# עיקרי טיעון – חדירה לענן בתיק טלגראס

**תוכן העניינים**


**כללי ..... 2**

**חדירה לענן איננה פעולה אקסטרה-טריטוריאלית ..... 7**

**חדירה לענן לא פוגעת בזכויות מוגנות של חשודים ונאשמים ..... 11**

**משפט משווה: הפרקטיקה של חדירה למחשבים מרוחקים המצויים בחו"ל מוכרת במדינות זרות ובמשפט הבין-לאומי ..... 14**

מדינות שהכירו בחדירה למחשבים מרוחקים המצויים בחו"ל ללא חקיקה ייעודית..... 14

ארצות-הברית ..... 14

הולנד ..... 16

נורבגיה..... 17

דנמרק ..... 18

שוויץ..... 18

מדינות שהכירו בחדירה למחשבים מרוחקים המצויים בחו"ל כפעולה מותרת על פי חקיקה ייעודית ..... 19

אוסטרליה ..... 19

ניו-זילנד ..... 20~~19~~

בלגיה ..... 20

מקורות נוספים במשפט הבין-לאומי..... 20

**הצדקות במישור הנורמטיבי להכרה בסמכותו של בית-משפט ישראלי להתיר חדירה לענן.... 21**

הצדקה במישור התפישתי - פעמים רבות למיקומו של חומר המחשב אין משמעות ..... 22~~21~~

הצדקה במישור הטכנולוגי - מיקומו ה"פיזי" של חומר המחשב לא תמיד ידוע ..... 23

הצדקה במישור המעשי - בקשה לעזרה משפטית אינה מספקת את צרכי החקירה (ובוודאי כך בענייננו) ..... 24~~23~~

**<u>כללי</u>**

1. במהלך דיוני ההוכחות בתיק נשמעה מטעם ההגנה הטענה לפיה בית-משפט השלום בראשון-לציון חרג מסמכותו (וכתוצאה מכך – חרגה משטרת-ישראל מסמכותה), כאשר ניתנו צווי חדירה לחומר מחשב המאפשרים למשטרת-ישראל במפורש לחדור לחומר מחשב המקושר למחשבים התפוסים כדין בישראל אך אגור בשרתים מרוחקים, לרבות שרתים שנמצאים מחוץ לתחומי ישראל (להלן: "**חדירה לענן**"). במסמך זה המאשימה תטען מדוע טענה זו שגויה, ומדוע בסמכותו של בית-משפט ישראלי להעניק לרשויות החקירה בישראל צווי חדירה לחומר מחשב המאפשרים חדירה לענן. כפועל יוצא מכך, המאשימה תטען כי משטרת-ישראל לא חרגה מסמכותה כאשר ביצעה חדירה לענן על-בסיסו של הצו השיפוטי שניתן לה.

2. כידוע, עניינה של הפרשה הנוכחית בעבירות שבוצעו ברובן במרחב המקוון, תוך שימוש של הנאשמים בפלטפורמת טלגרם ובשרתיה, ותוך ניצול מאפייניה הייחודיים של הפלטפורמה (אנונימיות, אופציות מחיקה של התכנים, פיתוח בוטים ועוד). על פי המיוחס לנאשמים, ניהול הקשר בין הנאשמים, כמו גם פעולות התיווך לסמים המסוכנים ותיאום עסקאות הסמים, בוצעו כולם על גבי פלטפורמת טלגרם תוך שהמידע נאגר בשרתיה.

3. עם התקדמות החקירה הסמויה בפרשה, התברר שראיות מרכזיות להוכחת פעילותו האסורה של ארגון טלגראס מצויות בחשבונות הטלגרם האישיים של החשודים (לימים הנאשמים בתיק זה ובתיק המקביל) ובקבוצות הטלגרם ששימשו אותם. ניתן היה אף להניח, על סמך המידע שנאסף בחקירה, כי המידע בחשבונות ובקבוצות אלה אגור בשרתים של חברת טלגרם (מחוץ לטריטוריה הישראלית), וכי קיים סיכון ממשי וקונקרטי למחיקת המידע האמור מרחוק. על כן, סברו חוקרי המשטרה – בצדק רב – כי הכרחי להשיג את המידע שנאגר בחשבונות ובקבוצות הטלגרם, וכי נדרש לעשות כן בהקדם האפשרי. נוסף על כך, התעורר חשד שמידע רב נוסף בעל ערך חקירתי משמעתי, עשוי להימצא בשרתים מרוחקים, ובין היתר: מידע בנוגע להעברות כספים בארנקים וירטואליים ובשירותי העברת כספים בדרך מקוונת, ומידע בנוגע לאופן ניהול כספי ארגון טלגראס ובסיסי הנתונים המשמשים את הארגון.

4. לפיכך, פנו חוקרי המשטרה ביום 28.2.2020 בבקשה ליועץ המשפטי לממשלה לאשר פנייה לבית-המשפט בבקשה למתן צו המתיר חדירה לשרתים מרוחקים, לחומרי המחשב האגורים בהם והמקושרים ל"מכשירי קצה" (טלפון נייד או מחשב), שייתפסו במסגרת החיפוש שייערך עם המעבר מחקירה סמויה לחקירה גלויה (חדירה לענן):

   א. ביום 5.3.2019 ניתן אישור על דעת היועץ המשפטי לממשלה ופרקליט המדינה לפנות לבית-המשפט בבקשה להתיר חדירה לחומרי מחשב שייתפסו במהלך החקירה, ובכלל זה גם חדירה לענן. מצ"ב האישור כ**נספח א'**.

   ב. היחידה החוקרת פנתה ביום 6.3.2019 לבית-משפט השלום בראשון-לציון בבקשות לקבלת צווי חדירה לחומר מחשב, לפי סעיף 23א לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 (להלן: "**פסד"פ**"). בבקשה לצו חדירה הוסיפה הרשות החוקרת את

הטקסט הבא, אשר נוגע להסמכתן לביצוע חדירה לענן (הטקסט הופיע בתיאור החפץ התפוס או בתיאור המקום): "...לרבות חדירה נמשכת לחומר מחשב אשר למחשב התפוס יש הרשאת גישה אליו בכל מקום בו מצוי אותו חומר מחשב". למען הסר ספק יובהר כי בדיון בבקשה לצו חדירה לחומר מחשב הוצג בפני בית-משפט השלום בראשון-לציון ההיתר שניתן על דעת היועץ המשפטי לממשלה ופרקליט המדינה לפנות בבקשה לקבלת צו חדירה לענן.

ג. לאחר מתן צו החדירה על-ידי בית-משפט השלום בראשון-לציון, ביום 12.3.2019, יום ה"פרוץ", תפסו חוקרי המשטרה כדין "מכשירי קצה" (בעיקר טלפונים ניידים ומחשבים) אשר יש להם חיבור לאינטרנט מרשותם של החשודים שנגדם הוצא הצו.

5. בפועל, במהלך חקירת הפרשה, חוקרי המחשב המיומנים ביצעו חדירה לענן באמצעות מכשיר קצה שנתפס כדין בחיפוש, והעתיקו בדרך זו תכנים הרלוונטיים לחקירה, וזאת בארבעה מקרים עיקריים: בעניינו של נאשם 5 רן בוגנים (להלן: "**בוגנים**"); בעניינו של נאשם 6 שמעון תוהמי (להלן: "**תוהמי**"), בעניינו של נאשם 12 בתיק המקביל – מתכנת ראשי בטלגראס בשם מאיר ניסן (להלן: "**ניסן**") ובעניינו של הנאשם ארז שמואלי המתנהל בבית המשפט המחוזי בתל-אביב בת.פ.ח 24518-06-19 (להלן: "**שמואלי**").

6. בעניין ניסן ובוגנים בוצעה החדירה לענן בנוכחות המחזיק במחשב או לאחר שהמחזיק במחשב חתם על טופס הצהרת מחזיק במחשב, בו הוא ויתר על נוכחותו בעת החיפוש (להלן: "**טופס ויתור נוכחות**"). זאת בהתאם לקבוע בסעיף ג' לאישור שניתן על דעת היועץ המשפטי לממשלה ופרקליט המדינה (נספח א'). יצוין כי הן ניסן והן בוגנים מסרו לחוקרים את סיסמאות הכניסה למחשביהם, ובוגנים אף הדריך את החוקרים היכן לבצע את החיפוש (ראה טפסי הצהרת חתומים ברקוד 156, 161, 2937 ודו"חות ברקוד 157, 162, 163, 2942, 3003, 3040 ו- 3043).

7. בעניינו של תוהמי התרחש אירוע חריג כמפורט להלן:

א. ביום 12.3.2019 הגיעו שוטרי משטרת-ישראל לביתו של תוהמי על מנת לערוך שם חיפוש. לאחר שהשוטרים דפקו על דלת הבית, הנאשם תוהמי לא פתח את הדלת (הגם ששהה בבית), ולבסוף הם נאלצו לפרוץ את הדלת בסיועו של "כוח פריצה" (ראו דו"חות פעולה ברקוד 2429, 2430). לאחר שנכנסו לביתו של תוהמי, הבחינו השוטרים כי מחשבו הנייד מונח בסלון כשהוא דלוק, ועשרות קבוצות טלגראס פעילות בו (ראו דו"ח מאת בוריס סיקלייר ברקוד 2432). למקום הוזעק החוקר המיומן אופיר בן שלום, אשר בדק את המחשב בדירה. בהמשך, התנפל תוהמי על השוטר סיקלייר אשר הודרך לשמור על מחשבו הנייד (ר' דו"ח פעולה בר קוד 2430, 2432). לאחר מכן נשכב תוהמי על המחשב, וניסה לשבור אותו בידיו האזוקות כשהוא הולם במסך וזאת בכוונה להשמיד ראיות (ר' דו"חות פעולה ברקוד 2424, 2430, 2431, 2442). תוהמי לא חדל להשתולל, ורק לאחר שכוח בילוש השתלט עליו, הצליחו לחלץ מידו את המחשב, לא לפני שעלה בידו לשבור את מסך המחשב (ר' תצלום המסך השבור בדו"ח פעולה ברקוד 2432).

ב. לנוכח הנסיבות שתוארו לעיל, הוחלט לתפוס את המחשב הנייד של תוהמי ולהעבירו למעבדה הפורנזית בלהב 433 לניתוח ומיצוי מידיים (ר' דו"ח אופיר בן שלום ברקוד 2425).

**Commented [HV1]:** הערה כללית לגבי כל החלק העובדתי: להבנתי אם מסמך מסויים לא הוגש כמוצג, לא ניתן יהיה להסתמך עליו במסגרת המצע העובדתי. המשמעות היא שכל מה שמופיע כרגע עם המלים "ברקוד 2432" או כדומה צריך להפוך ל-"ת/4", "ת/54" וכדומה. ואם משהו לא הוגש כמוצג, לא ניתן יהיה להסתמך עליו כאן.
לכן, צוות טלגראס צריך לעבור ולהמיר את הכל בהתאם.

**Commented [SR2]:** הכל יוגש במהלך הזוטא, ואמיר לבון אף יציין הכל במזכר שלו שיוגש גם כן

על מחשב זה נמצא חיבור פעיל לחשבון המשתמש (user) המרכזי של טלגראס, קרי, חשבון משתמש ששולט בכלל הקבוצות והערוצים שפעלו במסגרת ארגון טלגראס (להלן: **"יוזר טלגראס"**). המידע המקושר לחשבון משתמש זה, אשר נמצא בשרתים המרוחקים של טלגרם, הועתק בחלקו ונשמר על-ידי היחידה החוקרת.

ג. במהלך ביצוע פעולות החדירה הנ"ל, התברר לחוקרים כי משתמש שכינויו "אנג'וקס", המוכר לצוות החקירה כמנהל בטלגראס אולם זהותו האמיתית לא הייתה ידועה ליחידה החוקרת (ואף אינה ידועה עד היום), החל להסיר חשבונות מקבוצות הטלגראס. החוקרים חששו מהשתלטות של "אנג'וקס" על חשבון המשתמש המרכזי של טלגראס והמשך שיבוש החקירה על-ידו. לנוכח האמור הוחלט להסיר את כלל החיבורים הפעילים (הסשנים) המקושרים לחשבון מרכזי זה, ולהשאיר אך ורק את זה המופעל ממחשבו של תוהמי (ר' דו"ח פעולה מאת אופיר בן שלום, ק-49ב, 20). ביום 15.3.2019 התחבר השוטר דוד מגלשווילי למחשבו של תוהמי, ונכנס ליוזר טלגראס במחשב במטרה להפסיק את ביצוע העבירות על-ידי "טלגראס" ולמנוע את אפשרות שיבוש החקירה, והסיר ממנו הרשאות של יוזרים שונים שהוגדרו "אדמין", קרי ניתק חשבונות אחרים שהיו בעלי שליטה בחשבון זה (ברקוד 2440).

ד. יצוין כי ביום 17.3.2019, כחמישה ימים לאחר מעצרו, תוהמי אישר לחוקרים את ביצוע החיפוש בחומרי המחשב שלו, שלא בנוכחותו. ראו טופס ויתור נוכחות שעליו חתם תוהמי (ברקוד 2423).

ה. עוד יצוין כי ביום 20.3.2019 בוצעה השתלטות מרחוק של גורם לא ידוע על חשבון ה-iCloud של תוהמי, ושונתה סיסמת הכניסה אליו, וזאת באמצעות חשבון הטלגרם של חברתו של תוהמי, יעל כהן (ברקוד 2448). יצוין כי יעל כהן נחקרה במשטרה והכחישה כל קשר להשתלטות זו. לאחר מאמצים, עלה בידי היחידה החוקרת לשחזר את הנגישות אל חשבון ה-iCloud של תוהמי.

ו. נוסף על האמור, -------

**Commented [HV3]:** להשלים עובדתית כל מה שנדרש לגבי פעולות החדירה לענן שבוצעו בפועל, ככל שבוצעו

8. אשר לארז שמואלי, לאחר שהאחרון ביקש בחקירותיו להציג בפניו את כל התכתבויות הטלגרם ממכשיר הטלפון הנייד שלו, בוצעה חדירה לענן (חשבונות טלגרם ודוא"ל) בנוכחותו, לאחר שמסר את הסיסמא. כמו כן יצוין כי שמואלי חתם על טופס ויתור נוכחות (ברקוד 464) כמו גם על טופס הסכמה מדעת לביצוע חדירה לחשבון דוא"ל שלו בשירות Gmail (ברקוד 474).

