

1. אליחנדרו קאלוילו אונה, מס' דרכון מקסיקני.
2. סבסטיאן אלדברן באראגאן הידאלגו, מס' דרכון מקסיקני
3. גספאר רפאל קברירה היהננדיז, מס' דרכון מקסיקני
4. מאריו ארנסטו פאטרון סאנשיז, מס' דרכון מקסיקני
5. ח'ורה סאנטיאגו אגירה אספינוזה, מס' דרכון מקסיקני.

המיוצגים על ידי באי כוחם עו"ד עלא מחאגינה  
שייחי ג'ראח, דרך שכס 43, ת.ד. 19870, ירושלים  
טל: 02-5824717, פקס: 02-5826010

ו/או ע"י עו"ד מחמד דחלה ואח'  
רח' אבן בטוטה 2, ת.ד. 55999, ירושלים  
טל: 02-6274070, פקס: 02-6274060

התובעים

-נגד-

1. קבוצת אן. אס. או. טכנולוגיות בע"מ (ח.פ. 514395409)
  2. קיו סייבר טכנולוגיות בע"מ (ח.פ. 514971522)
- שכתובתן הרשומה היא: גלגל הפלדה 22, הרצליה, 4672222

הנתבעות

מהות התביעה: צו מניעה קבוע/כספית  
סכום התביעה: 2,505,000 ש"ח

כתב תביעה

1. בתביעה זו, התובעים יהיו מיוצגים ע"י באי כוחם הנ"ל אשר כתובתם להמצאת כתבי בית-דין הינה ככתובת באי כוחם כנ"ל.
2. כל טענה ו/או פרט ו/או עובדה הנטענים בכתב תביעה זה נטענים במצטבר ו/או בהשלמה ו/או לחילופין, הכל לפי העניין ולפי הקשר הדברים ו/או הדבקים.

א. מבוא

3. עניינה של תביעה זו הוא מערכת ריגול מיוחדת-רוגלה-שהנתבעות פיתחו ואשר נעשה בה שימוש כנגד התובעים כפי שיפורט בהמשך כתב התביעה. הריגול באמצעות המערכת מתבצע לאחר החדרת תוכנה מרחוק בתוך מכשיר טלפון חכם של האדם שאחריו רוצים לרגל ומבלי לקבל את

אישורו. עם סיום התקנת המערכת בתוך המכשיר היא מראה ומשקפת את תוכנו אצל הגוף שמבצע את הריגול.

4. מערכת הריגול-רוגלה- שהנתבעות פיתחו ידועה בשם "פגסוס"- Pegasus (להלן: "המערכת" או "מערכת פגסוס"). המערכת מאפשרת השתלטות על מכשירים ניידים באופן מלא. היא מאפשרת פעולות מעקב פסיביות כגון גישה לשיחות מוקלטות על המכשיר, קבלת גישה לצילומים השמורים במכשיר, גישה להודעות כתובות (טקסט), וגישה לתעבורת אינטרנט. בנוסף, המערכת מאפשרת גם לשלוט במכשיר באופן אקטיבי, למשל על ידי הפעלת המצלמה מרחוק כדי לצפות בסביבתו של המשתמש.

5. לפי מה שפורסם בכלי התקשורת השונים הן ברחבי הארץ והן בעולם, מערכת הריגול- הרוגלה שהנתבעות פיתחו נחשבת למתוחכמת ברמה חסרת תקדים והיא עדיפה על רוגלות אחרות מתחרות בשוק. ייחודה של מערכת "פגסוס" נובע מהדרך בה מותקנת בתוך המכשיר, וגם ביכולתה להישאר חבויה מבלי להבחין בקיומה ובפעילותה.

6. לאור אופיה של המערכת, ובהתחשב בפוטנציאל המסוכנות האדיר הטמון בה, ההתייחסות אליה היא כאל נשק, ועל כן מערכת "פגסוס", בדומה לנשק, נמכרת תחת פיקוחו של אגף הייצוא במשרד הביטחון, בהתאם לחוק הפיקוח על ייצוא בטחוני 2007. בהתאם לפרסומים השונים בכלי תקשורת ישראליים, משרד הביטחון מאשר לנתבעות למכור את המערכת רק לגופים ולמדינות מסוימות הנמצאות ביחסים תקינים עם מדינת ישראל.

7. על פיקוח המדינה באשר למכירת המערכת ניתן ללמוד מהעובדה כי ביום 5.7.2018 הותר לפרסום כי הפרקליטות הגישה כתב אישום תמור כנגד אחד מעובדיה לשעבר של הנתבעת מס' 1 שעל פי עובדות כתב האישום העתיק את מערכת "פגסוס" באופן לא חוקי וניסה למכור אותה לגוף זר וללא ידיעת הנתבעות וללא אישור משרד הביטחון. כנגד העובד לשעבר הוגש כתב אישום בעבירות של ניסיון לפגיעה ברכוש שהיה בו כדי לפגוע בביטחון המדינה, גניבה בידי עובד, ביצוע פעולת שיווק ביטחוני ללא רישיון שיווק ביטחוני ושיבוש או הפרעה לחומר מחשב.

=רצ"ב העתק כתבה מאתר "דה מרקר" מיום 5.7.2018 באשר להגשת כתב האישום, מסומן ע/1.

8. הנתבעות מכרו ומוכרות את המערכת לגורמים שונים בעולם, ובהם גופים ממשלתיים ועסקיים. כך בשנת 2014, ולעניינו, הנתבעות מכרו את התוכנה לגורמי ממשל במקסיקו, באמצעות חברה פרטית שהוקמה במקסיקו למטרה זו בלבד ככל הנראה, על פי חוזה שנחתם בין הצדדים ביום 11.11.2014. החוזה שנחתם כולל נספח טכני המפרט במדויק מהי מערכת "פגסוס", דרך החדרת המערכת למכשיר היעד, דרך הפעלתה, ואת שלבי עיבוד החומרים הנקלטים באמצעות המערכת אצל הגורם המבצע את המעקב.

=רצ"ב העתק מהחוזה מיום 11.11.2014 בשפה הספרדית, מסומן ע/2.

=רצ"ב תרגום לאנגלית של החוזה בשפה הספרדית מיום 11.11.2014, מסומן ע/3.



9. כפי שיפורט להלן, תפקידן של הנתבעות בפעולות המעקב אינו מסתיים עם מכירת המערכת לגורמים שונים, אלא הוא נמשך מעבר לשלב זה והנתבעות ממשיכות לגלות מעורבות אקטיבית בשלבים של העברת הנתונים, עיבוד הנתונים, הדרכה על הפעלת המערכת, וגם סיפוק עדכונים ושדרוג למערכת כפי שמובהר במפרט הטכני הנלווה לחוזה הנ"ל.

10. יש לציין, כי הנתבעות מעולם לא התכחשו לאחריותן על ייצור המערכת ו/או על העובדה כי הן התקשרו בעסקה באמצעותה מכרו את המערכת לגורמי ממשל במקסיקו והן התעלמו מפניות רבות לקבלת הבהרות שנעשו דרך שגרירות מקסיקו בישראל.

## **ב. הצדדים לתביעה**

### **התובעים**

11. התובעים הינם אזרחי ותושבי מקסיקו, והם קבוצה של פעילים חברתיים, פעילי זכויות האדם, עורכי דין ועיתונאים המתמחים בעיקר בסיקור נושאים הקשורים לשחיתות שלטונית.

12. התובע מס' 1 הוא מנכ"ל ארגון "El Poder del Consumidor" (כוחו של הצרכן), שהוא ארגון הפועל במקסיקו שמטרתו היא הגנה על זכויות צרכנים וקידומן, במיוחד בקשר לבריאות המזון והמאבק בהשמנה ומחלת הסוכרת במקסיקו. הארגון גם פועל בתחום ניידות עירונית ובטיחות מכוניות.

13. התובע מס' 2 הוא עיתונאי במקצועו שכותב בעיקר באתר Aristigui Noticia <https://aristeguinoticias.com/>, שהוא אתר עיתונות תחקירים המתמחה בסיקור נושאי שחיתות שלטונית. התובע מס' 3 גם הוא עיתונאי תחקירים שעבד בעבר באתר Aristigui Noticia. שניהם נטלו חלק פעיל בחשיפת פרשת שחיתות מהגדולות בתולדות מקסיקו- פרשת ה-Casa Blanca (פרשת הבית הלבן).

