

אוקטובר 2014

לכבוד

ייעוץ משפטי – ועדת החוקה, חוק ומשפט

הכנסת

הנדון: הצ"ח שימוש במקום לשם מניעת ביצוע עבירות (תיקון מס' 2), התשע"ד-2014

שלום וברכה,

לבקשתכם, אני מתכבד לחוות את דעתי בעניין הצעת החוק שבנדון. מטבע הדברים, התייחסותי עומדת בעיקר בהקשר לפרק ג', "הגבלת גישה לאתר אינטרנט לשם מניעת ביצוע עבירות". הדברים מובאים בצמצום ובתמצית. אשמח להרחיב על כל חלק בהם והמכלול, בפני הוועדה.

## תמצית מנהלים

- לצו הנובע מההסדר המוצע אין כל ערך אכיפתי. כל ניסיון של ספק שירותי גישה לאינטרנט ישראלי "לחסום תעבורה לאתר אינטרנט" שאינו מתארח אצלו, לא יצלח. ניתן לעקוף את ה"חסימה" באמצעים הנגישים לכל נפש, במאמץ אפסי וללא כל צורך במומחיות או ידע מקצועי כלשהו. העקיפה יכולה להתרחש כפועל יוצא של שירותים שרבים משתמשים בהם ממילא, ולעיתים אף תקרה העקיפה מניה וביה, ללא כוונתו או ידיעתו של המשתמש.
- מנגד, ניסיון להגבלת גישה באמצעות ספקי הגישה לאינטרנט עשוי ליצור נזק סביבתי משמעותי, שאין, ככלל, דרך להימנע ממנו. מדובר בעיקר בהפרעה לציבור הרחב והלא-מעורב מלגשת לאתרים רבים שאין בינם לבין העברייני לכאורה ולא כלום.
- ההסדר המוצע נותן בידי קצין משטרה סמכות כמו-שיפוטית לקבוע מהו תוכן או שירות באינטרנט הראוי לחסימה, למשך 60 יום. זוהי סמכות שאינה מידתית שגלישתה במדרון היא רק עניין של זמן. מתוך שאינו לשמה של צנזורה, בא לידי צנזורה.
- הצו המשטרתי הנובע מההסדר המוצע דורש למעשה מ"צינור" המידע – ספק שירותי הגישה של הציבור הרחב – להיות ידו הארוכה של השלטון באכיפת החוק, למרות שאין כל נגיעה לנשוא הצו עם ביצוע העבירה. הדבר דומה לדרישה מחברת "דרך ארץ" (כביש 6) להציב אנשים שיעצרו מכוניות שנחזות כאילו נוסעות למקום ביצוע עבירה, או מחברת "בזק" לחסום שיחות למספר טלפון שנדמה שמתבצעת בו עבירה, וכיוצא באלה.
- לאור כל אלה, אין היגיון בחקיקה כפי שמוצעת. אין בה כל תועלת, ונזקה רב. ההסדר המוצע עשוי להוביל לתחושה כוזבת של עשייה אכיפתית, בעת שהפעילות שאותה מנסים למנוע, שלעיתים היא אכן פשיעה מחליאה – תמשיך באין מפריע. הדרך הנכונה לטפל בבעיות של פשיעה המסתייעת בשימוש באינטרנט היא, כפי שהיא גם בפשיעה מסוגים אחרים, באמצעות חקירה מעמיקה, ובמקרה הצורך, פעולה המופנית לספק האינטרנט המספק שירות לאתר או למערכת המידע המעורב בעבירה. אם (כפי שלעיתים קרובות קורה) ספק זה נמצא מחוץ לישראל, יש להשתמש באמנות והסכמים בינלאומיים ובהבנות בילטראליות כדי להגיע אליו. כך נעשה בעולם החופשי; כך יש לעשות גם אצלנו.