9. פעולות החדירה לשלושת המחשבים הראשונים שנמנו לעיל, אשר כללו גישה לשרתים מרוחקים כאמור, הניבו בעיקרן התכתבויות טלגרם בין הנאשמים שמרשותם נתפסו המחשבים לבין מעורבים אחרים בפרשה, כמו גם התכתבויות בקבוצות שהנאשמים היו חברים בהן. פעולות אלה אף אפשרו את הורדת פעילות הבוטים ששימשו לניהול הפעילות הפלילית במסגרת ארגון טלגראס והסרת ההרשאות ניהול של משתמשים אחרים (ק-49ב, מסמך 15), ומנעו השתלטות מרחוק ומחיקתו של יוזר טלגראס אשר לתוהמי הייתה גישה פעילה אליו ממחשבו.

**Commented [HV4]:** שוב, לאורך כל החלק העובדתי, יש לוודא שמשתמשים באופן אחיד בסימון של המוצגים: כרגע אני רואה פעם סימוני "ברקוד", ופעם כנראה סימון ברשימת החומר שנאסף. יש לאחד וללכת על אותו סוג של רישום של החומרים שעליהם נסמכים

10. נוסף על עניינם של ארבעת הנאשמים שמנינו לעיל, במהלך החקירה ביצעה המשטרה פעולות לניתוק חיבורים (סשנים) פעילים בחשבונות הטלגרם של כמה מהנאשמים בתיק ובתיק

המקביל, וזאת לאחר תפיסת מכשירי הטלפון והמחשבים ששימשו את אותם נאשמים. מטרתה של פעולה זו הייתה למנוע אפשרות למחיקה מרחוק של התוכן הרלוונטי משרתי טלגרם וממכשירי הקצה.

11. יודגש כי פעולת החדירה לענן, כפי שהותרה בבית-המשפט וכפי שקודם לכן – אושרה על דעת היועץ המשפטי לממשלה ופרקליט המדינה - כללה את הדגשים הבאים, והתבצעה באופן הבא:
   א. מתוך מכשיר קצה שנתפס כדין בידי משטרת-ישראל. הפעולה לא התבצעה במישרין מתוך מחשב משטרתי.
   ב. הגישה נעשתה לחומרי מחשב מרוחקים המקושרים אל מכשירי הקצה שנתפסו כדין בחקירה.
   ג. החוקר ניגש רק למידע אשר למכשיר הקצה (וכפועל יוצא – למחזיק מכשיר הקצה) הייתה גישה מורשית אליו. כלומר, הגם שבפועל מחשבו של הנאשם תיקשר עם השרת המרוחק, הרי שהגישה הייתה אך ורק לחומרי מחשב המשויכים לחשבון של הנחפש באותו שרת מרוחק, המקושר למכשיר הקצה התפוס, ושייכים לנאשם. לא התבצעה גישה לחומרי מחשב אחרים בשרת המרוחק, אשר למשתמש בישראל לא הייתה גישה אליהם מתוך מכשיר הקצה התפוס כדין בישראל.

12. מהלך הטיעון יהיה כדלקמן: **ראשית**, נטען כי הפעולה של חדירה לענן איננה למעשה פעולה אקסטרה-טריטוריאלית, בוודאי לא פעולה אקסטרה-טריטוריאלית מובהקת, וזאת בניגוד לטיעוני ההגנה בעניין זה. בתוך כך נבקש להציג את המגבלות אשר הוטלו על רשויות החקירה בישראל, בהנחיות פנימיות, בבואן לבצע חדירה לענן – מגבלות אשר נועדו בעיקרן להגן על החוקרים הישראלים מפני טענות של מדינות זרות בנוגע לפגיעה בריבונותן. **שנית**, נבהיר מדוע לגישתנו טיעוני ההגנה בנוגע לפגיעה בזכויות חשודים ונאשמים הם שגויים. זאת, משום שייחודיותה של הפרקטיקה של חדירה לענן נעוצה ביחסים הבין-לאומיים שבין מדינת ישראל למדינות אחרות, ונוגעת לשאלות של ריבונות, ולא לשאלות של פגיעה אפשרית בזכויות חשודים ונאשמים. **שלישית**, נציג את הפרקטיקה של חדירה לענן כפי שמבוצעת במדינות זרות, אף בהעדר דין מפורש המסמיך את רשויות החקירה באותן המדינות לבצע חדירה לענן כאמור. משמע, שהפעולה הנדונה כאן אינה פעולה ייחודית למדינת ישראל. **רביעית**, נסקור מדוע ראוי, מבחינה נורמטיבית, לאפשר לרשויות החקירה לבצע חדירה לענן.

**Commented [YW5]:** לא בטוח שזו הגדרה מדויקת של המטרה.

**Commented [YW6]:** כנ"ל. כמו כן בהמשך מתייחסים גם להיבטי הפגיעה כלומר אלה היבטים רלוונטיים בכל מקרה.

13. עוד בטרם נתקדם אל הטיעון לגופו, נבקש להתייחס להוראות בדין הישראלי ביחס לסוגייה שלפנינו. הדין הישראלי שותק לגבי שאלת מעמדה העקרוני של פעולת חקירה אקסטרה-טריטוריאלית. בעוד שהדין הפלילי מתייחס בפירוט לסוגיית סמכות השיפוט האקסטרה-טריטוריאלית,[1] הרי שבכל הנוגע לסמכות לבצע פעולות חקירה בעלות מובנים העשויים להיחשב כאקסטרה-טריטוריאליים – הדין הפלילי שותק. שאלה אחרונה זו מתעוררת בעת ביצוען של פעולות חקירה במרחב המקוון, וזאת בשל העובדה שהמרחב המקוון הוא טרנס-מדינתי, ופעולות בסיסיות המתבצעות במרחב, כגון שליחת הודעת דוא"ל, גיבוי ב"ענן", פרסום תוכן ברשת חברתית וקיום שיחה בתווך האינטרנטי – עשויות להתבצע מישראל, אך כחלק

[1] כקבוע בפרק ג' (סעיפים 7-17) לחוק העונשין, התשל"ז-1977 (להלן: "**חוק העונשין**").

אינהרנטי מתהליך ביצוען, עובר המידע או נאגר מחוץ לטריטוריה הישראלית. העובדה שהדין הפלילי הישראלי, ככלל, שותק לענייננו אינה מפתיעה בשים לב לכך שדיני הסמכות (Jurisdiction) נוסחו בעיקרם בעידן הטרום-אינטרנטי. עם זאת, אין ללמוד משתיקתו של המחוקק בעניין זה כי בהכרח כל פעולה, אשר יש לה מאפיינים העשויים להיתפש כאקסטרה-טריטוריאליים, כאסורה על פי הדין הישראלי. כפי שנטען בהרחבה בהמשך, הפעולה של חדירה לענן כפי שבוצעה בתיק זה הייתה פעולה שמובניה האקסטרה-טריטוריאליים מעטים. הפעולה הייתה שקולה ומדודה, ובכל הנוגע לשאלה החשובה לענייננו – בדבר הפוטנציאל לפגיעה בזכויות החשודים (לימים הנאשמים) – לא הייתה מגולמת בה כל פגיעה עודפת.

14. כאן המקום לציין כי בשנת 2014 פורסמה הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד-2014 (להלן: "**הצעת חוק החיפוש**").[2] לטענת ההגנה, המאשימה ביקשה להסתמך על הקבוע בהצעת החוק כדי לבסס את ההצדקה לביצוע פעולת החדירה לענן (ראו למשל פרוטוקול הדיון מיום 26.7.2020, בעמ' 230-231). עוד טענה ההגנה כי ההסדרה של פעולת חדירה לענן בהצעת חוק החיפוש מלמדת שנכון להיום אין בידי רשויות החקירה הסמכות לבצע חדירה לענן. טענות אלה, בכל הכבוד, הן שגויות: המדינה לא נשענה, ולא נשענת כעת בטיעוניה, על הצעת חוק החיפוש. הצעת חוק החיפוש שותקת בכל הנוגע לסוגיה שבפנינו, ולא ניתן ללמוד מן הקבוע בה לגבי פעולת חדירה לענן. הצעת חוק החיפוש עוסקת בשלוש פעולות חקירה אחרות, שעשויות להיות בעלות מאפיינים אקסטרה-טריטוריאליים:

א. המצאה של חומר מחשב האגור מחוץ לישראל – הכוונה הינה להוראה אשר תינתן לצד ג', על-בסיס צו שיפוטי, אשר יחויב להמציא מידע ממוחשב אשר אגור ברשותו לרשויות החקירה. סעיף 73(א) להצעת חוק החיפוש קובע כי אם שוכנע בית-המשפט כי קיימת עילה למתן צו המצאה בכל הנוגע לחומר מחשב הקשור לעבירה, יהיה רשאי בית-המשפט לצוות על בעל הגישה לחומר המחשב להמציאו, בתנאים שייקבע בית-המשפט. ההגדרה של "בעל הגישה לחומר המחשב", הקבועה בסעיף 72 להצעת חוק החיפוש הינה "בגיר שיש לו הרשאת גישה לחומר מחשב, בין שחומר המחשב מצוי בישראל ובין שהוא מצוי מחוץ לישראל".

ב. חדירה בהסכמת החשוד לחומר האגור מחוץ לישראל – הכוונה היא לחיפוש בחומרי מחשב אשר נערך על-בסיס הסכמתו של החשוד. בעניין זה קובע סעיף 90 להצעת חוק החיפוש כי "שוטר רשאי לבצע חדירה לחומר מחשב בלא צו בית משפט, אם בעל הרשאת הגישה לחומר המחשב הסכים לכך". עוד בעניין זה נקבע בדברי ההסבר לסעיף זה כי "כאשר החדירה לחומר מחשב נעשית בהסכמה, השוטר בא בנעליו של המסכים לחדירה ורשאי לבצע כל פעולה שהמסכים רשאי לבצעה, לרבות גישה לחומר האגור במחשבים מרוחקים, בארץ ומחוץ לה, אם למסכים הרשאה וגישה לחומר זה".

ג. עיון במידע שאגור מחוץ לישראל אך נגיש באופן פומבי לכולי עלמא – הכוונה הינה לעיון של חוקרי רשויות החקירה בישראל במידע אשר נגיש באופן פומבי ברשת האינטרנט כמו למשל פרסום באתר חדשותי מסוים. סעיף 97(ב) להצעת חוק החיפוש קובע כי "הוראות סימן זה לא יחולו על חדירה לחומר מחשב הפתוח לעיון הציבור בין שחומר המחשב מצוי בישראל ובין שהוא מצוי מחוץ לישראל, בין בתשלום ובין שלא

**Commented [ET7]:** גם סעיף 74 רלוונטי לעניין צו שמירה של חומר מחשב.

**Commented [ET8]:** יש מקום להפנות להרחבה המפורטת בהמשך המסמך לעניין פס"ד שרון וכו'.

[2] הצעות חוק הממשלה 867 (2014).

בתשלום״. מדברי ההסבר להצעת חוק החיפוש עולה כי מטרת הוראה זו הייתה להבהיר כי ״פעולה בחומר מחשב הפתוח לעיון הציבור אינה נחשבת בגדר פעולה הדורשת צו לפי החוק המוצע״, וזאת משום שלגבי חומר זה אין ציפייה לפרטיות.

15. בכל הנוגע לפעולות של חדירה בהסכמת החשוד לחומר האגור מחוץ לישראל ועיון במידע שאגור מחוץ לישראל אך נגיש באופן פומבי לכולי עלמא (פעולות ב׳ ו-ג׳ לעיל), השתיים הוספו להצעת חוק החיפוש בעקבות הצטרפותה של מדינת ישראל לאמנת מועצת אירופה בדבר פשעי מחשב (אמנת בודפשט, 2001) (להלן: ״**אמנת בודפשט**״).[3] שתי הפעולות מנויות בסעיף 32 לאמנת בודפשט, וכחלק מהליך ההצטרפות, הוחלט לקבוע באופן מפורש את שתי הפעולות בחקיקה הישראלית.

בכל הנוגע לפעולה של המצאת חומר מחשב האגור מחוץ לישראל (פעולה א׳ לעיל) – פעולה זו רחוקה מהקשרנו שכן מדובר ב״המצאה״ ולא ב״חדירה״, קרי פעולה המתבצעת בפועל על-ידי הנחקר או האדם שאליו ממוען הצו, ולא בידי הרשות החוקרת.

16. לעומת שלושת המקרים המנויים לעיל, הסוגייה של חדירה לענן אשר תבוצע בידי רשויות החקירה בישראל מתוך מכשיר הקצה של החשוד עצמו ולמידע אשר איננו נגיש באופן פומבי לכולי עלמא - לא נשללה במסגרת הצעת חוק החיפוש. אין בהצעת החוק, או בכל דבר חקיקה אחר או בפסיקה של בתי-המשפט, כוונה לקבוע הסדר שלילי שיחול על הפעולה שלפנינו.

**חדירה לענן איננה פעולה אקסטרה-טריטוריאלית**

17. ההגנה טענה כי הפעולה שבוצעה במקרה שלפנינו היא פעולה אקסטרה-טריטוריאלית. המונח ״אקסטרה-טריטוריאליות״ הוא מונח שאינו מוגדר בדין הישראלי, ולמעשה המרחב המקוון הפך את הדיון בשאלת האקסטרה-טריטוריאליות לשאלה מורכבת. זאת מכיוון שכמעט תמיד במרחב המקוון יכולים להימצא מובנים אקסטרה-טריטוריאליים ברמה כזו או אחרת (בוודאי בהסתכלות ב״משקפיים״ של העולם הפיזי). על כן נכון יותר להתייחס למרחב המקוון ככזה שיכול להתקיים בו ספקטרום רחב של סיטואציות אשר יש בהן מידה שונה של אקסטרה-טריטוריאליות. ברמה מופשטת יותר, ניתן אף לטעון שפעולה שכל כולה מתבצעת במרחב הטריטוריאלי של מדינה מסוימת, עדיין יכולה להשפיע על אינטרסים של מדינה זרה, וככזו אף היא יכולה להתפרש כבעלת מובנים אקסטרה-טריטוריאליים.[4] לכן, למעשה אין הבחנה דיכוטומית בין פעולה טריטוריאלית מובהקת לבין פעולה אקסטרה-טריטוריאלית.