14. התובע מס' 4 הינו עורך דין ומנכ"ל של מרכז זכויות האדם על שם מיגל אגוסטין פרו הוארז (Centro de Derechos Humanos Miguel Agustín Pro Juárez). המרכז -ידוע בשמו הקצר "Centro Prodh"- נוסד בשנת 1988 והינו אחד מארגוני זכויות האדם המובילים והמכובדים ביותר במקסיקו. התובע מס' 1 (ובכירים אחרים במרכז) נפלו קורבן לפריצה באמצעות מערכת "פגסוס" בתקופה שהמרכז היה מעורב בפעילות הקשורות בהגנה, חקירה ותיעוד מקרים בולטים של הפרות זכויות אדם במקסיקו. פעילות המרכז כללה בין השאר מעורבות בולטת בחקר המקרה של היעלמותם ההמונית בכפייה של 43 סטודנטים בעיירה Ayotzinapa בשנת 2014. אירוע טרגי זה ידוע בשם "ההיעלמות ההמונית באיגואאלא". כמוכן, המרכז היה מעורב בחקירת ותיעוד פרשת הוצאות להורג וללא משפט של אזרחים על ידי הצבא המקסיקני בעיירה Tlatlaya במדינת מקסיקו. המרכז גם היה מעורב גם בפרשיות מסעירות אחרות במקסיקו כגון פרשת העינויים המיניים כנגד מספר נשים שהתבצעה על ידי המשטרה בעיירה San Salvador Anteco בשנת 2006 בזמן שאנריקה פנה נייטו (הנשיא היוצא של מקסיקו) היה המושל של מדינת מקסיקו.

15. התובע מס' 5 הינו עורך דין בכיר המתמחה בזכויות אדם ומשמש סמנכ"ל של מרכז Centro Prodh. מתוקף תפקידו נטל התובע מס' 5 חלק פעיל בחקירת פרשת ההיעלמות בכפייה של 43 סטודנטים בעיירה Ayotzinapa בשנת 2014, ונתן ליווי משפטי למשפחות הסטודנטים.

#### הנתבעות

16. הנתבעת מס' 1 הינה חברה הרשומה בישראל. הנתבעת הוקמה בשנת 2010, ע"י היוזמים ניב כרמי, שלו חוליו ועומרי לביא, והחברה נקראת בראשי תיבות של שמותיהם של המייסדים. הנתבעת מפתחת ומשווקת מערכות ריגול למעקב אחרי טלפונים ניידים.

17. הנתבעת מס' 2 הינה חברה הרשומה באותה כתובת של הנתבעת מס' 1, ומניותיה בבעלות מלאה של אותה חברה המחזיקה במניות הנתבעת מס' 1, והדירקטורים הרשומים של שתי החברות הנתבעות הינם אותם אנשים וישויות. על פי פרסומים בתקשורת, הנתבעת מס' 1 וואו בעלי מניותיה וואו מנהליה מנסים להמציא מחדש את המותג של הנתבעת מס' 1 והם עכשיו משווקים אותם מוצרים תחת השם של הנתבעת מס' 2.

=**רצ"ב** פלט מידע על הנתבעות 1 ו- 2 מאת רשם החברות, מסומן ע/4.

18. על פי המידע מרשם החברות, מניות הנתבעת מס' 1 והנתבעת מס' 2 מוחזקות באופן מלא על ידי OSY Technologies S.A.R.L, חברה הרשומה בדוכסות הגדולה של לוקסמבורג ושמספרה הרשום הוא 184226B. חברת האם, OSY Technologies S.A.R.L, הינה בבעלות מלאה של חברת 2 Square, ושמספרה הרשום הוא 192125B ואף היא רשומה בלוקסמבורג. חברת 2 Square היא בבעלות מלאה של חברת Triangle Holdings, הרשומה בלוקסמבורג תחת המספר 192115B, שהיא בבעלות מלאה של Osy Holdings (Cayman), הרשומה באיי קיימן. לפי דו"ח השנתי של OSY Technologies לשנת 2017, שוויה של הנתבעת מס' 2 הינו 408,549,000 דולר ארה"ב (408 מיליון דולר).

=**רצ"ב** הדו"ח השנתי לשנת 2017 של OSY Technologies, מסומן ע/5.

19. חברת האם, OSY Technologies, גם מחזיקה בחברות אחרות המתמחות בריגול, בין השאר, היא הבעלים של חברת CS Circles Technologies ו- CT Circles Technologies, שתיהן רשומות בלימסול שבקפריסין ומספרן הרשום הוא 336847HE ו- 239933HE בהתאמה. שתי החברות הינן בבעלות OSY Technologies באמצעות החברה הקפאריסאית IOTA Holdings Ltd, אף היא רשומה בלימסול ומספרה 337445HE. הנתבעת מס' 1 היא גם הבעלים של חברת PFOS Technologies Limited, הרשומה בבריטניה ומספרה 8521034. חברות אלו הינן חברות קשורות עם הנתבעות והן פועלות ביחד ומשתפות פעולה במישרים שונים.

20. כך למשל, באחד מהחוזים שהנתבעת מס' 1 חתומה עליו בנוגע להתקשרות בפעילות שלה במדינת איחוד האמירויות הערביות, הנתבעת מס' 1 מתוארת באופן הבא:



"NSO Group Technologies Ltd. ("NSO") and Circles Technologies Ltd. are affiliates of OSY Technologies S.a.r.l ("OSY", and together with any of its affiliates, the "Company")"

**רצ"ב** העתק מהחווה מיום 15.8.2016 בין נתבעת מס' 1 לגורם שלטוני באיחוד האמירויות הערביות, מסומן ע/6.

21. התובעים יטענו כי לגבי האירועים המתוארים בכתב תביעה זה והמקיס להם עילות תביעה כפי שיפורט בהמשך, נתבעת מס' 1 ונתבעת מס' 2 פעלו כיחידה אחת ובמשותף, וכל פעולה וואו אחריות המיוחסת לאחת מהנתבעות הללו היא גם מיוחסת לנתבעת האחרת.

### **ג. המסכת העובדתית**

#### **מערכת "פגסוס"-PEGASUS**

22. הנתבעות הינן המפתחות והמשווקות של המערכת הידועה בשם "פגסוס"- "Pegasus", שהינה טכנולוגית מעקב ברמה צבאית שלפי פרסומי השיווק של הנתבעות, הטכנולוגיה נמכרת בעיקר לסוכנויות ביון וביטחון ממשלתיות ברחבי העולם.

23. המערכות של הנתבעות, בעיקר "פגסוס", נסמכות על מה שידוע בשפה המקצועית כ- "Zero Day vulnerability", שהיא פרצה בתוכנה של המחשב (ובמקרה של הנתבעות, הטלפון החכם) שאינה ידועה ליצרן המכשיר או התוכנה. פרצות אלו מאפשרות לצד הפורץ גישה למידע הנמצא במכשיר ואף שליטה אקטיבית בכל הפונקציות של המכשיר, כגון הפעלת מצלמה, מיקרופון ועוד.

24. לפי המפרט הטכני של "פגסוס", חלק מהמערכת מוחדר לתוך מכשיר הטלפון החכם של היעד באמצעות שתי שיטות, שיטה ראשונה נקראת "Over the Air Programming- OTA", ושיטה שניה מתבצעת באמצעות שליחת מסר SMS לטלפון של היעד או מערכת מסרונים דומה.

25. הנתבעות אף מציעות שירות שהן מכנות "Enhanced Social Engineering Message" (ESEM) שהוא שירות שעוזר למפעיל המערכת לחבר הודעות טקסט במיוחד בהתאם לתחומי העניין של המטרות, על מנת לדרבן אותן מטרות ללחוץ על הקישור המצורף להודעה, דבר המאפשר התקנת המערכת לתוך הטלפון תוך זמן קצר ביותר וללא ידיעת המטרה. במילותיהן של הנתבעות כפי ששירות זה מתואר במפרט הטכני של "מערכת Pegasus מוצע מבחר רחב של כלים כדי לחבר מסרים תמימים שמעוצבים כדי לגרום למטרה לפתוח את הקישור".

**רצ"ב** העתק המפרט הטכני של מערכת "פגסוס" (בשפה הספרדית והאנגלית), מסומן ע/7.

26. לאחר שהמערכת מוחדרת אל תוך מכשיר היעד, היא מופעלת באופן אוטומטי כדי לנצל פרצות במכשירי הטלפון החכם, והיא מורידה ומתקינה עוד חלקים מהמערכת עד לרמה שבסוף ההתקנה המערכת מצליחה להשתלט על המכשיר מרחוק באופן טוטאלי. כל ההתקנות האלה מתבצעות תוך שניות ומבלי להשאיר סימנים שמערכת הריגול הותקנה בתוך המכשיר.

27. לאחר ההתקנה, ועל פי המפרט הטכני של "פגסוס", המערכת מתחילה מיידית באיסוף נתונים מהמכשיר שהוחדרה לתוכו. לפי המפרט הטכני, הנתונים הללו כוללים את כל המפורט להלן:

- Textual: Textual information includes text messages (SMS), emails, calendar records, called history, instant messaging, contact list, viewing history and much more. Textual information is usually structured and small in size, therefore easier to transmit and analyze.
- Audio: Audio information includes intercepted calls, ambient sounds (microphone recording) and other recorded audio files.
- Visual: Visual information includes instant cameras, photo recovery and screenshots.
- Files: each mobile device contains hundreds of files, some invaluable intelligence bears, such as databases, documents, videos and more.
- Location: tracking device location (Cell-ID and GPS) continues.