## פשיעה באינטרנט

רשת האינטרנט הפכה להיות חלק בלתי נפרד מחיינו. בהיותה מדיום תקשורת נגיש (ומנגיש) לחלק עצום מהאוכלוסייה, ובהיות הטכנולוגיות המתפתחות על גבה עשירות כל כך ביכולות תקשורתיות ואחרות, היא נעשתה לאמצעי התקשורת המועדף על רבים (ועבור חלקים מהציבור, כמעט היחיד). ולפי שהיא הופכת להיות כזו למגוון רחב באוכלוסייה, גם חלק מעולם הפשיעה מסתייע בפעולותיו באינטרנט – כפי שהוא משתמש גם בטכנולוגיות רבות אחרות.

אין בכך כדי להפוך את האינטרנט ל"מקום מסוכן" ואת ה"פשיעה באינטרנט" לאלמנט כה ייחודי ומזרה אימה כפי שמנסים לעשותו לעיתים. כפי שפושעים פנו להשתמש בטלפון, או בסוסים וכרכרות, או ברכבות, או בחשמל כדי לבצע את זממם, כך הם משתמשים באינטרנט היום. וכפי שלא יעלה על דעתנו לעסוק בסכנות רשת הטלפונים או רשת החשמל, או באיומים הנובעים ממכירה חופשית של סכינים (המשמשים, כידוע, לרצח), אין מקום להליכת אימים כאן.

קושי ייחודי ומוכר באכיפת החוק, בעולם הכולל אינטרנט, נוצר מתוקף העובדה שהפעילות באינטרנט חורגת מגבולות שטח שיפוט מדינה וחקיקה מדינתית. כך למשל יכול אתר אינטרנט המבצע פעולות המנוגדות לחוק לשכון בטרטוריה אחרת, כזו ששיתוף הפעולה האכיפתי איתה מצומצם או שאינו קיים. קושי זה הוא להבנתי המניע מאחורי הדיון שהצ"ח זו היא חלק ממנו.

## ההסדר המוצע – התייחסות כללית

הצעת החוק שלפנינו מציעה הסדר משפטי חדש המאפשר לקצין משטרה להוציא צו מנהלי זמני שתוקפו עד 60 יום, ושיכול להיות מוארך ע"י בית משפט מוסמך, המופנה אל ספק גישה לאינטרנט ומורה לו לחסום את אפשרות גישתם של לקוחותיו אל אתר אינטרנט מסוים. זאת, כחלק ממאבק ב"פשיעה באינטרנט"<sup>1</sup>.

הסדר זה, למרות שהוא מנסה, על פני הדברים, להיות מאוזן ומידתי, לקוי מאד, בכמה רבדים:

- הגבלת גישה לאתרי אינטרנט באמצעות ספק גישה ישראלי, אינה אפקטיבית כלל ואינה יכולה להשיג את מטרתה. עקיפתה קלה, נטולת כל מאמץ או צורך בידע מקצועי, ולעיתים אף תתרחש "על הדרך" (כלומר, אף ללא שהתכוון האדם לבצע אותה, אלא מתוך שהוא משתמש בכלים נפוצים מאד לצרכים אחרים).
- מתן סמכות כמו-שיפוטית לקצין משטרה לקבוע מהו תוכן או שירות אינטרנטי הראוי לחסימה הוא בעייתי בלשון המעטה ומהווה תחילתו של מדרון חלקלק. גם אם לדעתנו של קצין המשטרה מתרחשת פעילות לא חוקית, בהתאם לסעיפי ה"תוספת", ב"אתר" נתון, המעבר הישיר מדעתו זו לצו לפעולת חסימה בוטה מחד, ונטולת שיניים מאידך, אצל ספקי התקשורת בישראל, טרום קיום הליך המאפשר לנפגעים המרכזיים מהפעולה להתמודד עם הטענה, הוא כבר מתוך עצמו הגבלה לא מידתית של חופש הביטוי והתקשורת, ופתח להכבדה מתגלגלת בהמשך. ידוע שאמצעי שנוצר לצורך אחד משמש לעיתים קרובות, ברבות הימים, לצרכים אחרים בתכלית. האפשרות להארכה "חצי אוטומטית" כעבור 60 יום מוסיפה אך מעט לתקפות אותה סמכות.