**Commented [YW9]:** הכותרת לא מדויקת. השורה התחתונה של הפרק הזה היא זו - המאשימה סבורה כי המובנים האקסטרה-טריטוריאליים המגולמים בפעולת החדירה לענן כפי שתוארה לעיל הם מצומצמים למדי. כלומר לא שאין בכלל פעולה חוץ טריטוריאלית אלא שיש פה ספקטרום ואנחנו נמצאים בקצה הרחוק שלו – כלומר פעולה עם היבטים חוץ טריטוריאליים מצומצמים ביותר.

[3] מדינת ישראל הצטרפה לאמנת בודפשט ביום 9.5.2016, ראו החלטה 1405 של הממשלה ה-34 ״אישור הצטרפות מדינת ישראל לאמנת מועצת אירופה בדבר פשעי מחשב״ (14.4.2016).

[4] רעיון זה בא לידי ביטוי ב-Effects Doctrine במשפט הבין-לאומי, לפיה מדינה רשאית לרכוש סמכות שיפוט בשל העובדה כי להתנהגות מסוימת ישנן השפעות על אותה מדינה, זאת כאשר ההתנהגות הנדונה מתרחשת כולה מחוץ לטריטוריה של אותה מדינה. להרחבה על דוקטרינה זו ראו Malcolm N. Shaw INTERNATIONAL LAW 688-691 (6th ed., 2008). כן ראו: Hartford Fire Ins. Co. v. California, 509 U.S. 764 (1993), שם בית-המשפט העליון הפדרלי האמריקני קבע, בהקשר של הגבלים עסקיים, כי כאשר התנהגות אקסטרה-טריטוריאלית נעשתה במטרה להביא לאפקט פנימי בארצות-הברית, ובפועל נוצר אפקט שכזה – קיימת סמכות שיפוט לבתי-המשפט האמריקנים לדון לפי ה-Sherman Act, 15 U.S.C. (1980).

18. בעידן הטרום-אינטרנטי ניתן היה ליצור אבחנה חדה יותר, קרובה לדיכוטומית, בין פעולות בעלות מובנים מקומיים לבין פעולות בעלות מובנים אקסטרה-טריטוריאליים מובהקים המגלמים פוטנציאל ממשי לפגיעה בריבונותן של מדינות זרות. כך, למשל, במרחב הפיזי מובן וברור הוא ששוטר ישראלי אינו יכול לבצע חיפוש בבית בלונדון, שכן משמעות הדבר היא הפעלת סמכות שלטונית (שיכולה אף להתבצע תוך הפעלת כוח סביר בנסיבות המתאימות) בידי שוטר ישראלי, הנמצא פיזית בטריטוריה זרה ומבצע את הפעולה עצמה בטריטוריה הזרה. במרחב המקוון ניתן לנתק בין **מקום הימצא השוטר** לבין **מקום הימצא הראיה** המבוקשת (השרת שבו היא מאוחסנת), דהיינו השוטר יכול לבצע מישראל חדירה לחומר מחשב הנמצא בשרת המצוי בטריטוריה זרה. זאת, בעוד שבכל הנוגע לחיפוש במרחב הפיזי, השוטר יצטרך להימצא באותו המקום שבו תתבצע פעולת החיפוש. כמו כן, פרט למקום הימצא הראיה ומקום הימצא השוטר, גם **מקום ביצוע פעולת איסוף הראיה** הוא עניין מורכב יותר, כאשר מדברים על חקירה פלילית במרחב המקוון. פעולת חדירה לחומר מחשב הנמצא בשרת מרוחק מתבצעת למעשה בשני מקומות בו-זמנית: הן במקום שבו נמצא השוטר (בישראל) והן במקום שבו נמצא השרת המרוחק (שבו אגור המידע).[5]

**Commented [ET10]:** ראיתי שמפורט בהמשך, אבל האם אין מקום גם בניתוח כאן לציין הבחנה נוספת בין המרחב הפיזי למרחב המקוון במובן של מקום הימצא הראיה (בעוד שראיה פיזית מיקומה הוא יחיד, ראיה מקוונת עשויה בפועל להישמר בכמה שרתים שונים ובהתאם לכך אף בכמה במדינות שונות)

**Commented [NI11]:** אפשר להוסיף כבר פה שיש גם משמעות למקום הימצא המכשיר שבו מחפשים – האם הוא פיזית בישראל ובידי המשטרה, או האם מנסים לגשת גם אליו מרחוק בלי לדעת איפה הוא.

**Commented [GF12]:** אולי כדאי לחדד שביחס למרחב המקוון אין שינוי לענייו **מקום הפעלת הסמכות**. לשנות את הטרמינולוגיה ממקום הימצא השוטר למקום הפעלת הסמכות. למעשה, השוטר מפעיל את סמכויותיו עפ"י דין מתוך מדינת ישראל, גם אם מיקום הראיות אינו בתחומי המדינה.

19. בבואנו לבחון את קשת המצבים שבהם מתבצעות פעולות חקירה בעלות מובנים אקסטרה-טריטוריאליים במרחב המקוון, ניתן למנות בקצה האחד של הספקטרום מצב שבו, למשל, משטרת-ישראל תבקש לחדור לחומר מחשב של חברה זרה שנמצא בחו"ל, אותה הקים חשוד המצוי בישראל, כאשר חומר המחשב מצוי בשרת בחו"ל ומוגן בסיסמה. המשטרה תפרוץ את הסיסמה ותחדור לחומרים האמורים מתוך מחשב משטרתי בישראל. במקרה זה, מדובר בחשוד שביצע פעולה אקטיבית של הכפפה לדין הזר (על-ידי הקמת החברה הזרה בחו"ל), ומדובר בחדירה הכוללת "פריצה", תוך עקיפת הסיסמה מהמחשב המשטרתי אל השרת של החברה הזרה. ייאמר מייד כי גם סיטואציה זו אינה מצויה במדרגה של הסיטואציה מן המרחב הפיזי (של השוטר הישראלי המבצע חיפוש בבית בלונדון), מבחינת עוצמת הפגיעה באינטרס הריבוני הזר. בקצה האחר של הספקטרום ניתן למנות מצב שבו החשוד נמצא בישראל, חומרי המחשב מצויים בשרת ישראלי המופעל בידי חברה ישראלית, נפגעי העבירה ויתר המעורבים נמצאים בישראל. כידוע לכל, מצב זה הוא חריג למדי כאשר מדובר בחקירה בסביבה אינטרנטית, שכן חלק ניכר מהיישומונים שבהם נעשה שימוש יומיומי – הם למעשה יישומונים המופעלים בידי חברות זרות או ששרתיהם נמצאים מחוץ לטריטוריה הישראלית. להמחשה בלבד, נציין כי הפלטפורמות של פייסבוק, טוויטר, יוטיוב, Gmail, Dropbox, אינסטגרם, וואטסאפ, טלגרם, Google Drive, סקייפ, Zoom, Yahoo, iCloud, Google Photos,

[5] לפסיקה המכירה ברב-מקומיותו של המרחב המקוון, בהקשרים של סמכות שיפוט ראו למשל: רע"א 530/12 **יעקובוביץ נ' זיאס** (פורסם בנבו, 28.3.2012); בש"א 2267/12 **פרל נ' קבוצת איזנברג נדל"ן בארץ ובעולם בע"מ** (פורסם בנבו, 4.4.2012); תה"ג (מחוזי י-ם) 9037/09 **היועץ המשפטי לממשלה נ' עייש** (פורסם בנבו, 16.6.2010); ע"ר (מחוזי ת"א) 67771-07-18 **BOOKING COM .B.V נ' שפירא** (פורסם בנבו, 20.2.2019); ת"א (מחוזי ת"א) 30847-12-13 **Ciappa נ' דדון** (פורסם בנבו, 8.6.2014); ע"פ (מחוזי ב"ש) 21424-09-17 **מדינת ישראל נ' גולדשטיין** (פורסם בנבו, 26.9.2017); בש"א (מחוזי י-ם) 2841/03 **רעות אלקטרוניקה ורכיבים בע"מ נ' מראות אימאג' בע"מ** (פורסם בנבו, 14.12.2003); ת"א (מחוזי חי') 27608-04-11 **הטכניון - מכון טכנולוגי לישראל נ' Google Inc** (פורסם בנבו, 28.4.2011); ת"א (מחוזי נצ') 27593-09-12 **שטרוזמן נ' קידי- קיט י.ד.ע בע"מ** (פורסם בנבו, 29.11.2012); בש"א (שלום ק"ג) 884/02 **לנדאו נ' חסון** (פורסם בנבו, 1.5.2002); ת"א (שלום י-ם) 6612/05 **המכרז של המדינה בע"מ נ' אבו חצירה** (פורסם בנבו, 30.11.2005).

Google Maps, Viber – כל אלה ועוד רבות אחרות הן חברות זרות ושרתיהן אינם נמצאים בישראל.

במלים אחרות, נראה כי במרחב הסייבר פעולת חקירה בעלת מובנים העשויים להתפרש כאקסטרה-טריטוריאליים – היא הכלל, ולא החריג. זאת, בעוד שבמרחב הפיזי, פעולת חקירה בעלת מובנים אקסטרה-טריטוריאליים היא החריג, ולא הכלל.

20. כיצד יש למקם את הפעולה של חדירה לענן, כפי שהתבצעה במקרה שלפנינו, על הספקטרום של אקסטרה-טריטוריאליות? המאשימה סבורה כי המובנים האקסטרה-טריטוריאליים המגולמים בפעולת החדירה לענן כפי שתוארה לעיל הם מצומצמים למדי, וזאת אף אם נתבונן על מובנים אלה במשקפיים של המרחב הפיזי ובראי גישה טריטוריאליסטית מובהקת. זאת כיוון שמדובר בכניסה אל חשבון של המשתמש הישראלי בלבד בשרת המרוחק, וזאת מתוך מכשיר הקצה (מחשב או טלפון נייד) של החשוד, שנתפס כדין בישראל במסגרת פעולת חיפוש שנערכה בישראל. כיוון שבעניינו התאפשרה גישה פתוחה (דהיינו אין צורך להקליד את שם המשתמש או הסיסמה) מתוך מכשיר הקצה אל חומר המחשב המצוי בשרת המרוחק – יותר לחוקרים להיכנס אל חומר המחשב של המשתמש אשר נמצא בשרת המרוחק מבלי שנדרשה כל פעולת פריצה. על פי המתווה שלפיו מתבצעת החדירה לענן בעניינו, הרשות החוקרת למעשה רק **"נכנסת בנעליו" של החשוד** כמשתמש, ומעיינת **במידע בחשבונותיו של החשוד** בלבד ביישומונים ובשרתים, מידע שמהווה למעשה הרחבה מעשית של חומר המחשב של המשתמש שאגור במחשבו, הכל בהתאם למה שהותר לה בצו השיפוטי המסמיך ובהיתר שניתן על דעת היועץ המשפטי לממשלה.

21. זאת ועוד. מבחינה משפטית כבר הוכרו בישראל, לרבות בפסיקת בית-המשפט העליון, פעולות איסוף של מידע ממוחשב במרחב המקוון, שהן בעלות מובנים אקסטרה-טריטוריאליים משמעותיים. נפרט על כמה מהן להלן:

א. גישה לחומר מחשב הנגיש לכלל הציבור – הכוונה היא, לרוב, לאתר אינטרנט אשר נגיש לציבור הרחב הגולש באינטרנט, מבלי צורך להקיש פרטי התחברות או לשלם כדי לעיין בתכנים המפורסמים באתר האינטרנט. כך, למשל, נניח מקרה שבו נפתחה בישראל חקירה של הסתה לטרור ~~בפניסבוק~~ברשת חברתית, אשר בוצעה על-דרך של פרסום ברבים של קריאה לביצוע פעולות טרור על-גבי אתר אינטרנט הפתוח ונגיש לכלל הציבור. במסגרת אמנת בודפשט רשויות החקירה רשאיות לעיין במידע הנגיש לכלל הציבור ולהעתיקו, וזאת אף במקרה שבו אתר האינטרנט עצמו מאוחסן בשרת מחוץ לישראל.[6] כפי שהוזכר לעיל, עניין זה הוסדר במפורש גם בהצעת חוק החיפוש.

[6] סעיף 32(a) לאמנת בודפשט. יוער, כי התנאים המפורטים בסעיף 32 לאמנת בודפשט הם תנאי מינימום מבחינת האמנה, ומדינה החברה באמנה רשאית להוסיף עליהם מקרים נוספים שבהם היא תהיה רשאית לבצע פעולות בעלות מאפיינים אקסטרה-טריטוריאליים. ראו את דברי ההסבר לאמנת בודפשט: COUNCIL OF EUR., *Explanatory Report to the Convention on Cybercrime*, 53 (2001).

**Commented [CYS13]:** זה נכון גם כאשר החברה היא ישראלית. השרתים לא בהכרח בישראל

**Commented [ET14]:** לא הייתי מדגישה את זה כנימוק. בנוהל חיפוש בענן ניתן להקליד שם משתמש או סיסמה אם היא ידועה למשטרה ממקור אחר (ה"ס למשל), אבל אי אפשר להפעיל כלי פריצה.
מכאן שהעמדה שבאה לידי ביטוי בנוהל היא שגם אם יש צורך להקליד בפועל את הסיסמא, כל עוד לא מדובר בפריצה אין בכך כדי להעלות או להוריד לעניין שאלת האקסטריטוריאליות.

**Commented [GF15]:** מסכימה

ב. <u>גישה לחומר מחשב האגור בשרתים בחו"ל בהסכמה כדין של המחזיק בו</u> – הכוונה בפעולה זו היא למקרים שבהם מסכים החשוד כדין, הסכמה מדעת, לאפשר לרשויות החקירה לגשת אל המידע האגור בחו"ל שהחשוד הוא בעל הרשאת הגישה אליו.[7] על פי אמנת בודפשט, במקרה זה תהיינה רשויות החקירה רשויות לחדור אל המידע הממוחשב האגור בחו"ל.

**Commented [ET16]:** ככל שנכנסים לשאלה של מהו הדין הבינלאומי שחל בהקשר הזה , טענת הנגד היא כי אמנת בודפשט מהווה הסדר שלילי. יש לבחון (בעיקר מול המחלקה הבינלאומית) האם יש מקום לציין כאן או במקום אחר כי אמת בודפשט לא מהווה הסדר שלילי לעניין הדין הבינלאומי.