=**רצ"ב** איור מס' 4 מהמפרט הטכני הנ"ל, מסומן ע/8.

28. הנתונים שהמערכת פגסוס אוספת מתחלקים לשלושה סוגים:

- א. איסוף ראשוני (Initial Data Extraction)** שמתייחס לנתונים שכבר נמצאים על המכשיר ואלה כוללים, רישומי SMS, פרטי קשר, היסטוריית שיחות, רישומי יומן, מסרי דואר אלקטרוני, מסרונים מידיים והיסטוריית דפדוף באינטרנט.
- ב. איסוף נתונים- ניטור פסיבי (Passive Monitoring)** שמתייחס למעקב אחר נתונים חדשים שהמכשיר אוסף תוך כדי שימוש. אלה כוללים את כל הנתונים של האיסוף הראשוני בנוסף למעקב אחר מיקום בהתבסס על ה-cell ID.
- ג. איסוף אקטיבי (Active Collection)**, והוא מתייחס ליכולת של המפעיל להנחות את המכשיר הנגוע לאסוף נתונים מהמכשיר וסביבתו הקרובה בזמן אמת. המערכת יכולה לאסוף נתונים הקשורים למיקום, הקלטת שיחות טלפון, העברת קבצים, השימוש במיקרופון כמיקרופון חם לאיסוף והעברת קולות מסביבתו של המכשיר, להשתמש במצלמה לצילום הסביבה, והעברת צילומי מסך של המכשיר הנגוע. הנתבעות מתגאות בכך שיכולת האיסוף האקטיבי היא מה שמבדיל בין "פגסוס" וכל תוכנת איסוף מודיעין מתחרה אחרת.



29. בנוסף לאיסוף נתונים כמפורט לעיל, מערכת "פגסוס" יכולה גם לאסוף נתונים מאפליקציות שנמצאות במכשיר שנפרץ. לפי המפרט הטכני, המערכת יכולה לאסוף מידע מרוב האפליקציות בעולם. הנתבעות גם יכולות להתאים את המערכת לאפליקציות חדשות על פי בקשת הגוף הרוכש.

=**רצ"ב** פרטי איסוף הנתונים ואופן האיסוף ופעולות ההסוואה מפורטות בטבלה, מסומן ע/9.

30. הנתונים שהמערכת אוספת מועברים מהמכשיר הנגוע לשרתים. אם ההעברה אינה אפשרית הנתונים נשמרים באופן מוצפן על המכשיר שנפרץ עד שיהיה ניתן לשדר נתונים אלה. שמירת הנתונים נעשית באופן מוצפן ובכל מקרה לא תעלה על 5% מהזיכרון הפנוי כדי לא למשוך תשומת לב הבעלים של המכשיר.

31. העברת הנתונים שנאספו מתבצעת בדרך כלל בזמן אמת. האמצעי המועדף הוא Wi-Fi, אך אפשר גם להעביר נתונים באמצעות הרשתות הסלולריות שתומכות 3G, GPRS ו-LTE. אם למכשיר אין גישה לאינטרנט, המערכת יכולה גם לשלוח נתונים באמצעות SMS. כדי להסוות את שידור הנתונים, המערכת מפסיקה כל פעולת שידור כאשר הסוללה מגיעה ל-5% מיכולת הטעינה וגם כאשר המכשיר הנגוע נמצא במצב נדידה. במצב זה, שידור הנתונים מתבצע אך ורק באמצעות Wi-Fi.

32. חשוב לציין כי התקשורת בין המכשיר שנפרץ והשרת המרכזי נעשית באופן עקיף באמצעות רשת אנונימית כדי למנוע אפשרות של מעקב. כחלק מהשירות, הנתבעות בוטות רשת שידור שנקראת Pegasus Anonymous Transmission Network שהיא רשת מיוחדת לכל לקוח ולקוח. הרשת מורכבת משרתים שנמצאים במספר מקומות בעולם כך שהנתונים משודרים דרך מספר מסלולים לפני שהם מגיעים לשרתי Pegasus מה שמונע את אפשרות גילוי המערכת.

33. העברת הנתונים מהמכשיר שנפרץ אל השרתים הינה מוצפנת באמצעות AES-128 bit symmetric encryption.

34. היכולת לעלות על כך שמכשיר מסוים נפרץ על ידי מערכת "פגסוס" הינה כמעט בלתי אפשרית שכן המערכת מותקנת בתוך המכשיר ברמת ה-kernel, שהיא תוכנת הליבה המנהלת את ה-CPU (Central Processing Unit) של מכשיר הטלפון החכם. הקרנל שולט בזיכרון ב-CPU וכל פעולות המכשיר. מכיוון שמדובר ברמה הבסיסית ביותר, אי אפשר לגלות את מערכת Pegasus באמצעות מערכת anti-virus או anti-malware.

35. לאחר שהנתונים מועברים לשרתים של מערכת Pegasus, המערכת מציעה מבחר של כלים המאפשרים עיון, מיון, סינון וניתוח הנתונים שנאספו מהמכשיר. המערכת מאפשרת מעקב גיאוגרפי (הן בזמן אמת והן על בסיס מידע היסטורי) כך שכל תנועותיו של המטרה/היעד מוצגות על מפה שהמפעיל יכול לצפות בה. כמו כן, אפשר לעקוב אחר מספר מטרות באותו זמן, ולמיין את המטרות לפי קבוצות. אפשר גם לעשות חיפוש בנתונים כדי לחפש שמות, מספרים או מילות מפתח. כמוכן, המפעילים יכולים לעשות ניתוח של פעולות ותנועות המטרה/היעד על ציר הזמן,

ולהנחות את המערכת למסור התראות על התרחשות אירועים מסוימים כגון קבלת שיחות או הימצאות במקום מסוים. כל הנתונים מוצגים באמצעות ממשק נוח לשימוש וצפיה.

36. כאשר המפעיל מחליט כי אין עוד צורך בריגול אחרי המטרה/היעד, המפעיל יכול להסיר מרחוק את המערכת מהמכשיר שנפרץ. ההסרה נעשית מרחוק ומבלי ידיעת בעל המכשיר או המחזיק בו. במקרים מסוימים המערכת גם יכולה לבצע השמדה עצמית כדי למנוע את גילוייה. בשני המקרים, כאשר חלק זה מהמערכת מוסר מהמכשיר, הנתבעות מציינות במפרט הטכני כי המערכת לא משאירה שום סימן לכך שהמכשיר היה פרוץ באמצעות מערכת Pegasus.

37. כפי שעולה מהמפרט הטכני ומהחווה, מעורבותן של הנתבעות אינה מסתיימת עם מכירת המערכת לגוף המפעיל. הנתבעות מציעות ומספקות גם שירותי תחזוקה, תמיכה, ועדכון/שדרוג לטובת המפעיל. למעשה, הנתבעות מעורבות באופן אקטיבי בפעולות הריגול שהמפעיל מבצע במכשירים שנפרצו.

38. לפי המפרט הטכני, הנתבעות מציעות ומספקות שלוש רמות של תחזוקה ותמיכה. **ברמה הראשונה**, הנתבעות מספקות תמיכה טכנית באמצעות דואר אלקטרוני וגם שיחות טלפוניות. **ברמה השנייה**, הנתבעות מספקות תחזוקה ותמיכה ברמה יותר פרואקטיבית: מהנדסי הנתבעות בוחנים את המערכת ופותרים מרחוק את הבעיות הטכניות שמתגלות באמצעות "תוכנת שולחן עבודה מרחוק ורשת פרטית וירטואלית (remote desktop software and a Virtual Private Network VPN)". **ברמה השלישית**, עבודות התחזוקה שהנתבעות מספקות כוללות תיקון כשלונות של המערכת ושדרוגה.

39. לא זו אף זו, הנתבעות גם מציעות ומספקות תמיכה באתר של המפעיל (בין אם משרד מתוכנן מראש או אתר חירום), וגם השגחה על "בריאות" המערכת ותקינותה.

40. בנוסף לרמת התמיכה הגבוהה שהנתבעות מספקות, הן גם מספקות שדרוג למערכת מספר פעמים בשנה. השדרוגים כוללים פונקציות חדשות שהמערכת יכולה לספק, שדרוגים המאפשרים פריצת מכשירים או תוכנות הפעלה חדשות שהמערכת לא יכלה לפרוץ עד כה, ותכונות המותאמות לצרכים של המפעיל ותיקון באגים המתגלים במהלך הפעלת המערכת.

41. הנתבעות, וכפי שעולה ממסמכי ההתקשרות עם גורמי הממשל המקסיקנים, סיפקו גם, לפי המפרט הטכני, שירותי הדרכה למפעילים המקסיקנים בנוסף לשירותי (configuration) של המערכת.