משכך, אין ההסדר המוצע מועיל כלל ועיקר למאבק בפשיעה המתרחשת באינטרנט. יתרה מזאת: השימוש בו עשוי להוביל לתחושה כוזבת של עשייה אכיפתית, בעת שהפעילות שאותה מנסים למנוע, שלעיתים היא אכן פשיעה מחליאה – תמשיך באין מפריע. אין ספק שהטלת צווים למיניהם קלה יותר מביצוע פעולות חקירה מתישות בשיתוף פעולה בינלאומי, פעולות אכיפה מחוץ לתחומי המדינה וכיוצא באלה. אך אין בפעולה זו תועלת אכיפתית כלל, ונזקה רב.

קשה לחמוק מהאסוציאציה המתבקשת: (א) "חייבים לעשות משהו" (ב) X הוא משהו (ג) "חייבים לעשות X".

<sup>1</sup> ההסדר מוצע בעקבות עתירה מנהלית (עת"מ 10-45606) של איגוד האינטרנט הישראלי נגד מפכ"ל משטרת ישראל בעניין צווים כאלה שהוצאו לספקי האינטרנט הגדולים בארץ, ופסיקת ביהמ"ש העליון בערעור בעניינה. למען הגילוי הנאות: הח"מ נטל חלק בהכנת העתירה המקורית.

## הגדרת אתר אינטרנט כהרחבה של "מקום"

אחד היסודות בפרק ג' בהצ"ח היא הגדרתו של "אתר אינטרנט". אנו מוצאים כאן הגדרה סיבובית למשעי: "אתר אינטרנט" – אתר אינטרנט שיש לציבור אפשרות גישה... וגו'. ולא בכדי. מקום הימצאות מידע, או מקום התרחשות חלופת מסרים בין אנשים באינטרנט, בצורתו היום אינו "אתר" כהגדרתו לפני עשר שנים ובוודאי איננו יודעים מה תהיה צורתו בעוד חמש שנים.

רק לשם הדוגמא, – האם דף "פייסבוק" הוא אתר? האם דף של סוחר בתוך זירת מכירות אינטרנטית בסין, הוא אתר?

ורק לשם דוגמא נוספת, אחד הנושאים החמים כיום ב"קצה" האינטרנט הוא Named Data Networking (NDN), טכנולוגיה ניסיונית, שאם תיעשה פופולרית תהפוך את כל המושג המוגדר כאן של "אתר אינטרנט" לכמעט חסר משמעות. האם אלמנט מידע של NDN הוא אתר?

רוצה לומר: למרות כוונתה של הצעת החוק להיות חפה מספציפיות טכנולוגית וצופה פני עתיד, ההסדר המוצע נטוע עמוק בתפיסה, שכבר היום מתחילה להיות מיושנת, של "אתר אינטרנט" במשמעותו כשרת עצמאי המתארח בחוות שרתים (או ב"ענן") בכתובת IP נתונה.

## חסימת גישה ל"מקום" אינטרנטי ע"י ספק גישה לאינטרנט

### התייחסות עקרונית

ההסדר המוצע קובע שהצו שיפנה קצין המשטרה המוסמך יופנה לספקי גישה לאינטרנט בישראל. ספקים אלה הם מי שמאפשר למשתמש הקצה (הביתי – תמיד, הארגוני – ברוב המקרים) קישוריות לאינטרנט.

"אתרי האינטרנט" שבהם מתרחשת לכאורה הפעילות המנוגדת לחוק יימצאו, בדרך כלל (אם כי לא תמיד), אצל ספק שירותי אירוח אתרים כלשהו.

ספקי הגישה לאינטרנט הם לעיתים קרובות גם ספקי שירותי אירוח אתרים, אך ניתן להניח כי בכל המקרים בהם יינתן צו, אין האתר ה"נחסם" מתארח אצל ספק הגישה הישראלי.

במילים אחרות, ספק שירותי הגישה הוא בבחינת צינור, המשמש את הציבור הרחב לגישה לאינטרנט. הוא מממש את יכולתו, וזכותו, של הציבור לגשת למידע ולשירותים ברשת.