ג. <u>צו להמצאת חומר מחשב האגור בחו"ל</u> – בעניין **גלעד שרון** הכיר בית-המשפט העליון באפשרות להורות לחשוד, באמצעות צו המצאה, להמציא לרשות החוקרת חומרי מחשב המצויים פיזית בחו"ל. ובלשונו של בית-המשפט העליון:

> **"בחיים המודרניים של זמננו הנגישות אל חפץ מסוים אינה כרוכה בהכרח בהחזקתו הפיזית. לעתים יכול אדם להגיע 'בלחיצת כפתור' אל מידע המצוי בשליטתו, אך לא בהחזקתו הפיזית. את המסמכים שהחזיקו בעבר בני-אדם במגירה, בספרייה או בארכיון, מחליפים כיום, במקרים רבים, מאגרי מידע ברשת האינטרנט. כך למשל מקבלים לקוחות הבנקים מידע שוטף על פעולות בחשבונותיהם דרך האינטרנט ובאמצעות שימוש בססמה מזהה שמאפשרת להם, ולהם בלבד, נגישות מיידית אל המידע וכן את הנפקתו המיידית בצורה של מסמך. בצורה דומה מנויים בני-אדם על חשבונות דואר אלקטרוני שניתן להגיע אליהם, באמצעות ססמה, דרך כל מחשב המחובר לאינטרנט, בכל מקום ברחבי העולם, להדפיסם ולקבל את המידע בדרך של מסמך. התפתחויות אלה מחלישות במידה רבה את הקשר בין הנגישות או הזמינות של חפץ לבין החזקתו הפיזית. הן מלמדות כי מהיעדר החזקתו הפיזית של החפץ אין לגזור בהכרח את היעדר הנגישות אל אותו חפץ. בנסיבות אלה, כדי לקיים את תכליתו של סעיף 43 בנסיבות חיינו כיום, תכלית שהיא קידום החקירה או המשפט, מן הראוי לפרש את סעיף 43 כך שצו על-פיו יוכל להשתרע גם על חפצים אשר למי שהצו מופנה אליו שליטה עליהם במובן זה שבכוחו למוסרם או להציגם."**[8]

ד. <u>צווי חיפוש ותפיסה אקסטרה-טריטוריאליים בהליכים אזרחיים</u> - בתי המשפט בישראל התירו מספר פעמים, באמצעות צווים מסוג "אנטון פילר", לבצע חיפוש ותפיסה בעלי מאפיינים אקסטרה-טריטוריאליים בהקשרים אזרחיים. כך, למשל, בתי המשפט בישראל התירו לכונסי נכסים לבצע חיפוש בתיבות דואר-אלקטרוני, מבלי לסייג את מיקומם של השרתים שבהם נערך החיפוש לישראל בלבד. בעניין **פלוני**, התייחס בית-המשפט המחוזי בתל-אביב לצורך בהתאמת הדין למציאות הטכנולוגית, ובכלל זה מתן צווי תפיסה וחיפוש אף לחומרי מחשב מרוחקים. ובלשונו של בית-המשפט:

[7] סיטואציה זו הוכרה בסעיף 32(b) לאמנת בודפשט.
[8] ע"פ 1761/04 **גלעד שרון נ' מדינת ישראל**, פ"ד נח(4) 9, פסקה 9 לפסק דינו של השופט אור (2004).

**"ברם, ברור כי הדרך המקובלת כיום לאחסון מסמכים אינה מוגבלת אך ורק למסמכים פיזיים, כגון דפים וקלסרים, אלא במקרים רבים ואולי אף בדרך כלל, המידע מאוחסן במדיה דיגיטלית, כגון, בשרתי מחשב, בטלפונים ניידים ובשירותי ענן. על כן, חיפוש שיוגבל מראש רק למימד הפיזי (קלסרים ודפים) עלול להחמיץ את העיקר. המקרה שבפנינו יוכיח, שכן החייב נוהג להעביר הודעות והוראות גם באמצעות שימוש בתוכנת הווטסאפ ובמסרוני דואר אלקטרוני. יתר על כן, בנו פלמוני והעוזרת האישית פלונית, נוהגים אף הם בדרך דומה כאשר הם פועלים על פי הוראות החייב ומעבירים מסרים והודעות לצדדים נוספים, והכל מטעמו של החייב. ברור גם כי עולם המשפט איננו קופא על שמריו, ויש להתאימו למציאות הטכנולוגית המשתנה חדשות לבקרים, גם כאשר הטרמינולוגיה שבדברי החקיקה היא לעתים רבות ארכאית ומיושנת."**[9]

ראו גם את החלטת בית הדין הארצי לעבודה בעניין **כהן**, שבה הותר לכונס הנכסים לעיין בהודעות הדוא"ל שהיו אגורות בתיבת Gmail ("אצל חברת גוגל", כלשון בית-הדין), בין אם באמצעות שימוש במכשיר הקצה של המשיב ובין אם באמצעות "כל מחשב אחר", בלשון בית-הדין.[10]

22. לסיכום, אף אם ניתן לומר שבראייה פיזית-טריטוריאליסטית פעולת החדירה לענן היא אומנם בעלת מובנים אקסטרה-טריטוריאליים מסוימים, הרי שבוודאי אין לראות בה פעולה אשר פוגעת באינטרסים ריבוניים של מדינות זרות. בחקירה בסביבה מקוונת, המונח אקסטרה-טריטוריאליות הופך ממונח בוליאני ("0" או "1") למונח גמיש יותר. המקרה שלפנינו לא מבטא סטייה, מעקרונות של כיבוד ריבונותן של מדינות זרות, ואינו פוגע בעיקרון מחייב במשפט הבין-לאומי. מעל לכל, המשפט הישראלי הכיר זה מכבר בחריגות אקסטרה-טריטוריאליות בכל הנוגע לאיסוף מידע האגור בשרתים מרוחקים המצויים מחוץ לטריטוריה הישראלית.

**Commented [YW17]:** ניסוח בעייתי. עדיף לומר שהיבטיה האקסטרה טריטוריאלי מצומצמים או נמצאים בטווח הנמוך של המנעד. אני לא חושבת שאנחנו יכולים לדבר בשמן של מדינות זרות ולמר שלא פוגע.

**Commented [YW18]:** כנ"ל

**<u>חדירה לענן לא פוגעת בזכויות מוגנות של חשודים ונאשמים</u>**

23. כל ההגנות החוקתיות, וכל היבטי הזכות לפרטיות אשר הוכרו בחקיקה או בפסיקה בישראל – מוחלים בסיטואציה האמורה במלואם. משמע, החדירה לענן מבוצעת **באותו האופן ותחת אותן המגבלות** אשר במסגרתן מבצעות רשויות החקירה בישראל חיפושים בחומרי מחשב אשר אגורים בתחומי מדינת ישראל.

**Commented [ET19]:** כדאי לציין שוב במפורש שבית המשפט בהחלטתו היה מודע לכך שמדובר בצו חדירה לענן.

[9] פש"ר (מחוזי ת"א) 24052-10-17 **פלוני נ' אלמוני ואח'**, פסקה 23 לפסק דינו של השופט ברנר (פורסם בנבו, 8.6.2020). כאן המקום לציין כי בעניין זה, סמכותו של כונס הנכסים הוקמה מכוח צו החדירה שניתן על ידי בית-המשפט לפי סעיפים 108 ו-198 לפקודת פשיטת הרגל [נוסח חדש], התש"ם – 1980 (להלן: "**פקודת פשיטת הרגל**"). יודגש כי הסמכות לפעול בצורה אקסטרה-טריטוריאלית **לא** הוקנתה מכוח העובדה כי הכונס "נכנס בנעליו" של החייב, לפי סעיף 18ג(ד)(1) לפקודת פשיטת הרגל, אלא מכוח הכרעה שיפוטית מפורשת.
ראו גם התייחסות בפסק-דינו של בית-הדין הארצי לעבודה בע"ע (ארצי) 90/08 **איסקוב ענבר - מדינת ישראל - הממונה על חוק עבודת נשים ואח'** (פורסם בנבו, 8.2.2011), שם התייחס בית-הדין לאפשרות לחדור לשרתי דוא"ל מרוחקים, לרבות בחו"ל, באמצעות צווי אנטון פילר.

[10] בר"ע (ארצי) 38380-03-17 **כהן - טריגו חברה להשקעות ושיווק נדל"ן בע"מ**, פסקה 2 לפסק דינה של השופטת אופק גנדלר (פורסם בנבו, 11.6.2017).

בהתאם לכך, החדירה בענייננו התבצעה על בסיס צו שיפוטי, אשר איזן בין הפגיעה בפרטיותו של המחזיק בחומר המחשב לבין צרכי החקירה, בחן את נחיצות הצו ואת ההצדקה להוצאתו.

24. הפרוצדורה המחמירה של קבלת היתר מראש על דעת היועץ המשפטי לממשלה לפני הפנייה לבית-המשפט בבקשה לצו שיתיר חדירה לענן, נועדה להבטיח שהפעולה המתבקשת לא תחרוג מהאמור לעיל, ולא יתווספו לה מאפיינים אקסטרה-טריטוריאליים שיש בהם כדי להעצים טענות אפשריות לפגיעה בריבונותן של מדינות זרות. הגם שמטבע הדברים עניינו של התיק, והאיזון בין צרכי החקירה לבין פגיעה בזכות לפרטיות של החשוד ושל צדדים שלישיים, מובאים בפני היועץ המשפטי לממשלה, **הטעם המרכזי** לנקיטת פרוצדורה זו אינו מניעת האפשרות לפגיעה מוגברת בזכויות החשודים והנאשמים, אלא החיכוך הפוטנציאלי עם טענות בדבר פגיעה בריבונותן של מדינות זרות. בכך דומה הדבר לרציונל המחייב את אישורו של היועץ המשפטי לממשלה לצורך העמדה לדין של נאשם בעבירת חוץ.[11]

**Commented [GF20]:** האם נכון לשים על כך דגש כשיש כוונה לשנות את הנוהל ולייתר את הצורך במתן אישור יועץ

25. במלים אחרות, ההיתר של היועץ המשפטי לממשלה, והייחודיות של החדירה לענן, אינה במישור של הפגיעה בזכויות חשודים ונאשמים, שהן השאלות שעומדות לא אחת לדיון במסגרת ההליך הפלילי המתנהל בבית-המשפט, אלא במישור אחר, שהוא מחוץ להליך המשפטי המתנהל, של יחסי החוץ של מדינת ישראל עם מדינות זרות העשויות, בנסיבות מסוימות, לטעון לפגיעה בריבונותן, במקרים מסוימים של חדירה לשרתים מרוחקים. עקרון זה הושמע בפסיקת בית-המשפט העליון, בהקשר אחר מעט, בעניינו של **אייכמן**. באותו עניין נקבע כי פעילות אקסטרה-טריטוריאליות, בהקשר של נסיבות הבאת עבריין לתחום שיפוט, מעוררת שאלות במישור הבין-לאומי בלבד, ולא נוגעת למישור של זכויותיו של החשוד או הנאשם. ובלשונו של בית-המשפט:

> **"דין זה חל גם אם הטענה של העבריין היא, כי מעשה-החטיפה בוצע על-ידי שליחי המדינה התובעת אותו בפלילים, הואיל ובמקרה כזה הזכות שהופרה איננה זו של העבריין, כי אם הזכות הריבונית של המדינה שנפגעה – לאמור: הפרת הזכות מעוררת שאלה – אם פוליטית ואם שאלה של הפרת המשפט הבין-לאומי – בין שתי המדינות הנוגעות בדבר והיא צריכה למצוא את פתרונה במישור בין-לאומי זה. אך אין בכוחה לשמש נושא הדיון (justiciable) בפני בית-המשפט, אשר לתחום שיפוטו הובא העבריין."**[12]

26. להמחשת הפער בין שני המישורים – המישור של זכויות החשוד/הנאשם והמישור של יחסי החוץ – נציין את פרשת Gorshkov-Ivanov[13] בארצות-הברית משנת 2001. במקרה זה, ביצעו חוקרי ה-FBI חדירה מתוך מחשב הממוקם בתחומי ארצות-הברית אל שרת ברוסיה, ללא צו שיפוטי וללא ידיעת הרשויות הרוסיות. לאחר ביצוע החדירה והעתקת מידע מתוך השרת

---

[11] ראו סעיף 9(ב) לחוק העונשין.

[12] ע"פ 336/61 **אייכמן נ' היועץ המשפטי לממשלה**, פ"ד טז 2033, פסקה 13 לפסק הדין (1962). עקרון זה אומץ על-ידי בית המשפט העליון הפדרלי בארצות-הברית ב- United States v Alvarez-Machain, 504 US 655 (1992) וכן על-ידי בית-המשפט העליון בהולנד ב- Hoge Raad (Supreme Court) 5 Oktober 2010, Nederlandse Jurisprudentie 2011/169.

[13] United States v. Gorshkov, 2001 WL 1024026 (W.D. Wash., 2001).

הרוסי, פנו חוקרי ה-FBI לבית-המשפט האמריקני בבקשה לקבלת צו חדירה לחומר מחשב וקיבלו צו כאמור. לימים החשודים הועמדו לדין בארצות-הברית ובמהלך המשפט התעוררה הטענה מטעם הנאשמים כי הראיות הושגו שלא כדין, אך הטענה נדחתה והנאשמים הורשעו. חרף זאת, רשויות החקירה והתביעה ברוסיה הודיעו על הגשת כתב אישום נגד חוקרי ה-FBI אשר ביצעו את החדירה, וזאת בשל הפרת הדין הרוסי המקומי. פרשה זו ממחישה את ההבחנה בין המישור של ההליך המשפטי נגד החשודים, שהתנהל בהתאם לאמות המידה החוקתיות בארצות-הברית להגנה על זכויות החשודים והנאשמים בהליך המשפטי, לבין המישור של טענותיה של המדינה הזרה לפגיעה בריבונותה כתוצאה מפעולת חקירה הנוגעת לשרת מרוחק.

27. בענייננו, הזכויות המוגנות של החשודים והנאשמים ממשיכות לחול גם במקרה של חדירה לענן. מתוך תפישה זו, התבקש בית-המשפט להתיר את הפעולה, לאחר עריכת איזון קונקרטי בין צרכי החקירה לבין זכויות החשודים.

