים להבדיל בין הפניות 'טובות' לבין ניסיונות לבצע חיקוי (spoof) של אתרים. אם ספקי רישיונות יחליטו לבטל תעודות דיגיטליות של אתרים מסוימים כי הם מתנגדים לתוכן שלהם, אזי 'שרשרת האמון' שבה תלוי חלק ניכר מאבטחת האינטרנט עשויה להיפגע. בנוסף לכך, התערבויות ברמת התשתית, היות והן מפרות עיקרון תכנון מרכזי של האינטרנט הפתוח, עשויות להאיץ את הפיצול (השבירה לרסיסים) של האינטרנט, שכן גורמים שונים יתחילו לבנות תשתיות חדשות במטרה לעקוף התערבויות כאלו, וספקי תשתית קיימים יאלצו להתחיל להתמודד עם כללים סותרים וחסימות במדינה אחת או אחרת על פי סוג הכללים שלהם מצייתות מדינות אלו.

8. כללים לא עקביים יהיו בלתי נמנעים.

ספקי תשתית, כמו כל ספקי השירות שפועלים על פני מספר תחומי שיפוט שונים, כבר מתמודדים עם דרישות סותרות המבוססות על הכללים והערכים של המדינות שבהן הם פועלים. הציות לכללים הסותרים האלה הוא יקר וגם בלתי אפשרי לפעמים. בכך שספקים כאלה יתחילו לעסוק בשיטור של תכנים, הם יזמינו סטים חדשים של מחויבויות שעשויות לגרום לסוג של 'מרוץ לתחתית', כלומר לחסימה של כמה שיותר תוכן שיידרש כדי לענות לדרישותיו של תחום השיפוט שמצנזר הכי חזק.

מסקנה

האינטרנט הוא משאב חיוני למיליארדי בני אדם ברחבי העולם. אנו משתמשים בו כדי לתקשר, לארגן, למחות, לעבוד, ללמוד, לקנות ולמכור, לקבל גישה לשירותים ממשלתיים ועוד. אם אנו מצפים שהאינטרנט ימשיך למלא את התפקיד הזה, עליו להיות חזק, גמיש ומאובטח. אנו זקוקים לכך שספקי התשתית ימשיכו להתמקד במשימת הליבה שלהם: תמיכה באינטרנט מוצק וגמיש. המשימה הזו היא הרבה יותר חשובה, וגם מגנה הרבה יותר טוב על זכויות אדם, מאשר הניסיון ליצור תהליכי התערבות מבוססי-תוכן שבסופו של יום יגרמו ליותר נזק מתועלת.

על החתום

Access Now

American Civil Liberties Union (ACLU)

ARTICLE 19

ARTICLE 19 México y Centroamérica

ASEAN Youth Forum

Asociación por los Derechos Civiles (ADC)

Asociația pentru Tehnologie și Internet (ApTI)

Association for Progressive Communications (APC)

Bits of Freedom

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Chaos Computer Club (CCC)

Citizen D / Državljan D

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Comun.al, Laboratorio de resiliencia digital

Data Privacy Brasil Research Association

Derechos Digitales - América Latina

Digitale Gesellschaft Schweiz (Switzerland)

Don't Delete Art (DDA)

Electronic Frontier Foundation (EFF)

Epicenter.works - for digital rights

European Center for Not-for-Profit Law (ECNL)

European Digital Rights (EDRi)

Fight for the Future (FFTF)

Förderverein Informationstechnik und Gesellschaft (Fitug e.V.)

Foundation for Media Alternatives (FMA)

Freemuse

Fundación Huaira

Fundación InternetBolivia.org

Fundación Karisma

Fundación Vía Libre

Global Forum for Media Development (GFMD)

Hiperderecho

Homo Digitalis

Instituto Nupef

Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC)

Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

Instituto de Referência em Internet e Sociedade (IRIS)

Intervozes - Coletivo Brasil de Comunicação Social

IT-Pol Denmark

Kandoo

Masaar - Technology and Law Community

National Coalition Against Censorship (NCAC)

Open Knowledge Foundation

OpenMedia

Open Rights Group

Red en Defensa de los Derechos Digitales (R3D)

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

SeguDigital

SMEX

Southeast Asia Freedom of Expression Network (SAFEnet)

TAPOL

Taraaz

The Sex Workers Project of the Urban Justice Center

ספקי תשתיות לא אמורים להיות משטרת התוכן (The Stack): מגינים על ארסנל הכלים הטכנולוגי

The Tor Project

The William Gomes Podcast

The Woodhull Freedom Foundation

Usuarios Digitales