הצו המדובר בהסדר משתמש בצינור זה כזרועו הארוכה של השלטון, לצורך אכיפת חוק שידו קצרה מלאכוף באופן עצמאי ויעיל.

דומה הדבר לכך שיוציא הקצין צו אל חברת "בזק" כדי לחסום שיחות אל מספר טלפון שנדמה שמתרחשת בו עבירה, או אל חברת החשמל כדי שתחסום שימוש בחשמל למכשירים המשמשים בעבירה, או אל חברת "דרך ארץ" כדי שתציב בכביש 6 אנשים שיעצרו מכוניות נוסעות שנחזה כאילו הן נוסעות למקום שצפוי להתבצע בו פשע.

דוגמאות אלו עשויות להיראות אבסורדיות – אך מעת שאותו אקט בדיוק מופנה לספק הגישה לרשת האינטרנט, משום מה הוא נחזה כסביר יותר.

זאת, ועוד: למעשה, בצורת הפעלתו המוצעת, הצו אינו מושת על מבצע הפשע, כלל. הוא מושת על כלל הציבור. מבצע הפשע עשוי לא להיות ער כלל לעובדה שהופעל צו שכזה. ולמרות שההסדר המוצע מכיל אמצעים לאתר האינטרנט ה"נחסם" להשיג השגותיו, הרי שהנשוא העיקרי של הצו – הציבור – מושתק.

## הדרכים הזמינות להגבלת גישה ושימותן

הגבלת הגישה אליה מתייחסת הצעת החוק, כזו שמתבצעת באמצעות ספקי הגישה לאינטרנט, לחלוטין אינה יעילה ולמעשה, מגבילה באופן מזערי את הגישה אותה מתיימרים למנוע.

כל משתמש הרוצה בכך, יכול, במאמץ מזערי וללא כל צורך בידע מקצועי מיוחד, לעקוף את אותה "הגבלה" ובכך לגשת באופן חופשי ובאין מפריע לתכנים שקצין המשטרה החליט שיש למנוע גישה אליהם.

ברמה העקרונית, וללא כניסה לדיון טכני מדי, קיימות מספר דרכים ליישום "הגבלת גישה לאתר" כאשר זו נעשית ברמת ספק הגישה לאינטרנט<sup>2</sup>:

### הגבלה באמצעות שם האתר

בשיטה זו, מתערב ספק הגישה בשירות תרגום השמות לכתובות באינטרנט (DNS) המתבצע דרכו, ומשנה את תוצאות פענוח שמו של אתר האינטרנט נשוא החסימה לכתובת IP שאינה המקורית.

שיטה זו נעקפת באופן טריביאלי. טכניקת העקיפה תלויה באופן המדויק בו יושמה ההגבלה אצל ספק הגישה. לדוגמה, כאשר היא מיושמת באמצעות שירות פענוח השמות של הספק (DNS Resolver), אזי שינוי הגדרה אחת במחשב – הפניה לשימוש בשרת פענוח שמות ציבורי (Public DNS Resolver), שרבים כמותו זמינים לכל דורש באינטרנט ללא עלות, הפופולארי שבהם של חברת Google), במקום ההפניה הסטנדרטית אל שרת השמות של ספק האינטרנט, – יעקוף את החסימה. זוהי כאמור הגדרה אחת, פשוטה מאד, במחשב (או בטלפון, טאבלט וכו'), וניתן אפילו לעשותה פעם אחת בנתב (ראוטר) ביתי כך שתשפיע אוטומטית על כל באי הבית, מחשביו וטלפוניו. אופני ישום אחרים נעקפים בקלות דומה.

### הגבלה באמצעות כתובות IP

בשיטה זו, מספק דורש החסימה למקבל הצו כתובת IP שבה, למיטב ידיעתו, נמצא שרת המידע הפוגעני. ספק שירות הגישה מצווה לחסום כל תעבורה לכתובת IP זו.