יצוין כי בארצות-הברית, בפסק-דינו של בית-המשפט הפדראלי העליון בפרשת Verdugo-Urquidez משנת 1990, נקבעה גישה שונה, לפיה התיקון הרביעי לחוקה האמריקנית, הנוגע לאופן ביצועו של חיפוש תוך שמירה על הזכות להליך הוגן, חל רק במקרים שבהם בוצעה פעולת חקירה בתוך גבולותיה של ארצות-הברית. באותו מקרה, קבע בית-המשפט העליון כי התיקון הרביעי לחוקה האמריקנית חל רק בתוך תחומי הטריטוריה האמריקנית, ולא חל כאשר מתבצע מעצר במדינה אחרת.[14]

גם בישראל נשמעה בעבר בבית-המשפט העליון גישה דומה, בפרשת **אל-מצרי**. בפרשה זו קבע בית-המשפט העליון כי המקום הגיאוגרפי המכריע לעניין תחולתו של חוק האזנת סתר, התשל"ט-1979, הוא המקום בו נמצא המשוחח, ולא המאזין. לכן, סמכויות בית המשפט והמשטרה לפי חוק האזנת סתר אינן משתרעות על רצועת עזה כאשר משטרת-ישראל מבצעת האזנת סתר למשוחח שאינו אזרח ישראלי הנמצא בשטח רצועת עזה (בשנת 1989, תקופה שבה רצועת עזה הייתה מוגדרת כשטח ב"תפיסה לוחמתית") לצד האמור נקבע כי במקרים אלו המשטרה אינה משוחררת מכל מגבלה, אלא עליה~~היא לא נדרשת לעמוד בדרישות ובתנאים הנקובים בחוק האזנת סתר, התשל"ט-1979, אלא~~ לעמוד ~~רק~~ בכללי המשפט המנהלי בעת פהעלת שיקול דעתה (סבירות, מידתיות וכדומה).[15] משמע, שבית-המשפט העליון לא החיל את חוק האזנת סתר, ובכלל זה התנאים והמגבלות שקבע המחוקק הישראלי במסגרת החוק~~במלואן את זכויות היסוד שקבע המחוקק הישראלי~~ על האזנת סתר שהתבצעה מחוץ לתחומי מדינת ישראל.

**Commented [ET21]:** הדוגמא הזו לא כל כך ברורה, אולי רק נדרש לתקן את הנוסח של הפיסקה, אבל על פניו עולה כי בוצע חיפוש לא חוקי ראשוני (ללא צו), ולאחר העתקת חומרי המחשב ביצעו חדירה לחומר מחשב כדין לפי צו בית משפט. אם אלו פני הדברים, זו לא דוגמא כל כך מוצלחת בשים לב לפסיקת אוריך, ודווקא הדוגמא יכולה לעורר הרבה טענות נגד. העמדה מספיק חזקה גם בלי הדוגמא הזו. או לחלופין נדרש לחדד האם גם הפעולה שבוצעה ללא צו הייתה בהתאם לחוק.

[14] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990). באותו מקרה, ביצעו שוטרים מה-DEA (Drug Enforcement Agency) חיפוש ביתו של אזרח מקסיקני בתוך תחומי מדינת מקסיקו, על-בסיס הסכמה של הרשויות המקסיקניות אך מבלי להצטייד בצו שיפוטי. כאשר טען הנאשם במהלך משפטו כי יש לפסול את הראיות, דחה בית-המשפט העליון את הטענה וקבע כי כאשר הן פועלת בתחומי מקסיקו, רשויות החקירה האמריקניות אינן כפופות לחובה החוקתית הקבועה בתיקון הרביעי לחוקה האמריקנית לקבל צו מבית המשפט מבעוד מועד המסמיך אותך לערוך את החיפוש.

[15] ע"פ 4211/91 **מדינת ישראל נ' אל מצרי**, פ"ד מז(5) 624 (1993).

כאמור לעיל, בעניינו ~~נקטה גישה מרחיבה, שביקשה לפרוש את~~אין חולק כי חלות ההוראות של פקודת סדר הדין הפלילי וכלל ההגנות החוקתיות של החשודים בעת ביצוען של פעולות חדירה לענן. מכאן, שאף אם היינו רואים בפעולת החדירה לענן כפעולה אקסטרה-טריטוריאלית (וכאמור, המאשימה סבורה שהיא בוודאי איננה פעולה אקסטרה-טריטוריאלית במהותה), ממילא מתייתרת מאליה השאלה שנדונה בפרשת Verdugo-Urquidez ובפרשת **אל-מצרי** בדבר החלת ההגנות של התיקון הרביעי לחוקה האמריקנית וחוק האזנת סתר (בהתאמה) על הפעולות האקסטרה-טריטוריאליות שבוצעו שם.

**[ET22]Commented:** לא בטוחה שההבחנה נכונה. דומה כי דווקא אל מצרי נוקט באותה גישה שאנחנו נוקטים בה לעניין חיפוש במחשב – תחולת החוק מתייחס לסמכות השיפוט כלפי האדם (כך כאשר מדובר בסמכות לבצע האזנה למואזן הנמצא במדינת ישראל או הסמכות לבצע חיפוש בחומר מחשב של חשוד שיש לבית המשפט סמכות שיפוט לגביו).

**[ET23]Commented:** יש מקום להוסיף התייחסות או בפרק הזה או בפרק של המשפט המשווה, שאפשר ללמוד גם ממדינות אחרות בין אם הן עיגנו את הסמכות במפורש בחוק או שהן פועלות מכוח הפסיקה, כי השיקולים והתנאים להפעלת הסמכות נוגעים ככלל לפגיעה בריבונות ולא לקיומה של פגיעה עודפת בזכויות חשודים.

**משפט משווה: הפרקטיקה של חדירה למחשבים מרוחקים המצויים בחו"ל מוכרת במדינות זרות רבות ~~ובמשפט הבין-לאומי~~**

28. רשויות חקירה במדינות רבות בעולם מבצעות חדירה למחשבים מרוחקים, המצויים מחוץ לטריטוריה, במהלך חקירות פליליות. בחלק זה נבקש להציג את הפרקטיקה במספר מדינות, וזאת בהתבסס על הפסיקה או החקיקה באותן מדינות, ועל מסמכי מדיניות של מועצת אירופה (Council of Europe). מטבע הדברים, התנאים לביצוען של פעולת החדירה למחשבים המרוחקים נבדלים ממדינה למדינה.

תחילה נציג מספר מדינות שבהן הוכרה הפרקטיקה של חדירה לשרתים מרוחקים מחוץ לטריטוריה, וזאת על סמך החקיקה הקיימת המתירה חדירה לחומר מחשב, וללא חקיקה ייעודית לעניין החדירה לשרתים המרוחקים. לאחר מכן נציג מספר מדינות נוספות שהכירו בחדירה לשרתים מרוחקים מחוץ לטריטוריה על בסיס חקיקה ייעודית, ולבסוף נציג מקורות מן המשפט הבין-לאומי המתייחסים לסוגייה דנן.

מדינות שהכירו בחדירה למחשבים מרוחקים המצויים בחו"ל ללא חקיקה ייעודית

**[CYS24]Commented:** ההבחנה בין מדינות עם/בלי חקיקה לא מועילה לדעתי. אם המטרה היא להגיד שיש סמכויות אינהרנטיות בצו חיפוש ולא נדרשת חקיקה מיוחדת כדי לבצע פעילות חיפוש מהסוג הזה, מבחינת הדין הפנימי, אז הדוגמאות של הולנד וקנדה, שלא קשורות לצו חיפוש, לא רלוונטיות. וגם, האזכור של תיק מייקרוסופט בעייתי כי שם הרוב קבע את ההיפך.

בהנחה שהטיעון שהועלה על ידי הנאשמים הוא טיעון של ריבונות, לדעתי הפרק הזה צריך להראות באופן כללי שמדינות לא רואות חיפושים כאלה כפגיעה בריבונות של מדינות אחרות או כפעילות חוץ-טריטוריאלית שהיא חסרת סמכות.
אם הטיעון היה שנדרשת חקיקה כדי לבצע פעילות חוץ טריטוריאלית, אז אני לא בטוח שהפרקטיקה של מדינות אחרות עוזרת. זה טיעון שדומה להלכת אמסטרדם, ועניינו דין פנימי: עד כמה הסכמויות הקיימות ברורות מספיק, ועד כמה החדירה היא חלק אינהרנטי מעובדה שותפת של שוטר.

**[NI25]Commented:** אולי כדאי להעביר את ארה"ב למדינות שבהן כן קיימת חקיקה ייעודית מסוימת

ארצות-הברית

29. החל משנת 2016, לפי Rule 41(b)(6) of the Federal Rules of Criminal Procedure, הדין האמריקני מקנה סמכות לבית-משפט להורות על מתן צו חיפוש בחומר מחשב, בדרך של גישה מרחוק (warrant to use remote access), גם כאשר אותו חומר מחשב אינו אגור במחוז השיפוט של אותו בית-המשפט. זאת בהתקיים אחת מן החלופות הבאות:
   א. מיקומו של חומר המחשב הוסתר באמצעים טכנולוגיים.
   ב. במסגרת חקירת עבירת של הפעלת נוזקה[16] אשר השפיעה על מחשבים או משתמשים במעל חמישה מחוזות.

[16] לפי Computer Fraud and Abuse Act, 18 U.S.C § 1030(a)(5) (1986).

30. מפסיקת בתי-המשפט הפדרליים לערעורים, עולה כי Rule 41(b)(6) of the Federal Rules of Criminal Procedure פורש בצורה רחבה כך שניתן מכוחו להוציא צו המתיר לרשויות החקירה להפעיל תוכנה החודרת למחשבי קצה ולדלות פרטים מזהים, כמו למשל כתובת IP – ללא ידיעתו של מחזיק מחשב הקצה. לענייננו הנדון כאן, נקבע כי היות שרשויות החקירה אינן מודעות למיקומם של מחשבי הקצה בעת שהן מפעילות את התוכנה, הרי שקיימת אפשרות ממשית כי בפועל התוכנה תחדור למחשבי קצה הממוקמים מחוץ לגבולותיה של ארצות-הברית.[17]

31. בהקשר בעל קרבה מסוימת לענייננו הנדון, מן הראוי להזכיר את פסיקתו של בית-המשפט הפדרלי לערעורים ב-2nd Circuit בעניין Microsoft[18], שם דובר בסוגייה של צו להמצאת מסמכים לפי ה-Stored Communications Act[19]. בעניין Microsoft נפסק כי לא ניתן לחייב את חברת Microsoft להמציא תוכן של תיבת דואר-אלקטרוני, כאשר תוכן זה מאוחסן על-גבי שרתים באירלנד, דהיינו מחוץ לטריטוריה האמריקנית. דעת הרוב העניקה משקל רב לכך שמדובר בצו המצאה המכוון כלפי צד שלישי (חברת Microsoft), אשר פרטיותו אינה נפגעת כתוצאה מהעברת המידע לרשויות אכיפת החוק – אלא הפגיעה היא בפרטיותו של בעל החשבון. במסגרת חוות-הדעת של אחד משופטי הרוב (Judge Lynch), ניתן משקל לכך שזהותו של בעל החשבון לא הייתה ידועה, ובפרט לא היה ידוע האם מדובר באזרח אמריקני. עוד נקבע על-ידו כי ככל שהיה מדובר באזרח אמריקני, הרי שהיה בעובדה זו כדי להחליש את האופי האקסטרה-טריטוריאלי של צו ההמצאה נשוא פסק הדין.

32. בהתייחס לפסק-הדין בעניין Microsoft, נבקש להעיר ולאבחן כדלקמן:

א. ראשית, כאמור לעיל יש להבחין בין צו המצאה אותו מבצע האדם שאליו מופנה הצו לבין צו חדירה לחומר מחשב אותו מבצעות רשויות החקירה. כמו כן, בענייננו, אין המדובר בצו המצאה המופנה לצד שלישי, כי אם המדובר בצו חדירה לחומרי מחשב המתבצעים בידי הרשות החוקרת ומכוונים ישירות לגורמים שהחזיקו כדין במידע הדיגיטלי בו נערך החיפוש. כאן המקום לציין כי בכל הנוגע לצווי המצאה המופנים לחשוד (הנמצא בישראל), בית-המשפט העליון הישראלי, בעניין **גלעד שרון**,[20] כבר פסק כי מותר לדרוש מהחשוד להמציא חומרים השייכים לו ומוחזקים מחוץ לטריטוריה הישראלית.

ב. בענייננו, דובר בצו חדירה לענן שהתבצע מתוך מכשירי קצה המקושרים למידע האגור בשרתים בחו"ל, והכל כאשר – מטבע הדברים - זהותם של מחזיקי המכשירים ידועה וכולם נמצאים בישראל.

ג. בענייננו, בשל המאפיינים הייחודיים של פלטפורמת הטלגרם, לא ניתן היה לזהות את מיקומו הפיזי של המידע המבוקש. על כך יש להוסיף את גישתה של חברת טלגרם,

[17] ראו למשל: United States v. Werdene, 883 F.3d 204 (3d Cir. 2018); United States v. Eldred, 933 F.3d 110 (2d Cir. 2019); United States v. Henderson, 906 F.3d 1109 (9th Cir. 2018); United States v. Levin, 874 F.3d 316 (1st Cir. 2017); United States v. Horton, 863 F.3d 1041 (8th Cir. 2017); United States v. Taylor, 935 F.3d 1279 (11th Cir. 2019).

[18] Microsoft v. United States, 829 F.3d 197 (2d Cir. 2016). יצוין כי בית-המשפט העליון הפדרלי העניק רשות ערעור (certiorari) לבקשת המדינה (United States v. Microsoft Corp., 138 S. Ct. 1186 (2018)), אך הדיון בערעור התייתר מאחר שבמהלך שמיעת הטיעונים נחקק ה-CLOUD Act (כפי שיפורט להלן), ורשויות החקירה פנו לקבלת צו בהתאם לחוק החדש.

[19] Stored Communications Act, 18 U.S.C. §§2701-2712 (1986).

[20] לעיל ה"ש 8.



**Commented [ET26]:** הייתי מציינת למען הסדר הטוב שסמכות זו לא כוללת חיפוש בתוכן של חומר המחשב (בשונה מהסוגיה שבפנינו).

**Commented [NI27]:** מציעה להדגיש את החלק הזה ואולי להעביר לתחילת הפסקה. בעניינו טלגרם לא איפשרה לגלות היכן מאוחסן המידע, נכון?