42. התובעים יטענו כי כל הפעולות האלה של תמיכה, שדרוג ותחזוקה מעידות על מעורבות מרכזית מתמשכת בפעולות של המפעילים לאחר מכירת המערכת אליהם, כך שכל אי חוקיות שדבקה בפעולותיו של המפעיל אפשר גם לייחס אותה לנתבעות במידה שווה כשותפות שמידת תרומתן הינה מרעית.



## התקשרות הנתבעות עם גורמי ממשל במקסיקו

43. לפי החוזה שנחתם ביום 16.10.2014, רכש משרד התובע הכללי במקסיקו, הידוע כ-PGR, את מערכת "פגסוס" מהחברה המקסיקנית GRUPO TECH BULL, SA DE CV תמורת 32,016,000 דולר ארבי"ב (32 מיליון דולר). החברה המקסיקנית התאגדה רק כשנה אחת לפני ביצוע העסקה (10.10.2013), ועל פי פרסומים בעיתון El Universal, שהוא אחד העיתונים המובילים במקסיקו, היא אינה ידועה בתחום הסייבר או הביטחון.

=**רצ"ב** כתבה בעיתון El Universal, מסומן ע/10.

44. העובדה שמשרד התובע הכללי המקסיקני בחר להתקשר עם חברה כה צעירה וחסרת ניסיון מוכח בתחום רגיש ומסובך גורמת להרמת גבה, במיוחד כי עד לשבוע ימים לפני שהחברה התקשרה בחוזה, לבעלים הרשום והמנהל היחיד לא היה ניסיון עסקי כלשהו.

45. הסברה הרווחת היא ש- GRUPO TECH BULL הינה חברת קש שבבעלותה ושליטתה של חברת Balam Seguridad Privada שאף היא חברה חדשה יחסית (נוסדה בשנת 2012) ומתמחה בענייני ביטחון וטכנולוגיה. כך מסר אחד ממנהלי GRUPO TECH BULL, מר Luis Armando Perez Herrero, שחתם על החוזה עם משרד התובע הכללי מטעם GRUPO TECH BULL, באחד מהודעות הדואר אלקטרוני לחברת Hacking Team, שהודלפו ל-Wikileaks.

=**רצ"ב** הודעת דואר אלקטרוני ממר Luis Armando Perez Herrero, מסומן ע/11.

46. כפי שפורסם בעיתון El Universal, הסיבה להסוואת הבעלות והשליטה בחברת GRUPO TECH BULL היא שהבעלים האמיתיים, Balam Seguridad Privada, ידועה בקשריה ההדוקים עם גורמי ממשל במקסיקו. אחד השותפים הבכירים ב-Balam Seguridad Privada, מר Rodrigo Ruiz de Teresa Treviño, הינו אחיינו של מר Guillermo Ruiz de Teresa, המתאם הכללי של מחלקת הנמלים והמרינות המסחריות במשרד התקשורת והתחבורה, והאיש החזק במפלגת ה-PRI, אותה מפלגה שהייתה בשלטון במשך שנים רבות ושהנשיא היוצא נבחר לנשיאות מטעמה.

47. יצויין כי מספר גורמים בממשל הפדרלי במקסיקו הודו כי מקסיקו רכשה את מערכת "פגסוס". על פי דיווח בניו יורק טיימס, הנשיא (היוצא) אנריקה פנה נייתו עצמו הודה כי ממשלתו רכשה את המערכת. כמו-כן, ביום 18.5.2018 הודה משרד התובע הכללי של מקסיקו בפני שופט פדרלי במסגרת הליך פלילי כי המשרד רכש רישיון שימוש במערכת "פגסוס".

48. עוד יצויין כי הנתבעות מעולם לא הכחישו את קיום ההתקשרות החוזית למכירת המערכת במקסיקו.

**סירוב הנתבעות לשתף פעולה עם חקירה פלילית בעניין הפריצות**

49. לאחר שפריצות באמצעות מערכת "פגסוס" נתגלו, נפתחה במקסיקו חקירה פלילית בעניין. באוקטובר 2017, פנו רשויות החקירה במקסיקו, באמצעות משרד החוץ בישראל, לקבלת עזרה בחקירה על ידי הפניית שאלון לנתבעת מס' 1 בהתייחס לקשר בינה לבין הרשויות במקסיקו. למרות פניות חוזרות בנובמבר 2017 והן במרץ 2018 מצד שגרירות מקסיקו בישראל, לא נתקבלה שום תשובה לבקשה. הנתבעת מס' 1 לא שיתפה פעולה וכיום, 10 חודשים לאחר הפנייה, היא עדיין מסרבת לשתף פעולה.

### פירוט הפגיעות בכל אחד מהנתבעים

#### התובע מס' 1

50. מתוקף תפקידו כמנהל ארגון זכויות צרכן ובריאות ציבורית (El Poder del Consumidor), התובע מס' 1 תמך ושיחק תפקיד פעיל בקידום הטלת מס על משקאות מוגזים ומשקאות עתירי סוכר. התובע מס' 1 מתח ביקורת על ההשפעה הגוברת של חברות המזון והמשקאות על ממשלת מקסיקו. בדיוק שבוע לאחר שהופיע במסיבת עיתונאים לתמיכה בהעלאת המס על משקאות סודה, התובע מס' 1, ואחרים המעורבים באותו נושא (קבוצה שכוללת בין השאר פעילים בתחום הבריאות ומומחים בעלי שם בתחום), החלו לקבל הודעות טקסט שכללו קישורים המובילים לתשתית מערכת הרוגלה של "פגסוס". באותה עת, התובע מס' 1 היה מעורב בקמפיין לאימוץ סטנדרטים גבוהים יותר של תיוג מוצרים אלה וזאת במטרה להגברת המודעות לגבי הסכנות בצריכת מוצרים אלה.

51. ביום 8 יולי 2016 קיבל התובע מס' 1 מסרון SMS שתוכנו כלהלן: "Alejandro perdon pero acaba de fallecer mi padre, estamos mal, t envio los datos del velatorio, espero asistas: hxxp://bit.ly/29xpUI0 ובתרגום לעברית המסרון אומר "אליחנדרו אני מצטרער אבל אבי נפטר, אנחנו במצב רע, שלחתי לך את תאריכי ה-wake [טקס שנעשה לפני או מייד אחרי הלוויה], אני מקווה שתבוא: http://bit.ly/29xpUI0"

52. הקישור הקצר במסרון (<http://bit.ly/29xpUI0>) מפנה לקישור אחר שהוא הקישור האמיתי (<https://smsmensaje.mx/91584s>) שמפנה לדומיינים (domains) המזוהים עם הנתבעות.

53. ככל הנראה הנסיון הראשון לא צלח, וביום ה-11 ביולי 2016 הנתבע מס' 1 קיבל עוד מסרון SMS כלהלן: "Alejandro buen dia, te envio esta nota de proceso donde hacen mencion de tu nombre, se esta viralizando mira: http://bit.ly/29COxD2" ובתרגום לעברית המסרון אומר "אליחנדרו יום טוב, אני שולח לך כתבה שבה הם מזכירים את שמך, זה נראה ויראלי": "<http://bit.ly/29COxD2>"

54. גם במסרון השני הקישור הקצר מפנה לקישור אחר (<https://smsmensaje.mx/5062299s/>) שמפנה לדומיינים המזוהים עם הנתבעות.



55. עם משלוח מסרונים אלה, מכשיר הטלפון החכם של התובע מס' 1 נפרץ והוחדרה לתוכו מערכת "פגסוס" דבר שהביא לפגיעה בזכויותיו ובפרטיותו, כתוצאה מפגיעה זו נגרם נזק לתובע מס' 1 כמפורט בהמשך התביעה.

### התובעים מס' 2 ו-3

56. בנובמבר 2014, התובעים מס' 2 ו-3, ביחד עם עיתונאים מאתר החדשות "Aristegui Noticias" (שגם הם היו קורבנות של ניסונות פריצה באמצעות מערכת "פגסוס") פירסמו כתבה שחשפה פרשת השחיתות מהגדלות בתולדות מקסיקו, הידועה בשם "Casa Blanca". הכתבה תיעדה איך הבית שבאותו עת התגורר בו הנשיא היוצא אנריקה פנה נייתו ביחד עם בני משפחתו, וששוויו כ-7 מיליון דולר, נרכש בנסיבות שמעוררות חשד לקבלת שוחד וואו טובות הנאה. הבית נרכש מקבלן שהוא והחברות שלו קיבלו חוזים בשווי מיליונים כאשר הנשיא אנריקה פנה נייתו היה מושל מדינת מקסיקו.

=**רצ"ב** העתק מהתחקיר על פרשת "הבית הלבן", מסומן ע/12.