הגבלה זו יכולה להיעקף בפשטות, לדוגמה, ע"י שימוש ב-Proxy, אמצעי המעביר את הגישה לאינטרנט של משתמש מסוים דרך שרת המהווה כעין שלוח שלו. הגישה לאתרים מתבצעת דרך כתובת IP של שרת ה-Proxy שעשוי להימצא מחוץ לישראל. כל הנדרש הוא לשנות הגדרה פשוטה בדפדפן. גם כאן לא נדרשת שום מיומנות מקצועית או מיוחדת, אלא הקלדת הגדרה אחת בתפריט אחד.

### הגבלה באמצעות האזנה אקטיבית לתוכן (Deep Packet Inspection)

בשיטה זו, נדרש ספק הגישה להאזין לתוכנה של תעבורת המידע היוצאת ממחשבי לקוחותיו. כאשר הוא רואה ניסיון גישה לאתר שאליו נדרשה הגבלת גישה, עליו לחסום אותו.

שיטה זו היא פולשנית במיוחד היות שהיא דורשת בדיקה של תוכן כל התעבורה, של כל משתמש ומשתמש. ועם זאת, יכולות החסימה שהיא מספקת, לצורך ההסדר המוצע, כמעט ואינן עולות על אלו של השיטות הקודמות.

שימוש בשירות מסוג VPN, שירות לגיטימי הזמין לכל דורש, אם בתשלום חודשי מזערי ואם בחינם, מהווה, לאו דווקא במתכוון, עקיפה מלאה של כל סוגי ההגבלה שפורטו לעיל. שירותים ממין זה משמשים כיום תושבי ישראל רבים, למשל כדי ליהנות משירותי הזרמת וידאו ואודיו מארה"ב. כאשר מופעל שירות זה, המשתמש "גולש" באינטרנט דרך כתובת IP המסופקת לו ע"י שירות ה-VPN, ושאינה בישראל. כל שספק הגישה המקומי רואה הוא

<sup>2</sup> לא נדרשת בסקירה זו לאמצעים קיצוניים ופולשניים באורח אבסורדי, כגון חדירה למחשבי כלל התושבים כדי לעקוב ולחסום גישה לתכנים אסורים, שאף אם הם אפשריים טכנית, אני יוצא מהנחה שאין לאף אדם בישראל כוונה להציעם.

תעבורה מוצפנת שתעודתה שרת לגיטימי לחלוטין בחו"ל; הוא עיוור לחלוטין לאינטראקציה עם השרת נשוא דרישת ההגבלה, וכמובן שאין בידו דרך טכנית לחסום אותה.

אמצעי פופולארי נוסף לעקיפות כאלה, שנמצא בשימוש מגזרים שונים באוכלוסיה, הוא מערכות להסתרת מקור, כדוגמת TOR. זוהי רשת עולמית של שרתים שתפקידם לטשטש את מקורו של שימוש ("גלישה") באינטרנט. מערכת זו פותחה במקור כדי להגן על יכולתם של משתמשי אינטרנט בארצות החיות תחת משטרים טוטליטאריים, כגון סין או צפון קוריאה, לגשת למידע ואף לשלוח מידע ללא שהשלטון יוכל לאתרם. לימים, החלו להשתמש במערך זה גם שוחרי רע ופושעים למיניהם, המנהלים באמצעותו תקשורת וסחר ביניהם, וגם, ולהבדיל אלפי הבדלות, שוחרי פרטיות וחופש מידע, המעוניינים להגן על פרטיותם מפני מעקב. השימוש ב-TOR הוא פשוט למדי ונגיש לכל אדם.

אין בידי ספקי הגישה כל דרך אפקטיבית להגביל גישה לאתר אינטרנט ממי שמעוניין בה. לעיתים, תיעקף ה"חסימה" אף ללא שהמשתמש מתכוון לכך או מודע שעקף משהו.

## תחום החלת הצווים

אם ניקח כדוגמא את הצווים שהוצאו במקרה שגרר את העתירה המנהלית ואת הצעת החוק, הרי שנראה שהם הוצאו כנגד שלושת ספקי האינטרנט הגדולים.