**Commented [CYS28]:** לא בטוח שזה רלוונטי ושזה מוסיף משהו להעלות את תיק מייקרוסופט. זה מביא את הדיון למקום אחר, שאין כאן ממש תועלת כי אנחנו לא רוצים לפתוח פתח לאמירות מהשופט בנושא הזה. (למשל, הבחנה בין המקרה נוכחי שהוא "טריטוריאלי" ולכן לא בעייתי, לעומת מקרה כמו במייקרוסופט שהוא" חוץ-טריטוריאליות" ולכן בעייתי יותר)

**Commented [ET29]:** מצטרפת להערה של סדריק מלה לעניין הרלוונטיות של פסק הדין (וכן ההרחבה בהמשך לעניין פסיקה נוגדת וה cloud act.,
מדובר בצו המצאה, שכפי שציינתם מעלה הוא עולם אחר מחדירה לחומר מחשב.
מוצע לכל היותר לציין את הדברים בקצרה. מכל מקום, יש להדגיש את ההבדל הראשוני לעניין ההבחנה בין צו המצאה לצו חקירה למחשב. לאחר מכן ההבחנה הנוספת בין חומר מחשב שמופנה לצד שלישי לבין חומר מחשב המוחזקים באופן ישיר.

המסתייגת מסיוע לרשויות חקירה זרות.[21] זאת בשונה מעניין Microsoft, בו היה ידוע כי המידע המבוקש אגור בשרתי החברה הממוקמים באירלנד. מדינת אירלנד אף הצטרפה להליך כ"ידידת בית-המשפט" והצהירה כי היא מוכנה לסייע בהמצאת המידע, בהליך של עזרה משפטית. במלים אחרות, בעניינו אין בהכרח חלופה מעשית לפעולת החדירה לענן, בעוד ש

ד. עוד יצוין כי בעקבות עניין Microsoft, נענה המחוקק לקריאת בית-המשפט ובשנת 2018 נחקק ה-CLOUD Act[22] המסדיר את סוגיית המצאת מידע על-ידי חברות אמריקניות כאשר המידע עצמו אגור בשרתים מחוץ לגבולות ארצות-הברית. יובהר כי ה- CLOUD Act קבע הסדר לעניין המצאת מידע על-ידי צד שלישי בלבד, ולא לעניין צו חדירה לענן באמצעות מכשיר קצה.

ה. סוגיית התחולה האקסטרה-טריטוריאלית של צו המצאה המכוון כלפי צד שלישי נדונה במדינות אחרות, ושם נפסק באופן מנוגד לפסיקה בעניין Microsoft. ראו למשל פסיקת בית-המשפט הפדרלי לערעורים בעניין eBay Canada,[23] שם נפסק כי חברת eBay Canada חייבת להמציא מידע האגור בשרתים מחוץ לגבולות קנדה משום שהמידע נגיש וזמין, ולכן אינו מהווה "foreign-based information". כן ראו את פסיקת בית-המשפט העליון בבלגיה בעניין Yahoo!,[24] שם נדחה ערעורה של חברת Yahoo! על הרשעתה בגין סירובה לספק לרשויות החקירה מידע על-אודות משתמשים (במסגרת חקירה פלילית בגין הונאה) בטענה כי מדובר במידע האגור מחוץ לטריטוריה של בלגיה.

**Commented [CYS30]:** גם כאן, מוצע לשקול את הטיעון הזה. זה נותן פתח לאמירה לפיה החוקיות של פעולה נעשתה בהתאם לידיעה מראש של המשטרה על מיקום השרתים. לפעמים יש ידיעה, לפעמים אין, לפעמים יש השערה סבירה אבל לא ידיעה אבסולוטית. וכשיודעים , לא תמיד אפשר/רצוי לפנות למדינה.

**Commented [CYS31]:** זה לא Rule 41?

**Commented [CYS32]:** אבל גם שם זה לא היה שאלה של חדירה לענן, כך שזה לא דוגמה של פרקטיקה של חדירה כאשר המכשיר נמצא בתוך המדינה

**Commented [CYS33]:** כנ"ל

## הולנד

33. בשני המקרים שלהלן התירו בתי-המשפט בהולנד לבצע חדירה לענן:[25]

א. Bredolab Case (2010) – במסגרת חקירה פלילית גילו רשויות החקירה בהולנד רשת של מחשבים "נגועים" (Botnet) שהכילה כ-30 מיליון מחשבים, חלקם מחוץ לטריטוריה ההולנדית. רשויות האכיפה ההולנדיות השתלטו על הרשת והודיעו באמצעות שליחת SMS לכל המחשבים הנגועים על כך שהם נגועים. לבסוף, הפילו רשויות החקירה בהולנד את השרתים ששימשו את הרשת.

ב. Descartes Case (2011) – בתיק זה התיר בית-משפט הולנדי חדירה לשרתי TOR אשר היה ידוע שאינם ממוקמים בהולנד (וככל הנראה מיקומם היה בארצות-הברית). השרתים הכילו תכנים פדופיליים רבים. במהלך החדירה, הועתק חלק מהחומר על-ידי רשויות האכיפה ההולנדיות וחומרי המחשב שהיו על השרת – הושמדו.

**Commented [ET34]:** הולנד צריכה להיות תחת הכותרת של מדינות שעיגנו את הסמכות בחקיקה.
במסגרת כך, התיאור צריך להיות הפוך, יש להביא קודם את החוק ההולנדי שמעגן את הסמכות בחקיקה, ורק אח"כ לציין לשלמות התמונה שעוד טרם חקיקת החוק בתי המשפט הכירו בסמכות חדירה לשרתים מרוחקים.
כפי שכתוב עכשיו אנחנו נותנים את הדגש לסמכות בית המשפט גם בהיעדר חקיקה מפורשת, בעוד שהלכה למעשה המחוקק ההולנדי סבר כי יש מקום לעגן סמכות זו במפורש ולא להסתפק בחוק הקיים.

**Commented [CYS35]:** זה לא מקרה דומה (לפחות מהעובדות שמוזכרות כאן) – זה לא נראה כמו תיק פלילי כי פעולת החדירה שמתוארת כאן לא קשורה לביצוע של צו חיפוש. זה יותר פעילות של הגנת סייבר כדי להפסיק מתקפה. צריך גם להביא ה"ש עם אסמכתא

[21] הרחבה בעניין זה תוצג להלן בפרק שכותרתו "הצדקות במישור הנורמטיבי להכרה בסמכותו של בית-משפט ישראלי להתיר חדירה לענן".
[22] CLOUD Act, 18 U.S.C §2523 (2018).
[23] eBay Canada Ltd. V. Canada (National Revenue) 1 F.C.R 145 (Ca., 2010).
[24] Yahoo! v. Belgium P.13.2082.N (Be., 2015).
[25] המקרים מובאים אצל Bert–Jaap Koops & Morag Goodwin, CYBERSPACE, THE CLOUD, AND CROSS-BORDER CRIMINAL INVESTIGATION 55-56 (2014) וכן אצל Cybercrime Convention Committee (T-CY) *Transborder Access and Jurisdiction: What are the Options?* 35-36 (2012).

משני המקרים שצוינו לעיל עולה כי הוכרה בהולנד פרקטיקה של חדירה לשרתים מרוחקים מחוץ לטריטוריה ללא חקיקה ייעודית.

להשלמת התמונה יצוין כי בשנת 2019 נקבע בחוק ההולנדי כי רשויות החקירה מוסמכות לחדור לחומר מחשב הנמצא בשימוש החשוד ולעיין בחומרי המחשב האגורים בו.[26] בכל הנוגע למיקום הפיזי של חומר המחשב, אין מגבלה לפיה על החדירה להתבצע לחומרי מחשב בהולנד בלבד. ככל שרשויות החקירה יודעות כי חומר המחשב אינו אגור בטריטוריה ההולנדית, עליהן לציין זאת בבקשה לצו החדירה.[27]

יתרה מכך, סעיף 125j ל-Dutch Code of Criminal Procedure מעניק סמכות לרשויות החקירה, לגשת ולבצע חיפוש בחומרי מחשב הנגישים מהמכשיר הנחפש, זאת במסגרת ביצוע חיפוש בחצרים לפי צו שיפוטי. בשנת 2018 פסק ה-Appeals Court of the Hague במפורש כי הגם שסעיף 125j לא מציין זאת במפורש, הרי שיש לפרשו כסעיף המסמיך את רשויות החקירה בהולנד לבצע חיפוש בדואר-אלקטרוני או בענן.[28]

**Commented [CYS36]:** שוב, הטיעון נראה קצת חלש, כי ההקשר לא מוסבר – אם זה מבחינת זכויות של נאשם, או בגלל גישה של מדינות לנושא הריבונות.

**Commented [CYS37]:** אם כן, אז זה שייך לחלק של "מדינות עם חקיקה"

<u>נורבגיה</u>

34. גם החוק הנורבגי לא מציין במפורש את הסמכות לפעול בדרך של חדירה לענן. עם זאת, בית-המשפט העליון הנורבגי פסק כי בסמכותה של משטרת נורבגיה לערוך חיפוש בשרתים הממוקמים מחוץ לגבולותיה של נורבגיה.[29]

35. באותו מקרה, השתמשה משטרת נורבגיה במחשביה של חברה בשם Tidal Music, במהלך חיפוש שנערך במשרדי החברה, כדי להוריד מידע אשר היה אגור בשרתים מחוץ לנורבגיה ונשמר שם על-ידי Tidal. החיפוש נערך על-בסיס צו שיפוטי של בית-המשפט המחוזי במחוז אוסלו וכלל, בין היתר, היתר גישה של המשטרה ל"Relevant data carriers and electronically stored information to which the person in question has access". במהלך החיפוש עצמו התנגדו נציגי החברה לכך שהחוקרים ייגשו למידע משני סוגים: קוד המקור של החברה, אשר היה מאוחסן בשרתים בבעלות Amazon בארצות-הברית; ופריטי דואר-אלקטרוני של המנהל הטכנולוגי של החברה, אשר הורדו מחשבון ה-Google של אותו עובד (ואשר המיקום המדויק של השרתים שבהם היו מאוחסנים הפריטים הללו לא היה ידוע).

36. בית-המשפט העליון בנורבגיה פסק כדלקמן:

א. המונח "storage place", המופיע בחקיקה הנורבגית המסדירה חיפוש בחצרים, כולל בתוכו גם שרת הממוקם מחוץ לגבולות נורבגיה. בהקשר זה נדחתה טענתה של Tidal לפיה על צו החיפוש להתייחס במפורש לביצוע החיפוש מחוץ לגבולות נורבגיה.

[26] Article 126nba of the Dutch Code of Criminal Procedure.
[27] Article 126nba(2) of the Dutch Code of Criminal Procedure.
[28] Doe v. State Case no. 22-004828-15 (The Netherlands, 2018)
[29] Tidal Music AS v. The Public Prosecution Authority, case no. 19-010640STR-HRET (Norway, 2019).

ב. משטרת נורבגיה לא הפרה הוראה בדין הבין-לאומי האוסרת עליה לבצע חדירה לענן כמתואר לעיל.

ג. לשם בחינת השאלה האם הופרה ריבונותה של מדינה זרה, יש לבחון האם הפעלת הכוח הכופה על-ידי רשויות החקירה בנורבגיה מפריעה לסמכות האכיפה הבלעדית של מדינה זרה. על כך השיב בית-המשפט העליון בשלילה וקבע כי כאשר מדובר בחיפוש שנערך מתוך אדמת נורבגיה, בחומרי המחשב של חברה נורבגית, על-בסיס צו שיפוטי נורבגי ותוך הפעלת סמכות אכיפה כדין כלפי החברה ועובדיה – הרי שאין מדובר בהפרת ריבונותה של מדינה זרה. עוד בהקשר זה ציין בית-המשפט העליון הנורבגי כי מדובר במידע ש-Tidal אחסנה בחו"ל, וכי היא יכולה הייתה לגשת אליו בכל עת.

<u>דנמרק</u>

37. אף בדנמרק הוכרה פעולת חדירה לשרתים שמחוץ לטריטוריה בפסיקת בית-המשפט העליון, וללא חקיקה ייעודית. בשנת 2012 קבע בית-המשפט העליון בדנמרק כי משטרת דנמרק רשאית לערוך חיפוש בשרתים הממוקמים מחוץ לגבולותיה של דנמרק.[30]

38. באותו מקרה, חשוד (המכונה "T") נחשד בביצועה של עבירה פלילית בתחום הסמים. משטרת דנמרק ביצעה חיפוש סמוי בחשבון הפייסבוק ובהתכתבויות הפייסבוק-מסנג'ר שלו, תוך שימוש בשם המשתמש והסיסמה של T, אשר היו ידועים למשטרה (כתוצאה, ככל הנראה, מהאזנות סתר). ככל הנראה, הכניסה לחשבונותיו של T מרחוק על-ידי המשטרה נעשתה כאשר החשוד עצמו שהה מחוץ לדנמרק. לטענת הנאשם באותו מקרה, החיפושים נערכו שלא כדין משום שהמידע היה ממוקם בשרתים מחוץ לדנמרק (בארצות-הברית, קנדה ולוקסמבורג), ולא ניתנה הסכמה של המדינה הזרה שעל אדמתה בוצע החיפוש.

39. בית-המשפט העליון של דנמרק פסק כי המשטרה הייתה רשאית לגשת לחשבונותיו של T משנודעו לה פרטי שם המשתמש והסיסמה. זאת, כיוון שמדובר בעבירה אשר נחקרה לפי החוק הדני, בידי הרשויות בדנמרק, וכיוון שבנסיבות העניין דיני העונשין הדניים חלים על העבירות המיוחסות לחשוד - רשאית הייתה המשטרה, כאמור, לבצע את הפעולות שביצעה בשרת המרוחק כפי שביצעה.

<u>שוויץ</u>

[30] Prosecution v. T, U 2012.2614 H (Denmark, 2012).

40. בשנת 2017 קבע בית-המשפט העליון בשוויץ קביעות דומות לאמור לעיל וקבע כי רשויות החקירה בשוויץ רשאיות לבצע חדירה לענן.[31] גם בשוויץ הסמכות האמורה הוכרה על-ידי בית-המשפט העליון בלא שהדבר הוסדר בחקיקה מפורשת.

41. באותו מקרה, הנאשם הואשם בעבירה פלילית של סחר בקוקאין, וביקש מבית-המשפט להורות על פסילת ראיות שהושגו תוך חדירה של משטרת שוויץ לחשבון הפייסבוק שלו. החדירה בוצעה באמצעות סיסמה שרשם החשוד בעודו במעצר על-גבי פתק.