57. באותו עת, התובעים מס' 2 ו-3 היו חלק מהיחידה לתחקירים מיוחדים של ארגון התקשורת היוקרתי "Noticias MVS Primera Emisión". פרשת הבית הלבן התפרסמה תחילה באתר Aristegui Noticias ובכלי תקשורת אחרים לרבות כלי תקשורת בינלאומיים. העיתונאית הידועה קרמן אריסטיגוי, נטלה חלק בחשיפת הפרשה (שגם היא הייתה קורבן להתקפה באמצעות "פגסוס") ובזמנו אירחה תוכנית בתחנת Noticias MVS Primera Emisión. למרות מעורבותה של קרמן אריסטיגוי בתחקיר, התחנה ביקשה ממנה לא לפרסם את הפרשה. חודשיים לאחר מכן, במרץ 2015, התובעים 2 ו-3 וקרמן אריסטיגוי פותרו מ-MVS. צעד זה נחשב לנסיון להשתקת קרמן אריסטיגוי והצוות שלה (לרבות התובעים 2 ו-3) ביחס לעבודתם.

58. בנוסף לחשיפת פרשת הבית הלבן, הצוות תיעד פרשות שחיתות אחרות שפגעו במוניטין של ממשלת מקסיקו ושזכו לחשיפה גבוהה. פרשות אלה כללו בין השאר חשיפת רשת זנות שפעלה ממשרדי מפלגת השלטון אז "PRI" (מפלגתו של פנה נייתו) במקסיקו סיטי וסיקור נרחב של פרשת ההיעלמות בכפייה ההמונית באיגואלה משנת 2014.

59. בנוסף לכך, בשנת 2015, אלמונים פרצו למשרדים של קרמן אריסטיגוי והצוות שלה. למרות הפריצה, לא נגנבו חפצים בעלי ערך, ואירוע זה נחשב לניסיון התנכלות והפחדה. זהו ההקשר הרחב והכללי יותר לאורו יש לבחון את ניסיונות הפריצה באמצעות מערכת "פגסוס" כנגד התובעים מס' 2 ו-3 ונגד קרמן אריסטיגוי ובנה שהיה קטין דאז.

60. ביום 12 למאי 2016, קיבל התובע מס' 2 את הודעת הטקסט שלהלן: "Tengo pruebas clave y fidedignas en contra de servidores publicos, ayudame tiene que ver con este "asunto http://bit.ly/1s2eguc ובתרגום לעברית: "יש לי ראיות מפתח ואמינות נגד עובדי ציבור, עזור לי במה לעשות עם העניין הזה: http://bit.ly/1s2eguc"

61. הקישור הקצר (<http://bit.ly/1s2eguc>) מפנה לקישור אחר שהוא הקישור האמיתי (<https://secure-access10.mx/2618844s/>), שמפנה לדומיינים (domains) המזוהים עם הנתבעות.

62. הודעה זו הייתה מותאמת באופן אישי לתובע מס' 2, שכן היא נופלת בתחום העבודה וההתעניינות שלו בתור עיתוניאי שמתמחה בענייני שחיתות.

63. כתוצאה מניסיונות אלה, מכשיר הטלפון החכם של התובע מס' 2 נפרץ והוחדרה לתוכו מערכת "פגסוס", דבר שהביא לפגיעה בזכויותיו ופרטיותו. כתוצאה מפגיעה זו נגרם נזק לתובע מס' 2.

64. התובע מס' 3 נפל קורבן למערכת Pegasus לאחר שבעה נסיונות. הניסיון הראשון היה ביום 18 במאי 2018. באותו יום נשלחה לתובע 3 הודעה כלהלן: "TELCEL.COM/ EL SIGUIENTE MENSAJE SE HA MARCADO COMO URGENTE Y NO SE RECIBIO , http://bit.ly/1NzkyeZ : COMPLETAMENTE RECUPERELO EN TELCEL.COM/ THE FOLLOWING MESSAGE HAS BEEN MARKED AS URGENT AND WAS NOT COMPLETELY RECEIVED. RECOVER IT (AT: http://bit.ly/1Nzkye )". הקישור הפנה לקישור האמיתי (<https://smsmensaje.mx/8435662s>) שמפנה לדומיינים (domains) המזוהים עם הנתבעות.

65. יום למחרת, 19.5.2106, התובע מס' 3 קיבל הודעה נוספת: "TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE \$8,854.90 M/N VERIFIQUE DETALLES: https://ideas-telcel.com.mx/3975827s , ובאנגלית "TELCEL.COM/ DEAR USER WE REMIND YOU THAT YOU OWE \$8,854.90 " https://ideas-telcel.com.mx/3975827s VERIFY THE DETAILS". קישור זה מפנה לדומיינים (domains) המזוהים עם הנתבעות.

66. ביום 20.5.2016 נעשה עוד ניסיון כאשר התובע מס' 3 קיבל את ההודעה: "Facebook reporta intentos de acceso a la cuenta: Rafa Cabrera. Evite bloqueo de cuenta, verifique en: Facebook reports an attempt to access " https://fb-accounts.com/2408931s , ובאנגלית: "your account: Rafa Cabrera. Avoid the blocking of your account, verify in: https://fb-accounts.com/2408931s". קישור זה מפנה לדומיינים (domains) המזוהים עם הנתבעות.

67. ניסיון נוסף נעשה ביום 23.5.2016. התובע מס' 3 קיבל הודעה " UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. UNOTV.COM/ /DETALLES: https://unonoticias.net/1867745s , ובאנגלית " CARMEN ARISTEGUI COULD RUN AS AN INDEPENDENT CANDIDATE IN 2018. DETAILS: https://unonoticias.net/1867745s ". קישור זה מפנה לדומיינים (domains) המזוהים עם הנתבעות.

68. המפעילים של מערכת "פגסוס" לא ויתרו והם שינו טקטיקה והתחילו לשלוח אליו הודעות מקוממות. כך שביום 24.5.2016, התובע מס' 3 קיבל את ההודעה הבאה: "No tienes los



huevos de ver como me fajo a tu pareja. Mira nada mas como co\*\*\*\*s bn rico y en tu You don't have the balls to watch how " ובתרגום לאנגלית "http://bit.ly/246dkRy cama: http://bit.ly/246dkRy I make out with your partner. Look how we f\*\*k so good and in your bed: http://bit.ly/246dkRy הפנה לקישור האמיתי (http://bit.ly/246dkRy) http://bit.ly/246dkRy שםפנה לדומיינים (domains) המזוהים עם הנתבעות. (https://smsmensaje.mx/4667624s/)

69. שטף ההודעות לא פסק, וביום 30.5.2016, התובע מס' 3 קיבל שתי הודעות. הראשונה הייתה: UNOTV.COM/ PRESIDENCIA DEMANDARA POR DIFAMACION A " QUIENES PUBLICARON REPORTAJE DE LA CASA BLANCA. UNOTV.COM/ THE PRESIDENCY " ובאנגלית "NOTA: http://bit.ly/1hMG15k WILL SUE FOR DEFAMATION AGAINST THE PUBLISHERS OF THE CASA BLANCA REPORT http://bit.ly/1hMG15k הקצור (http://bit.ly/1hMG15k) הפנה לקישור האמיתי (http://fb-accounts.com/1074139s) שםפנה לדומיינים (domains) המזוהים עם הנתבעות.

70. ההודעה השנייה שנשלחה לתובע מס' 3 באותו יום כללה איומים במאסר ונקטה בזו הלשון: UNOTV.COM/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRIA " ENCARCELAR REPORTEROS MIENTRAS INVESTIGA VER NOMBRES: [ lin UNOTV.COM/ BECAUSE OF THE CASA " ובאנגלית: "http://bit.ly/1LLY8oK BLANCA ISSUE THE PRESIDENCY COULD INCARCERATE REPORTERS WHILE IT INVESTIGATES SEE NAMES: http://bit.ly/1LLY8oK הקצור (http://bit.ly/1LLY8oK) הפנה לקישור האמיתי (http://unonoticias.net/3423768s) שםפנה לדומיינים (domains) המזוהים עם הנתבעות.

71. ניסיונות הפריצה באמצעות הודעות מאיימות הללו היו אישיות וכוונו לתובע באופו ספיציפי שכן היוו חלק מתופעת הפגיעה בעיתונאים במקסיקו. למשל, על פי נתוני הארגון Article 19, בין השנים 2012 ו-2018 (שנות כהונתו של הנשיא אנריקה פנה נייתו), נהרגו במקסיקו כ-40 עיתונאים. חלק גדול מההטרדות נגד העיתונאים נעשה על ידי זרועות המדינה, במיוחד כאשר מדובר בעיתונאים המתמחים בזכויות אדם ונשאים הקשורים בשחיתות שלטונית.

=רצ"ב תדפיס מאתר הארגון Article 19, מסומן ע/13.