משכך, מי שהגבלה נשואת הצווים השפיעה עליו (אם בכלל) הם לקוחותיהם של שלושה ספקים אלה, ולא של כל יתר ספקי שירות הגישה. מצד אחד, שלושה ספקי גישה אלה משרתים את חלק הארי של הציבור בישראל. מצד שני, גם אם היינו מניחים לצורך הדיון אפקטיביות מסוימת בחסימה, הרי מי שמעוניין לא להיות נתון לה, כל שעליו לעשות הוא לעבור לאחד מספקי הגישה האחרים (יש רבים כאלה), פעולה הכרוכה בשיחת טלפון אחת.

זאת ועוד. חלק מהרשתות הארגוניות בישראל, כמו גם רשתות המוסדות האקדמיים, מקושרות לאינטרנט באמצעות קוים משלהם, ואינן משתמשות בשירותי הגישה של ספקי הגישה הישראליים. שוב, מי שמעוניין לא להיות נתון לניסיון החסימה, יכול לעשות את מה שמלאו ליבו לעשות מתוך רשת ארגונית כזו או מתוך רשת אחד המוסדות האקדמיים.

## נזק סביבתי

הגבלת הגישה באמצעות ספקי הגישה לאינטרנט נושאת בחובה נזק סביבתי משמעותי, כזה שמושת על ציבור תמים, שאין כל קשר בינו לבין העבירה שבגינה הופעל הצו.

הגבלה באמצעות כתובות IP, שאמורה להיות מכוונת אל אתר מידע מסוים שנמצא בכתובת זו, תחסום את הגישה לכל האתרים האחרים שנמצאים בכתובת IP זו. במציאות האינטרנטית דהיום, ספקי אירוח אתרים מארחים לעיתים קרובות מאות אתרי אינטרנט בכתובת IP אחת. חסימת הגישה לכתובת IP אחת כזו תפריע לציבור מלגשת לכל אותם אתרים תמימים שאין כל קשר בינם לבין נשוא הצו למעט שהתמזל מזלם להיות כולם לקוחות של אותו ספק אירוח.

יתרה מזו: לקצין המשטרה המוסמך יהיה קשה מאד לדעת על כך. סעיף 4ב' ס"ק ד' להצ"ח אומר ש"קצין המשטרה המוסמך סבר שניתן באמצעות ספק שירות איתור (!) אינטרנטי להגביל את הגישה באופן ממוקד" (ההדגשה שלי, אני מניח שזו שגיאה במקור) – דא עקא, שברוב המקרים אין לו כל דרך אמינה כזו, ולכן אמירה זו ריקה מתוכן.

ועוד: לגבי חלק גדול מהעבירות שנמצאות כרגע במרכז שדה הראיה של מגישי הצעת החוק, כגון פדופיליה, מאבק בארגוני פשיעה, סחר בסמים, זכויות יוצרים (!) – הסבירות היא דווקא גבוהה מאד שאתרי אינטרנט שבהם מתרחשת פעילות כזו יימצאו מתארחים אצל ספק אירוח לגיטימי, לצידם של מאות רבות של אתרי אינטרנט לגיטימיים ובלתי מעורבים, כחלק משמירה על "פרופיל נמוך" והתערבות בקהל.

הגבלה באמצעות האזנה (DPI), נזקיה הסביבתיים גדולים, מעצם טבעה. היא דורשת הפעלת מסננים על תוכנו (ולא רק על תעודתו) של כלל המידע המועבר באינטרנט ע"י כלל המשתמשים. מסננים אלה פוגעים קשות בפרטיותו של כלל הציבור, אשר מתייחס לספקי הגישה לאינטרנט כאל נאמן שלו. סינון כזה חשוף גם לכמות משמעותית של התראות שווא, שיצמצמו מאד את יעילותו ויגדילו את נזקו הסביבתי. ומעבר לכך, בנוסף, עלותו של סינון כזה, עלות שתושט כמובן על ציבור המשתמשים, גבוהה, והוא עשוי אף להאט את מהירות הגישה לאינטרנט.

בסה"כ, סינון באמצעות DPI מקומו לא יכירנו במדינה חופשית והוא מוזכר כאן רק לצורך השלמות.