42. בית-המשפט העליון בשוויץ קבע כי מי שמשתמש באמצעות חיבור אינטרנטי הנמצא בפנים הארץ בשירותיה של חברה זרה הניזונים מהאינטרנט, אינו פועל "בחו"ל". גם עצם העובדה, שהנתונים האלקטרוניים של אותו שירות הניזון מהאינטרנט מאוחסנים על שרתים המנוהלים בחו"ל, עדיין אינה מובילה לכך שהחקירה המקוונת המבוצעת בשוויץ תיתפש כחקירה בלתי מורשית בתחומה של טריטוריה זרה. בית-המשפט הוסיף וקבע כי ניתן להשתמש בתוצרי החיפוש האמור כראיות במשפט, וציין כי לא נפגעו זכויותיהם של צדדים שלישיים, חוץ מנמעני ההתכתבות שהיו גם הם שותפים לעבירה בנסיבות אותו מקרה.

**Commented [HV38]:** צריך להדפיס למעשה את כל פסקי-הדין בשפת המקור, ולצרף כנספחים לתגובה. לגבי המקומות שהשתמשנו במקורות משניים – נביא אותם (למשל בהולנד, אולי בעוד מקומות). לגבי תרגום – נסו לראות אם לפסקי-הדין האמורים יש תרגום באנגלית מהאינטרנט. אם לא, יש לפעול לתרגום פסקי-הדין דרך שירותי המשרד. עדיף לתרגם לאנגלית ולא לעברית.

<u>מדינות שהכירו בחדירה למחשבים מרוחקים המצויים בחו"ל כפעולה מותרת על פי חקיקה ייעודית</u>

43. מעבר למדינות שנסקרו לעיל, ניתן למנות מדינות נוספות שהעניקו, באמצעות חקיקה ייעודית, סמכות לרשויות החקירה לערוך חיפוש בדרך של חדירה לענן, לשרתים מרוחקים, אף אם הם מצויים מחוץ לטריטוריה של המדינה החוקרת.

<u>אוסטרליה</u>

44. החל משנת 2018, לבתי המשפט באוסטרליה ישנה סמכות להתיר לרשויות החקירה לבצע חדירה לענן, זאת לפי Section 43A of the Surveillance Devices Act (2004). סעיף זה קובע כי בבואו להוציא צו חיפוש במחשב (computer access warrant),[32] בית-המשפט אינו רשאי להעניק צו כאמור, אם התגלה כי צו כאמור עשוי להתבצע במדינה זרה, כל עוד לא התקבלה הסכמתו של גורם רשמי מוסמך מטעם המדינה הזרה. עם זאת, נקבע בהמשך הסעיף, כי חרף האמור לעיל, במקרים שבהם מתקיימים שני התנאים המצטברים הבאים, ניתן לבצע את החיפוש גם אם חומרי מחשב אגורים בשרת מרוחק, ואין צורך לקבל לשם כך את הסכמתו של הגורם הרשמי המוסמך מטעם המדינה הזרה:

[31] A v. Regionale Staatsanwaltschaft Berner Jura-Seeland, BGer, 1B_29/2017 (Switzerland, 2017).
[32] Section 6 of the Surveillance Devices Act (2004) מגביל את תחולת החוק לעבירות מסוימות, בין היתר עבירות שעונשן עולה על שלוש שנות מאסר, עבירות הלבנת הון ועוד.

א. האדם אשר אחראי על ביצוע הצו השיפוטי[33] יהיה נוכח באוסטרליה בעת ביצוע הצו.

ב. המיקום של המידע אינו ידוע, או שלא ניתן לגלותו במאמץ סביר.

**[CYS39]:** זה נראה כמו גישה מאוזנת. שאלה שעלולה לעלות היא – האם יש ריסון דומה בישראל? לדעתי צריכים להתייחס לזה. אחרת, זה פותו פתח לטיעון אפשרי לפיו באוסטרליה הסדירו את זה בחקיקה עם תנאים, וישראל לא הסדירה את זה בחקיקה בכלל ומנה לעשות זאת בלי תנאים

<u>ניו-זילנד</u>

45. לפי Section 103(4)(k) of the Search and Surveillance Act (2012), בתי-המשפט בניו-זילנד מוסמכים להוציא צו המתיר לרשויות החקירה לבצע חיפוש בדרך של גישה מרחוק (remote access search).[34] "חיפוש בדרך של גישה מרחוק" מוגדר בצורה רחבה וכולל חיפוש של "דבר" (thing) (אשר גם הוא מוגדר בצורה רחבה וכולל אף חפצים לא מוחשיים, ובין היתר כתובת דואר-אלקטרוני),[35] לרבות "מרכז מאגר מידע אינטרנטי" (Internet data storage facility), אשר אינו מוגבל מבחינת מיקומו הגיאוגרפי רק לשטחה של מדינת ניו-זילנד.[36]

<u>בלגיה</u>

46. לפי סעיף 88ter של ה-Code d'instruction criminelle (חוק סדר הדין הפלילי הבלגי), שופט חוקר מוסמך לתת צו המתיר לרשות חקירה לחדור לחומרי מחשב מרוחקים הנגישים ממכשיר קצה שנתפס כדין. ככל שחומרי המחשב המרוחקים אגורים מחוץ לטריטוריה, יש לדווח לרשויות הרלוונטיות במדינה הזרה. זאת רק אם ניתן, באופן סביר, לאתר את המיקום הפיזי של חומרי המחשב.

<u>מקורות נוספים</u> ~~במשפט הבין-לאומי~~

**[YW40]:** גם כאן זה משפט משווה ולא בינלאומי

47. בסקר שנערך על-ידי הנציבות האירופית (European Commission) בשנת 2018, עלה כי הדין הפנימי ב-20 מהמדינות החברות באיחוד האירופי מסמיך את הרשויות החוקרות, לאחר קבלת היתר שיפוטי, לבצע חדירה שהיא Extended, קרי גישה לחומרי מחשב מרוחקים דרך מכשיר קצה שנתפס כדין, וכן לבצע חדירה שהיא Remote, קרי גישה ממחשב משטרתי לחומרי מחשב מרוחקים, לאחר קבלת פרטי התחברות לחשבון, וזאת אף ללא ביצוע הכניסה דרך מכשיר קצה שנתפס במסגרת החקירה:

---

[33] המונח "אשר אחראי על ביצוע הצו השיפוטי" ("the person […] responsible for executing the warrant") אינו מוגדר ב-Surveillance Devices Act (2004). מבדיקה כללית בדין האוסטרלי עולה כי המונח "computer access warrant" הוא המונח המשמש בדין האוסטרלי לצורך הסמכת רשויות החקירה באוסטרליה לחיפוש במחשבים, ואין הכוונה לצו המצאה של חומר מחשב. זאת ניתן ללמוד, בין השאר, מכך ש-Section 27D of the Surveillance Devices Act (2004), אשר כולל את רשימת פרטי המידע הכלולים בצו שכזה, כולל גם את פרטי השוטר אשר יוציא לפועל את הצו. בנוסף, Section 27E of the Surveillance Devices Act (2004) כולל את רשויות הסמכויות הנלוות ל-computer access warrant, וכולל גם את סמכות הכניסה לחצרים ואת סמכות הוצאתו של המחשב מהחצרים שבהם נמצא המחשב – סמכויות משטרתיות באופיין.

[34] ראו: New Zealand Law Commission, *Review of the Search and Surveillance Act 2012*, §§12.25,12.73 (2017).

[35] Section 97 of the Search and Surveillance Act (2012).

[36] Section 97 of the Search and Surveillance Act (2012).

**"Direct access" refers to cases where authorities access data without the help of an intermediary, for instance following the seizure of a device ("extended search") or following the lawful acquisition of login information ("remote search"). The national law in at least 20 Member States empowers authorities, subject to judicial authorisation, to seize and search a device and remotely stored data accessible from it, or to use credentials for an account to access and search data stored under that account. This tool becomes more relevant as data is now regularly stored not on the local device but on servers in a different location, possibly outside of the Member State concerned or even outside of the EU"**[37]

48. עוד יצוין כי עמדתה של הנציבות האירופית היא שכאשר מיקומו של ספק השירות אינו ידוע, ראוי לאפשר לרשויות החוקרות לבצע אף חדירה שהיא Remote, שכאמור כוללת מספר רב יותר של מאפיינים אקסטרה-טריטוריאליים מאשר החדירה לענן אשר בוצעה בענייננו (שדומה במהותה לחדירה שהיא Extended). בהקשר זה, צוין מטעם הנציבות האירופית כי מיקום שרתיה של חברת טלגרם אינו ידוע:

**"Therefore, remote access could be considered in situations where other forms of access (e.g. direct cooperation with service providers) are: not possible or cannot be considered as feasible: e.g. the location of the provider is unknown, such as Telegram;"**[38]

~~49. במדריך טאלין השני,[39] מומחי נאט"ו טענו כי חיפוש בחומרי מחשב האגורים במדינה זרה, אך המיועדים להיות נגישים מתוך המדינה המחפשת – אינו מהווה פעולה אקסטרה-טריטוריאלית. זאת אף כאשר מדובר בחומרי מחשב המוגנים באמצעות סיסמה, וגם כאשר השגת פרטי ההתחברות נעשתה בשלב החקירה הסמוית.[40]~~

**Commented [CYS41]:** זה לא מקור שאנחנו רוצים לצטט

**הצדקות במישור הנורמטיבי להכרה בסמכותו של בית-משפט ישראלי להתיר חדירה לענן**

**Commented [ET42]:** אני חושבת שהפרק הזה צריך להיות לפני המשפט המשווה

[37] European Commission, *Impact Assessment: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* SWD 118, 11 (2018).

[38] שם, עמ' 70.

~~[39] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017). מדריך זה, שנכתב על-ידי צוות של מומחים למשפט בין-לאומי שמונו מטעם נאט"ו, עוסק בתחולת המשפט הבין-לאומי על פעילויות סייבר, אשר אינן עולות כדי מתקפות סייבר. כלומר, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO מדובר בהרחבה של מדריך טאלין הראשון CYBER WARFARE (Michael N. Schmitt ed., 2013) העוסק בתחולת המשפט הבין-לאומי על מתקפות סייבר.~~

~~[40] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 66-70 (Michael N. Schmitt & Liis Vihul eds., 2017).~~

49.~~50.~~ כפי שהצגנו עד כה, הפעולה של חדירה לענן איננה פעולה אקסטרה-טריטוריאלית; היא נוגעת לשאלות של יחסים בין-לאומיים וריבונות (ולא לזכויות מוגנות של חשודים ונאשמים); וישנן מדינות רבות אשר מבצעות גם הן פעולות חקירה דומות. בחלק זה של הטיעון, נציג שלוש הצדקות במישור הנורמטיבי להכרה בסמכויות של בית-משפט ישראלי להתיר חדירה לענן (וכפועל יוצא מכך – להכיר בסמכותן של רשויות החקירה לבצע את הפעולה של חדירה לענן): **ראשית**, במישור התפישתי – פעמים רבות למיקומו של חומר המחשב אין משמעות. **שנית**, במישור הטכנולוגי – מיקומו ה"פיזי" של חומר המחשב לא תמיד ידוע. **שלישית**, במישור המעשי – החלופה לחדירה לענן, בדמות בקשה לעזרה משפטית, אינה מספקת פעמים רבות את צרכי החקירה (ובוודאי כך בעניינו). נציג כעת הצדקות אלה כסדרן.

**Commented [GF43]:**

**Commented [GF44]:** גם כאן נראה לי נכון להתייחס להצדקה לעניין מקום הפעלת הסמכות במרחב המקוון שאינו משתנה, גם בחדירה לענן. בניגוד לביצוע פעולות חיפוש במרחב הפיזי.

## הצדקה במישור התפישתי - פעמים רבות למיקומו של חומר המחשב אין משמעות

50.~~51.~~ פעמים רבות למיקומם של חומרי המחשב אין משמעות, לא מבחינת התאגיד המספק את השירות המקוון, לא מבחינת מדינת ההתאגדות של התאגיד ולא מבחינת המשתמש. ניטול כדוגמה שירות של דוא"ל כגון Gmail. מבחינת המשתמש, אין משמעות מיוחדת לכך שמדובר בשירות זר, וניתן להניח כי המשתמש לרוב אף אינו טורח לברר היכן מצויים שרתי החברה. מבחינת חברת גוגל, מעניקת השירות, נראה כי אף היא אינה מייחסת חשיבות רבה למדינת התושבות של משתמש חדש הנרשם לשירותיה.[41] כך הוא גם ביחס לארצות-הברית, מדינת ההתאגדות של חברת גוגל העולמית, אשר אינה מפעילה כל מדיניות של התערבות, חובות דיווח, רישוי או כיו"ב פעולות המעידות על יחס לשאלת המיקום הטריטוריאלי של מקבלי השירות של Gmail.

**Commented [CYS45]:** זה לא בהכרח נכון לגבי כל החברות. למיטב זכרוני במייקרוסופט היה קשר למיקום השרתים ומקום פתיחת החשבון או הצהרת מדינת המוצא של הלקוח. יש גם לעיתים שיקולים של latency, וקרבת השרתים. בנוסף, בהקשרים אחרים אנחנו כן נרצה לטעון שיש בעלות "ישראלית" על שרת שממוקם בישראל. לכן, יש לעדן את הטיעון ולהגיד שהמיקום של השרת הוא לא המאפיין היחיד והוא לא בהכרח המאפיין העיקרי. אפשר לאזכר שלעיתים יש יותר משרת אחד שמאחסן אתו מידע.

**Commented [NI46]:** פה אתם מתייחסים לכך שאין חשיבות מהי מדינת התושבות של מקבלי השירות, לא לשאלת מיקום חומר המחשב. אולי אפשר להשאיר את האמירה שגוגל מעבירה את המידע של משתמשיה בין שרתיה ברחבי העולם לפי צרכיה ולא לפי מקום תושבותם.

51.~~52.~~ בשל מהפכת ה"טלפונים החכמים", הצריכה של שירותים מקוונים יכולה להינתן מכל מקום בו מצוי מקבל השירות. למעשה, תיאור נכון של המרחב המקוון של ימינו הוא כי לא זו בלבד שאפשר להגיע באמצעותו לכל "מקום", אלא שניתן לעשות כן "מכל מקום". במלים אחרות, מיקומו של מקבל השירות, נותן השירות, מיקומו של המידע בבסיס השירות – כל אלה נזילים וחסרי משמעות במקרים רבים (בוודאי במקרים של שירותים הניתנים ב"חינם", שאינם כרוכים בהעברת תשלום, מיסוי בגין מתן השירות בתשלום או כדומה).