#### התובעים מס' 4-5

72. התובעים מס' 4 ו-5, עורכי דין המתמחים בזכויות אדם והם בהתאמה המנהל והסגן של ארגון זכויות אדם Centro Prodh, שמתעסק בפרשות הפרת זכויות אדם בעלות פרופיל גבוהה והחמורות והרגישות ביותר במקסיקו. השנים, ביחד עם אחרים במכרז, נפלו קורבן לניסיונות פריצת מכשירי הטלפון החכם שלהם באמצעות מערכת Pegasus, וזאת על רקע מעורבותם האקטיבית והאנטנסיבית בחקירת המקרה של "ההיעלמות בכפייה ההמונית באיגואאלא" של 43 סטודנטים בעיירה Ayotzinapa משנת 2014, והוצאה להורג ללא משפט של אזרחים על ידי



הצבא המקסיקני בעיירה Tlatlaya במדינת מקסיקו, וייצוג הקורבנות בפרשת עינויים מיניים בעיירה Anteco San Salvador בפני בית הדין האינטר-אמריקאי לזכויות אדם. חשוב לציין כי ישנן ראיות חזקות הקושרות פקידי ממשל לפרשות חמורות אלה. המדובר בעניינים רגישים הנוגעים באופן ישיר במוניטין ובאינטרסים של הממשל הנוכחי במקסיקו.

73. ביום 20.4.2016, קיבל התובע מס' 4 את ההודעה: " EL GOBIERNO DE MEXICO THE GOVERNMENT OF " ובאנגלית "10MADRUGA AL GIEI: <http://bit.ly/20Y9r> "10MEXICO TAKES GIEI OFF GUARD: <http://bit.ly/20Y9r> הקצור (https://secure-access10.mx/4257391s/ http://bit.ly/20Y9r10) הפנה לקישור האמיתי שםפנה לדומיינים (domains) המזוהים עם הנתבעות.

74. עם משלוח מסרים אלה, מכשיר הטלפון החכם של התובע מס' 4 נפרץ באמצעות מערכת Pegasus ובכך נפגעו זכויותיו ופרטיותו. כתוצאה מפגיעה זו נגרם נזק לתובע מס' 4.

75. גם כאן אפשר לראות ששולחי ההודעות דאגו לכתובת מסרון שהותאם במיוחד עבור התובע מס' 4 כדי לדרבן אותו ללחוץ על הקישור. GIEI היא קבוצת מומחים עצמאית ובינתחומית שנתמנתה על ידי ה-Inter-American Commission on Human Rights כדי לספק סיוע טכני בחקירת "ההיעלמות בכפייה ההמוניות באיגואאלא". מתוקף עבודתו, התובע מס' 4 היה מטבע הדברים מעוניין בכל מה שקשור לקבוצה. יצוין כי למרות שקבוצת המומחים הגיעה למקסיקו על פי בקשת ממשלת מקסיקו שהבטיחה לחבריה חסינות דיפלומטית, חברי הקבוצה, גם הם, נפלו קורבן לפריצת מכשירי הטלפון באמצעות מערכת "פגסוס".

=**רצ"ב** דו"ח ארגון **Citizen Lab** שמתייחס לפריצת מכשירי חברי **GIEI**, מסומן ע/14.

76. ביום 20.5.2016, קיבל התובע מס' 5 את ההודעה הבאה: " SrJorge soy Juan Magarino ayuda con mi hermano Heriberto se lo llevo la policia por ser maestro es un delito Mr Jorge I'm Juan Magarino please help with my brother Heriberto, the police took him for being a teacher this is a crime : http://bit.ly/1XFaS4F " ובאנגלית "http://bit.ly/1XFaS4F". הקישור הקצר (http://bit.ly/1XFaS4F) הפנה לקישור האמיתי (https://network190.com/8361397s) שםפנה לדומיינים (domains) המזוהים עם הנתבעות. גם כאן אפשר לראות שההודעה נכתבה בכוונה לעורר את העניין של עורך דין זכויות אדם המתמחה בנושא היעלמות בכפייה.

77. ביום 8.6.2016 המפעילים שינו טקטיקה והחליטו לקרוץ לצדו האקדמי של התובע מס' 5 שהינו גם מרצה באוניברסיטה. ההודעה הפעם הייתה: " Mtro, tuve un incidente, le envio nuevamente mi tesis, basada en su tesina para que me de su comentarios Professor, I had a problem, I am resending my thesis, based in your dissertation so you can give me comments: http://bit.ly/292heXd " ובאנגלית: "http://bit.ly/292heXd". הקישור הקצר (http://bit.ly/292heXd) הפנה לקישור האמיתי (https://network190.com/2066781s) שםפנה לדומיינים (domains) המזוהים עם הנתבעות.



78. ביום 28.6.2016, התובע מס' 5 קיבל הודעה דומה שמתייחסת לכאורה לעבודתו האקדמית של התובע. טקסט ההודעה היה " Buen día Mtro. trabajo en mi tesis, tome como base su "tesina, me interesa su opinion, le mando los adelantos : <http://bit.ly/1U0yzVG> , ובאנגלית: " Good day professor, I'm working in my thesis, I took your dissertation as a base, I'm interested in your opinion, I am sending you an advanced copy : <http://bit.ly/1U0yzVG> ". הקישור הקצר (<http://bit.ly/1U0yzVG>) הפנה לקישור האמיתי (<https://network190.com/6214010s/>) שמפנה לדומיינים (domains) המזוהים עם הנתבעות.

79. ניסיון זה צלח, ומכשיר הטלפון החכם של התובע מס' 5 נפרץ באמצעות מערכת "פגסוס" ובכך נפגעו זכויותיו והפרה פרטיותו. כתוצאה מפגיעה זו נגרם נזק לתובע מס' 5.

#### **דפוסי הפעילות והשיווק של הנתבעות וחברות קשורות**

80. על אף שהנתבעות והחברות שבבעלותן או חברות הקשורות בהן עוסקות בתחום רגיש במיוחד ועוסקות בפיתוח טכנולוגיה מסוכנת בעלת יכולת לפגוע בזכות לפרטיות של ציבורים בלתי מוגבלים באורח קשה ביותר, הנתבעות והחברות הקשורות שחלקן הוזכר למעלה אימצו דפוסי התנהגות שהפכו לתרבות ארגונית המאופיינת בהפגנת זלזול בזכויותיהם של אחרים ובראשונה הזכות לפרטיות. התנהגות הנתבעות והחברות הקשורות לא משאירה ספקות כי הן מעודדות באופן אקטיבי הפרות בוטות של זכויות אדם, הכל במטרה לשווק את המערכת ובכך להשיג רווח כלכלי גדול יותר.

81. להמחשת הטענה, נביא להלן דוגמא טובה להתנהגות כזו המלמדת על תרבות המזלזלת בזכות לפרטיות ועל נקיטת אמצעים פסולים במטרה לשווק את המערכת ללקוחות פוטנציאליים. כך במהלך שנת 2014 מנהל בחברת Circles Technologies הרשומה בקפריסין, שהיא כאמור בבעלות מלאה של חברת האם של הנתבעות OSY Technologies, ניסה לשדל את הגופים השלטוניים של מדינת איחוד האמירויות הערביות לרכוש מערכת ריגול מהתוצרת של החברה.

82. מהתכתבויות בדואר אלקטרוני בין אריק באנון, מנהל בCircles Technologies, לבין אחמד עלי אל-חבסי מהמועצה הלאומית לביטחון לאומי באיחוד, מר אל-חבסי ביקש ממר באנון הוכחה "חיה" על היכולת של המערכת המשווקת באמצעות פריצת וריגול אחרי מספרי טלפון שמר אל-חבסי סיפק למר בנון. בהודעת דואר אלקטרוני מיום 6.8.2014 בשעה 15:08 מאחמד עלי אל-חבסי אל אריק באנון נשלחו 4 מספרי טלפונים לצורך ניסוי המערכת לפני רכישתה.

83. נציגי Circles Technologies עטו על ההזדמנות ובלי היסוס ניסו לספק את הסחורה על ידי פריצת מכשירים אלה! והנתונים שהחברה השיגה כמעוול ראשי נשלחו למר אל-חבסי. התנהגות זו מלמדת בהכרח כי המערכת הוחדרה למכשירי היעד ובכך התאפשר ריגול אחרי בעליהם. מדובר בדוגמא אחת המוכיחה כי הנתבעות אינן ספקיות של המערכת בלבד, כפי שהיחצנים שלהן ניסו לתרץ תפקידן לאחר חשיפת המקרה של התובעים בתקשורת ברחבי העולם, אלא מדובר במעוולות ראשיות יחד עם הגוף המפעיל המזמין את המערכת.

=רצ"ב העתק התכתבות דואר אלקטרוני מהימים 6.8.2014 ו-10.8.2014 באחמד עלי אל-חבסי לבין אריק באנון ומירוסלב פטריקוב מ-Circles Technologies, מסומן ע/15.