אפילו הגבלה באמצעות התערבות בשירות פענוח השמות, שהיא לכאורה ממוקדת (אם גם כמעט חסרת משמעות אכיפתית), עשויה לגרום לנזק סביבתי מכיוון שמדובר בהתערבות ידנית בשירות פענוח השמות האינטרנטי. טעות אנוש או אי דיוק בהגדרות יכולים ליצור חסימה גדולה מהנדרש או תקלות בגישה לשירותים אחרים, בעיות שיהיו קשות לאיתור.

ניסיון להגבלת גישה באמצעות ספקי הגישה האינטרנט עלול ליצור נזק סביבתי משמעותי, לציבור הרחב, שככלל, אין דרך יעילה להימנע ממנו.

## המלצות

הדרך הראויה לטפל בבעיות של פשיעה המסתייעת בשימוש באינטרנט היא, כפי שהיא גם בפשיעה מכל סוג אחר, באמצעות חקירה מעמיקה, ובמקרה הצורך, ע"י פעולה המופנית לספק האינטרנט המספק שירות לאתר או למקור המידע המעורב בעבירה. אם (כפי שלעיתים קרובות קורה) ספק זה נמצא מחוץ לישראל, יש להשתמש באמנות והסכמים בינלאומיים ובהבנות בילטרליות כדי להגיע אליו. כך נעשה בעולם החופשי; כך יש לעשות גם אצלנו.

לעיתים אפילו פנייה רשמית מגורם אכיפה ישראלי או שיחת טלפון לספק האינטרנט הרלבנטי (זה המספק קישוריות לשרת הנושא את התוכן הבעייתי), גם אם הוא נמצא מחוץ לישראל, עשויות לגרום לו להוריד את המידע הפוגעני. במקרים רבים, הוא לא יהיה מעוניין להסתבך בעיסוקים שכאלה.

מומלץ שהמדינה, כולל רשויות האכיפה השונות, וגופים נוספים, יבנו ויטפחו קשרים מתמשכים עם גופי אכיפה ומודיעין לאומיים ובין לאומיים, בדומה לאלה שקיימים בתחומים שאינם אינטרנטיים, קשרים שיסייעו בטיפול בעבירות המתבצעות באמצעות מחשבים.

## סיכום

1. ההסדר המוצע מאפשר לקצין משטרה, ללא בקרה שיפוטית, לקבוע כי גישה לתוכן אינטרנטי מסוים אסורה, למשך 60 יום. זוהי סמכות שאינה מידתית שגלישתה במדרון היא רק עניין של זמן. מתוך שאינו לשמה של צנזורה, בא לידי צנזורה.
2. דא עקא שאין כל אפשרות לספק האינטרנט לחסום גישה לאתר אינטרנט נתון. הספקים יפעילו מסננים כדי לצאת חובת הצו, כל מי שמעוניין לגשת למידע ה"חסום" יוכל לגשת אליו בקלות וללא מאמץ או צורך בידע מקצועי, ולגוף האכיפה תהיה התחושה הכוזבת כי ביצע פעולת אכיפה, והעבירה כבר לא מתרחשת (לפחות לא בישראל).
3. מנגד לחוסר התוחלת באמצעים אלה, יש סכנה לנזק סביבתי רחב. לדוגמה, הגבלת גישה למאות או אלפי אתרים שכל "חטאם" הוא שימוש באותה כתובת IP שבה משתמש העברייני. מי שיינזק באמת מניסיונות האכיפה, הוא הציבור הרחב בישראל.
4. הצו המשטרתי דורש למעשה מ"צינור" המידע – ספק שירותי הגישה של הציבור הרחב – להיות ידו הארוכה של השלטון באכיפת החוק, למרות שאין כל נגיעה לנשוא הצו עם ביצוע העבירה.
5. הטיפול הנכון בעבירות שמתבצעות באמצעות שירותי מידע הנמצאים מחוץ לישראל הוא באמצעות חקירה מעמיקה ושימוש בהסכמים בינלאומיים, אמנות והבנות בילטרליות עם גופים מקבילים בעולם כדי לבצע אכיפה יעילה נגד הגורם העברייני עצמו.