52.~~53.~~ יצוין כי בכל הנוגע לסמכות שיפוט (Jurisdiction to adjudicate) במישור הפלילי, בתי המשפט בישראל החילו את סמכותם לשפוט על עבירות ~~פלילית~~ המתבצעות מתוך שרת בחו"ל, כל עוד התוכן נצרך או נקלט בישראל.[42] זאת מתוך הבנה שהמרחב המקוון חוצה גבולות

[41] בתנאי השימוש של חברת גוגל, אין התייחסות לפתיחת חשבון או שימוש בו ממדינה מסוימת, ראו: https://policies.google.com/terms?hl=en-US. לצד זאת, חברת גוגל מפרסמת באופן גלוי את מיקומם הגיאוגרפי של מרכזי המידע שלה, ראו: https://www.google.com/about/datacenters/inside/locations/. חברת גוגל איננה מפרסמת, ככלל, את האופן שבו מבזרת את המידע של משתמשיה, בחלוקה לפי מדינות.

[42] ב"ש (מחוזי ת"א) 90861/07 **קרלטון נ' יחידה ארצית לחקירות הונאה** (פורסם בנבו, 17.6.2007), אשר הוזכר בהסכמה בבית-המשפט העליון בע"פ 6889/11 **מדינת ישראל נ' עובד**, פסקה 11 (פורסם בנבו, 14.5.2012); ב"ש (מחוזי

מדיניים. לפיכך, נראה כי אין מקום לנקוט גישה הפוכה דווקא בכל הנוגע לסמכות האכיפה (Jurisdiction to enforce), ולקבוע כי, מצד אחד, אם מקצת העבירה מגיע אל מחשבים בישראל – קמה סמכות שיפוט; ומצד שני, אם מקצת מפעולת החקירה מגיע אל מחשבים מחוץ לישראל – נשללת סמכות האכיפה.

53. ~~54.~~ אם כך, וכאשר למיקומו של חומר המחשב אין משמעות (לא מבחינת המשתמש; לא מבחינת נותן השירות; לא מבחינת המדינה שבה מאוחסן המידע) – מתעמעם הטיעון לפיו חדירה לענן מהווה פגיעה בריבונותה של מדינה זרה, ומתחזקת ההצדקה להכיר בסמכותו של בית-משפט ישראלי להורות על חדירה לענן – שכן רק לישראל הזיקה המהותית לחקירת העבירה הפלילית.

**Commented [CYS47]:** זה לא טיעון משכנע. מקובל להגיד שסמכות שיפוט יכולה להיות קיימת באופן מקביל לשתי מדינות או יותר. אבל סמכות אכיפה בשטח של מדינה בה מתבצעת האכיפה. במקרה רגיל במרחב הפיזי, אפילו אם חוקרים רוצים רק קצת מהמידע שנמצא בחו"ל, הם צריכים לפעול בערוצי עזרה משפטית רגילים.

**Commented [CYS48]:** זאת אמירה גורפת מדי ואין לנו אינטרס לטעון אותה. עדיף להגיד שמיקומו של השרת שבו מאוחסן החומר הוא לא בהכרח גורם מכריע לעניין הסמכות

**Commented [NI49]:** אולי להוסיף שמבחינת טריטוריאליות יש יותר משמעות למקום העבריין, הקורבן והעבירה, יותר מאשר למקום חומר המחשב.

## הצדקה במישור הטכנולוגי - מיקומו ה"פיזי" של חומר המחשב לא תמיד ידוע

54. ~~55.~~ יישומים ושירותים שונים הניתנים באינטרנט כוללים מתן שירותי אחסון מידע. כך הוא למשל בכל הנוגע לשירותי גיבוי ב"ענן", שירותי דואר-אלקטרוני (בהם הדואר האלקטרוני אגור בשרת, ולא במכשיר הקצה), שירותי שיתוף קבצים ועוד. המשותף לכל השירותים הללו הוא שהמידע עשוי להיות אגור בשרתים שונים, הפזורים במקומות שונים בעולם. לעתים, בפרט למשל במקרה של שירותי מחשוב "ענן", אחסון המידע מתבצע באופן מבוזר, על פני שרתים שונים, שאינם ידועים למשתמש או למדינה החוקרת. משמע, למשל, שהודעת דואר-אלקטרוני אחת יכולה להיות מאוחסנת במספר שרתים ברחבי העולם, כאשר בכל שרת מאוחסן חלק אחר מההודעה (שם הנמען; תאריך השליחה; כותרת ההודעה; תוכן ההודעה; הצרופות להודעה וכן הלאה). אף אם מיקומם של השרתים היה ידוע, הרי שכאשר השירות מבוזר על פני כמה שרתים, לא ידוע בהכרח באיזה מן השרתים מצוי המידע המבוקש לחקירה. יוצא, אפוא, שניסיון לאתר את מיקומו הפיזי של המידע – נדון מראש לכישלון במבחן המעשה.

55. ~~56.~~ יצוין עוד כי קיימת הבחנה בין מדינת ההתאגדות של החברה המעניקה את השירות המקוון לבין מיקומם של השרתים של החברה. כך, למשל, שירות הדוא"ל של Gmail ניתן בידי חברת Google העולמית, המאוגדת בארצות-הברית, אולם שרתי החברה נמצאים במקומות שונים בעולם.[43]

56. ~~57.~~ בעניינו, טלגרם אינה מפרסמת את מיקומיהם של מרכזי המידע שלה. מעבר לכך, לפי פרסומים רשמיים של טלגרם, המידע של כל משתמש בפלטפורמה מאוחסן באופן מבוזר ברחבי העולם, בשרתים הממוקמים במדינות שונות.[44] כפי שיפורט להלן, ביזור המידע נעשה במכוון בכדי להקשות על גורמים מדינתיים המבקשים לקבל מידע מטלגרם.

**Commented [CYS50]:** מוצע לעדן את האמירה ולחשוב על מה נבקש לקדם בעתיד. לפי החוק האוסטרלי צריך לעשות מאמץ סביר לאתר את השרתים. אפשר לשאול את החברה. אולי הכיוון צריך יותר להיות שזה לא מעשי לנסות כל פעם לאתר את השרתים, או משהו כזה.
לפי Wikipedia:
For users who signed in from the European Economic Area (EEA) or United Kingdom, the General Data Protection Regulations (GDPR) are supported by storing data only on servers in the Netherlands, and designating a London based company as their responsible data controller
יש גם שאלה – האם נעשה ניסיון סביר לאתר את השרתים? לשאול את החברה?

---

י-ם) 1153/02 **מדינת ישראל נ' אברג'יל**, פ"ד תשסא(2) 728 (2002); ע"פ (מחוזי מרכז) 59085-08-16 **מזרחי נ' מדינת ישראל** (פורסם בנבו, 1.1.2018).

[43] https://www.google.com/about/datacenters/locations/, וכן ראו פירוט לעיל, ה"ש ~~13~~41.

[44] https://telegram.org/faq#q-do-you-process-data-requests. כמו כן, כאמור לעיל, גם בסקר של הנציבות האירופית נשמעה התייחסות לכך שמיקומיהם של שרתיה של חברת טלגרם אינם ידועים לרשויות אכיפת החוק בעולם. ראו ה"ש ~~25~~38.

<u>הצדקה במישור המעשי - בקשה לעזרה משפטית אינה מספקת את צרכי החקירה (ובוודאי כך בעניינו)</u>

57.~~58.~~ בכל הנוגע לחקירה פלילית ביחס לראיות דיגיטליות במרחב המקוון, החריג – של חקירה בעלת מובנים אקסטרה-טריטוריאליים – הופך לכלל, והמנגנונים של עזרה משפטית אינם בנויים לקצב המתחייב מקיומה של חקירה פלילית. הדבר נכון שבעתיים כאשר עסקינן בתיק מעצר כמו במקרה דנן, אשר במסגרתו לא ניתן היה במסגרת החקירה להשלים הליך של קבלת ראיות במסגרת בקשה לעזרה משפטית תוך עמידה במגבלות החוק בדבר מעצר ימים לצורכי חקירה.

58.~~59.~~ כידוע, מנגנון העזרה המשפטית ה"קלאסי" מותאם לחקירות במרחב הפיזי, והקצב שבו מתנהלים ההליכים של עזרה משפטית, אינו תואם את מאפייני המרחב המקוון כפי שיפורט להלן. מטבעו של מנגנון העזרה המשפטית, הוא מצריך שיתוף פעולה והדדיות בין מדינות, זאת מלבד לדרישת הפליליות הכפולה.[45] סקר שנערך על-ידי מועצת אירופה מצא כי זמן הטיפול הממוצע בבקשה לעזרה משפטית נע בין 6 ל-24 חודשים.[46] כאשר מדובר בראיות דיגיטליות אשר מצויות בשטחיה של מדינה זרה, מתחדד הקושי בקבלת עזרה משפטית. זאת, בין היתר, בשל המאפיינים הבאים:

א. כפי שפורט לעיל, לעיתים הראיות הדיגיטליות מבוזרות על פני שירותים (אפליקציות) שונות, ולעתים קרובות חלק מהשירותים משתמשים במספר שרתים שונים במדינות שונות, שמיקומם אף אינו ידוע למדינה החוקרת.

ב. לעתים השרתים בהם מאוחסן המידע הם במדינות עמן אין למדינת-ישראל יחסי עזרה משפטית כלל, ולעתים אף מדובר במדינות אויב.

ג. נוכח העובדה שרשת האינטרנט היא בין-לאומית, פעמים רבות מבצעי העבירות ימקמו את פעילותם מתוך שרת במדינה בה מותר לבצע את הפעולה, ובמקרים מעין אלה, אף אם תוגש בקשה לעזרה משפטית למדינה בה אגור המידע, זו תסורב מהטעם שאין "פליליות כפולה".

ד. הראיות הדיגיטליות נדיפות וניתנות לשינוי, למחיקה או להעברה ב"לחיצת כפתור", ועל כן הבקשות לעזרה משפטית לגבי כל תיק עלולות להיות מורכבות מדי ומאוחרות מדי. כך גם בעניינו, שכן בתיק זה החזיקו הנאשמים במנגנון "השמדת ראיות" יעיל במיוחד אשר אמור היה להיות מופעל בלחיצת כפתור.

ה. אמנם קיימים מנגנונים משטרתיים לשמירת ראיות הפועלים "סביב השעון" (24/7 network), עוד בטרם העברה של בקשה מסודרת לעזרה משפטית. אולם, מנגנונים אלה פועלים רק בקרב המדינות החתומות על אמנת בודפשט (או מדינות שהן צד להסכמות ה-

[45] ראו: Christine Galvagna, *The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform*, 9 NOTRE DAME J. INT'L COMP. L. 57, 59-60 (2019).

[46] Council of Europe, *T-CY Assessment Report. The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, CYBERCRIME CONVENTION COMM. 123 (2014),

G8 בנושא); הם רלוונטיים רק כאשר מיקומן של הראיות ידוע למדינה החוקרת, וכאשר אין בעיה של "פליליות כפולה"; לעתים ההקפאה תתבצע אך מסירת הראיות המוקפאות למדינה המבקשת בדרך של עזרה משפטית תתעכב.

59.~~60.~~ בכל הנוגע לחברת טלגרם, שבה עסקינן בענייננו – הדבר נכון שבעתיים. לפי פרסומים רשמיים של טלגרם, החברה שמה לה למטרה להפחית למינימום ההכרחי את שיתוף הפעולה עם רשויות החקירה בעולם.[47] כפי שהוצג לעיל, המידע של כל משתמש בטלגרם מבוזר בין שרתים הממוקמים במדינות שונות ברחבי העולם.[48] זאת בכוונה תחילה, בכדי שטלגרם תוכל לדרוש לקבל הוראה שיפוטית למסור את המידע מכל המדינות שבהן מאוחסן חלק מהמידע.[49] משמעות הדבר היא שעל רשויות החקירה בישראל לפנות במספר בקשות עזרה משפטית, למדינות שונות, בבקשה לקבל חלקים שונים מתוך המידע המאוחסן בשרתים של טלגרם. בהקשר זה יצוין עוד כי חברת טלגרם ציינה במפורש כי אף פעם לא נענתה לבקשה לקבלת מידע שהתקבלה מרשות מדינתית זרה כלשהי. כך, בכל הנוגע לטיפול בבקשות לקבלת מידע (data requests), ציינה חברת טלגרם כי:

> **"To this day, we have disclosed 0 bytes of user data to third parties, including governments."**[50]

60.~~61.~~ בהעדר חלופה מעשית יעילה דיה, הרי שבמצב הנוהג כיום, רשויות החקירה חסרות מידע ערכי רב כמעט בכל חקירה הכוללת ראיות דיגיטליות (ובפועל אלה הן מרבית החקירות), שכן "שדה הראייה" שלהן מוגבל מראש בכל הנוגע לחשבונות דוא"ל ומידע נוסף האגור בחו"ל, ובפרט בכל הנוגע למידע בטלגרם. יתרה מכך, ללא הכרה בסמכות של בית-המשפט להתיר לחוקרים לבצע חדירה לענן, בנסיבות כבענייננו, עלול להיווצר תמריץ חזק למבצעי עבירות לנהל את פעילותם באמצעות שרתים מרוחקים הנמצאים במדינות שאינן משתפות פעולה עם רשויות החקירה במדינת ישראל, או באמצעות פלטפורמות שאינן משתפות פעולה עם מדינת-ישראל. כך, יצליחו מבצעי העבירות ליצור לעצמם מרחב חסינות מפני אכיפה פלילית.

**Commented [CYS51]:** להיזהר עם הטיעון הזה כי במקרים בהם יש צורך לחדור בחשבונות של פייסבוק וגוגל אי אפשר לטעון אותו כי החברות האלה כן משתפות פעולה.

[47] https://telegram.org/faq#q-do-you-process-data-requests.
[48] ראו ה"ש **Error! Bookmark not defined.**~~13~~, בעמ' 70.
[49] ה"ש **Error! Bookmark not defined.**~~16~~.
[50] ה"ש **Error! Bookmark not defined.**~~29~~.