84. סביר להניח כי שיטה שיווקית זו אף שימשה הנתבעות להוכחת האפקטיביות של המערכת שעה שמכרו אותה לגורמי הממשל במקסיקו תמורת 32 מליון דולרים! הרי לא יעלה על הדעת כי גורמי הממשל במקסיקו ישלמו הון עתק תמורת המערכת מבלי אף לבדוק יעילותה!

85. כאן המקום לציין גם כי הדוגמא הזו מעלה כי קיים נדבך חשוב נוסף מהשימוש הנעשה במערכת שהנתבעות מספקות. שימוש זה הינו מסוכן כיוון שביכולתו לפגוע בריבונות של מדינות אחרות ונתיניהן.

86. דוגמה נוספת לאדישות הנתבעות כלפי הקורבנות שלה ותרבות הארגונית שלא מתחשבת כלל בזכויות אדם היא המקרה של אחמד מנסור, פעיל זכויות האדם ותושב איחוד האמירויות. על פי דו"ח ארגון Citizen Lab, בשנת 2016, היה נסיון לפרוץ למכשיר הטלפון של מר מנסור, ככל הנראה על ידי שירותי בטחון של האיחוד. מר מנסור נעצר ובחודש מאי 2018 הוא נשפט לעשר שנות מעצר בגלל פוסטים ב-Facebook. מעצרו ומשפטו של מר מנסור סוקרו היטב על ידי ארגוני זכויות אדם בינלאומיים ואף גונו על ידי מומחי זכויות אדם באו"ם.

<https://www.amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/>

<https://www.hrw.org/news/2018/04/09/uae-one-year-award-winning-human-rights-defender-ahmed-mansoor-whereabouts-remain>

<https://www.bbc.co.uk/news/world-middle-east-39416734>

<https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21449&LangID=E>

87. לאחרונה, ארגון זכויות האדם Amnesty International הודיע כי היה ניסיון פריצה למכשיר הטלפון השייך לאחד מעובדיו באמצעות מערכת "פגסוס". הפיתוי הפעם היה ידיעה בערבית על הפגנה נגד כליאת פעילים בערב הסעודית. באותה תקופה פעילים סעודים שנמצאים מחוץ לסעודיה קיבלו הודעות דומות עם קישורים לאתרים שהם חלק מתשתית "פגסוס", מה שמוביל למסקנה שהמערכת גם נמכרה לגורמי אכיפה בערב הסעודית שמשתמשים בה נגד פעילי זכויות אדם ופעילי אופוזיציה.

=רצ"ב דוח של אגון אמנסטי שהתפרסם בחודש אוגוסט 2018, מסומן ע/16.

88. מקרים אלה מוכיחים שמערכת "פגסוס" נמכרת לכל מדינה ומשטר הנמצאים בקשרים תקינים עם ישראל - גם אם קשרים אלה אינם גלויים - ויש להם את האמצעים לשלם עבור מערכת זו (שעלותה בין 50,000-65,000 דולר לכל פריצה) ללא כל קשר למצב זכויות האדם במדינות אלה וללא נקיטת אמצעי זהירות כלשהם בהעברת העמרכת.



## ד. עילות התביעה

89. התובעים יטענו, כי במכירת מערכת "פגסוס" אל גורמי ממשל במקסיקו כפי שהוכח לעיל, ובמתן וסיפוק שירותים נלווים אחרים לאחר מכן כפי שפורט לעיל וכמתחייב מההסכם ומהמפרט הטכני הנלווה אליו, הנתבעות פגעו בפרטיותם של התובעים, במישרין, בעקיפין, במעשה או במחדל, ובהתרשלות, ולתובעים עומדים עילות תביעה שונות כנגד הנתבעות כדלקמן:

### **עולה אזרחית בגין פגיעה בפרטיות**

90. התובעים יטענו, כי הנתבעות אשר מכרו מערכת "פגסוס" אל גורמי ממשל במקסיקו והמשיכו לספק להם שירותים נלווים בהפעלת המערכת ובהחזקתה, פגעו פגיעה חמורה בפרטיותם של התובעים ללא הסכמתם.

91. הפגיעה בפרטיותם של התובעים הינה ברף החמור ביותר וזאת נוכח מידת החשיפה הרבה שמאפשרת מערכת "פגסוס" במכשיר המוחדרת אליו ושנגדו מנוהל המעקב. באמצעות המערכת הזו, הנתבעות יכלו לעקוב אחר הנעשה במכשירים הניידים של התובעים בזמן אמת, ואף להפעיל מעקב באופן אקטיבי כפי שהמערכת מאפשרת. מדובר במערכת מסוכנת ביותר וטמון בה פוטנציאל אדיר של יכולת מעקב בלתי מוגבלת אחר חייהם הפרטיים של אנשים נורמטיביים כדוגמת התובעים מתוך מטרות ומניעים פוליטיים בראש ובראשונה.

92. אין להכביר במלים באשר למידת הפגיעה בזכותם של התובעים לפרטיות נוכח הפעלת המערכת נגדם שכן כל בר דעת יכול לדמיין בראשו את אופיו וטיבו של המעקב שניתן היה לבצע נגדם באמצעות המערכת בזמן אמת.

93. התובעים יטענו כי הנתבעות פגעו בפרטיותם בשני מישורים עקרוניים, הכל כפי שיפורט להלן:

**המישור הראשון**, הפרת הפרטיות נעשתה על ידי הנתבעות באופן ישיר ו/או כמעוולות במשותף כלפי התובעים עם גורמי ממשל במקסיקו, ובקשר לחלק מהשירותים. אשר על כן בית המשפט הנכבד מתבקש להטיל על הנתבעות אחריות בגין הפרת החובות המוגנות מפורשות בחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות").

**המישור השני**, הפרת הפרטיות נעשתה על ידי ובאמצעות לקוחות של הנתבעות אשר עושים שימוש בשירותים אותם מספקות הנתבעות, ומשכך חייבות הנתבעות בגין פעילותיהן העקיפות, מכוח אחריותן לפי חוק הגנת הפרטיות ומכוח דוקטרינת ההפרה התורמת. השירותים שהנתבעות מספקות, שכוללים החזקת המערכת ושדרוגה ומתן תמיכה טכנית באופן מתמשך ברמות שונות, כפי שפורט לעיל, איפשרו לגורמי ממשל במקסיקו לבצע מעקב אחרי התובעים. יצויין, אילולא התרומה המכרעת של הנתבעות לביצוע המעקב, פעולות הריגול כנגד התובעים לא היו מבוצעות! מדובר בתרומה מכרעת ואף הכרחית שבלעדיה המעקב לא היה יוצא לפועל. הקשר הסיבתי בין פעילות הנתבעות (ומחדליהן) לבין הנזק הינו חזק וברור. הנתבעות אינן יכולות להסתתר מאחורי הטענה כי במכירת המערכת הן סיימו את

חלקן וכי עיקר האחריות רובץ על גורמי הממשל של מקסיקו. זוהי טענה שקרית אשר סותרת את האמור במפרט הטכני ונועדה להעביר את האחריות מכתפי הנתבעות.

94. מהתשתית העובדתית כמפורט לעיל עולה כי הוכחו יסודותיה של דוקטרינת ההפרה התורמת: ראשית, התובעים יטענו כי פרטיותם, כאמור בחוק הגנת הפרטיות, נפגעה על ידי שימוש שעשו גורמי ממשל במקסיקו במערכת שהנתבעות ייצרו ובשירותים אותם הנתבעות מספקות כולל החזקה ושדרוג ומתן תמיכה טכנית. השימוש שעשו גורמי ממשל במקסיקו במערכת שיצרו הנתבעות ובשירותים הנלווים לצורך הפעלתה, הוא זה שהביא לפגיעה בפרטיותם של התובעים במובנו של חוק הגנת הפרטיות. למעשה, לא תתכן כלל מחלוקת באשר לפגיעה בפרטיותם של התובעים כתוצאה מהשימוש שנעשה במערכת נגדם. שנית, הנתבעות הן הספקיות של המערכת והשירותים, תורמים ומעודדים ביודעין את הפרת הזכות לפרטיות על ידי המפרים הראשיים-גורמי הממשל במקסיקו במקרה דנן. לנתבעות ישנה ידיעה ממשית על הסיכון הצפוי בשימוש בשירותים אותן הן מספקות שכן המערכת מיוצרת אך ורק לשם ריגול. פיקוחו של משרד הביטחון על פעולות השיווק של המערכת הוא עוד הוכחה על ידיעת הנתבעות לטיב המוצר שהן פיתחו. זוהי גם הסיבה שהנתבעות דואגות להבהיר כי הן אינן בעלות אחריות לשימוש הנעשה במערכת לאחר מכירתה וכי הן מקפידות על כך שיעשה בתוכנה שימוש לא פוגעני. שלישית, השימוש העיקרי בשירותים אותן הנתבעות מספקות גורם להפרת הפרטיות באופן נרחב בכל רחבי העולם, במיוחד כאשר המערכת נמכרת והשירותים מסופקים לממשלות כגון מקסיקו ואיחוד האמירויות, שאינן מקפידות, בלשון המעטה, על שמירה על זכויות הנתונים שלהם לפרטיות.

95. התובעים יטענו כי לנתבעות קיימת אפשרות שליטה על המידע העובר אל הלקוחות אשר הן מספקות, וכי הן אינן נוקטות אמצעים אקטיביים למניעת ההפרות. חמור יותר, וכפי שצויין לעיל, הנתבעות אינן אף מתעניינות כנגד מי מבוצע המעקב, הן מוכנות לספק השירותים הללו גם במחיר של פגיעה בחפים מפשע.

### **עוולה נזיקית בהתאם לחוק המחשבים, התשנ"ה-1995**

96. סעיף 7 לחוק המחשבים קובע כהאי לישנא:

"מעשה מן המעשים המנויים להלן הוא עוולה על פי פקודת הנויקין [נוסח חדש], והוראותיה של פקודה זו יחולו עליו –

(1) הפרעה שלא כדין לשימוש במחשב או בחומר מחשב, בכל דרך שהיא, לרבות על ידי גזילת דבר המגלם חומר מחשב;

(2) מחיקת חומר מחשב, גרימת שינוי בו או שיבושו בכל דרך אחרת, שלא כדין.

97. התובעים יטענו כי מעשי ו/או מחדלי הנתבעות כפי שתוארו בפרוטרוט לעיל עולים לכדי עוולה נזיקית במובן סעיף 7 לחוק המחשבים. התובעים יטענו כי במעשיהם ו/או מחדליהם המתוארים לעיל הנתבעות גרמו להפרעה שלא כדין לשימוש במחשב או בחומר מחשב, לרבות על ידי גזילת



דבר המגלם חומר מחשב. עוד יטענו התובעים כי הנתבעות הפרו את הוראת סעיף 7 לחוק המחשבים בכך שגרמו למחיקת חומר מחשב, גרמו לשינוי בו או שיבשו אותו בכל דרך אחרת.

98. התובעים יצינו כי על הנתבעות רובץ נטל הראיה להראות כי מעשיהם המתוארים לעיל נעשו כדין. החוק מעביר נטל הראיה אל כתפי הנתבעות לבוא ולהוכיח כי מעשיהם ו/או מחדליהם נעשו כדין. העובדה כי שיווק המערכת לגורמים במקסיקו קיבל אישור משרד הביטחון אינה מהווה כשלעצמה ראיה לכך כי פעילותיה המתוארים נעשו כדין.

### **מחדליהם ורשלנותם של הנתבעות**

99. מבלי לגרוע מכלליות האמור לעיל, התובעים יוסיפו ויטענו, כי נזקיהם נגרמו בשל רשלנותן וחוסר זהירותן של הנתבעות אשר התבטאו, בין היתר, במעשים ובמחדלים כדלקמן:

- א. הנתבעות לא פעלו כפי שחברות סבירות, המספקות שירותי סייבר אשר מטיבם וטבעם פוגעים או עלולים לפגוע בפרטיות, אמורות לפעול וצריכות לפעול בנסיבות העניין.
- ב. הנתבעות פעלו בחוסר זהירות, תוך הפרה בוטה של הוראות הדין, אשר נועדו לטובת התובעים ולהגנתם.
- ג. הנתבעות לא נקטו באמצעים מספיקים או הדרושים כדי למנוע את הפגיעה בפרטיותם, כבודם של התובעים.
- ד. הנתבעות לא קבעו נוהלים והוראות שיבטיחו את השמירה על כבודם, פרטיותם, של התובעים.
- ה. הנתבעות לא דאגו לבקרה ולפיקוח על הפעילות, הנעשית על ידי הלקוחות שלהן, בשירותים אותם סיפקו.
- ו. הנתבעות יצרו מערכת מסוכנת שהשימוש בה עלול לפגוע נאשות בזכותם של התובעים ואחרים לפרטיות.
- ז. הנתבעות פיתחו ועודדו תרבות של זלזול בפרטיות ואף פגעו בפרטיות לשם הדגמת יכולת המערכת.
- ח. הנתבעות המשיכו למכור מערכות ולספק תמיכה ושדרוג מערכות למדינות הידועות בהפרת זכויות אדם גם לאחר שנתגלה שמדינות אלה משתמשות במערכות נגד פעילי זכויות אדם ועיתונאים ובניגוד לחוק.
- ט. הנתבעות סרבו, ועדיין מסרבות, לבקשות רשמיות חוזרות ונשנות לשיתוף פעולה בחקירה פלילית המתנהלת בעניין.

י. מעשיהם אלו של הנתבעות גרמו לתובעים נזקים כבדים, כמפורט בהרחבה להלן.

יא. התובעים יטענו כי החובה לנהוג בזהירות במקרה זה מובהקת, מאחר והנתבעות יצרו את הסיכון שגרם לנזק, קרי, פיתחו ושיווקו את הטכנולוגיה המאפשרת שימוש לרעה.

יב. התובעים יטענו כי הנתבעות צפו את ההתנהגות והשימוש לרעה בטכנולוגיה האמורה על ידי לקוחותיה, במיוחד שמדובר בגורמים שיש לגביהם סימני שאלה בדבר מידת שמירתם על זכויות אדם בארצותיהם.

100. זאת ועוד, אחריותן של הנתבעות קמה הן באופן ישיר והן כמשדלות ו/או מסייעות (סעיף 12 לפקודת הנוזיקין (נוסח חדש), נ"ח התשכ"ח 266 (להלן: "פקודת הנוזיקין").

101. התובעים יטענו כי הנתבעות יצרו מערכת מסוכנת המאפשרת פגיעה קשה בפרטיות ומאפשרת שימוש לרעה המהווה גורם שבלעדיו אין. הטכנולוגיה שהנתבעות מפתחות ומשווקות מהווה גורם שאלמלא קיומו לא היה נזק נגרם והנתבעות היו צריכות לצפות כי טכנולוגיה זו מטיבה ומטבעה תגרום לנזק בגין פגיעה בזכות לפרטיות. אשר על כן, יטענו התובעים כי יש להטיל על הנתבעות אחריות מוחלטת. לחלופין, התובעים יטענו להחלת חזקה "הדבר המסוכן" הקבועה בסעיף 38 לפקודת הנוזיקין והקובע, כי בהקשר שלנו על הנתבעות נטל הראיה להוכיח שלא הייתה התרשלות וכי נקטו אמצעי זהירות נאותים למניעת הנזק (סעיף 41 לפקודת הנוזיקין).

102. התובעים יטענו כי החובה לנהוג בזהירות במקרה זה הינה מובהקת, מאחר והנתבעות יצרו את הסיכון שגרם לנזק, שכן הן אלה שיצרו את הטכנולוגיה המאפשרת לבצע ריגול אחרי התובעים ורבים אחרים.

103. התובעים יטענו כי הנתבעות צפו את ההתנהגות והשימוש לרעה בטכנולוגיה שהן יצרו על ידי צד שלישי אתו הן התקשרו בחוזה. אחריותן של הנתבעות קמה הן באופן ישיר והן באופן עקיף כמשדלות ו/או מסייעות במובן סעיף 12 לפקודת הנוזיקין.

### **הפרת חובה חקוקה**

104. התובעים יטענו כי באספקת המערכת ובמתן ואספקת השירותים הנלווים לה כפי שתואר לעיל, הנתבעות אחראיות כלפי התובעים בגין הפרת חובה חקוקה לפי סעיף 63 לפקודת הנוזיקין. הפרת החובה החקוקה באה לידי ביטוי בהפרת החובות המוטלות על הנתבעות שלא לפגוע בפרטיותם של התובעים וכלל הציבור. לצד הוראות חוק הגנת הפרטיות, הנתבעות הפרו את חובתן החקוקה שלא לפגוע בזכותם החוקתית לכבוד המעוגנת בחוק יסוד: כבוד האדם וחירותו, וכן הפרו את החובה הקבועה בסעיף 2(ג) לחוק האזנת סתר, תשל"ט-1979 שקובעת כי: "המציב או המתקין מכשיר למטרת האזנת סתר שלא כדין או כדי לאפשר שימוש בו למטרה האמורה, דינו – מאסר חמש שנים."



105. התנהגותן של הנתבעות גרמה לתובעים את הנזק שאותו החיקוק התכוון למנוע. קרי פגיעה בפרטיותם ובכבודם.

### **מניעת פגיעה עתידית בתובעים ובאחרים**

106. התובעים יטענו כי השירותים אותם הנתבעות מציעות ומספקות כוללים פוטנציאל לפגיעה עתידית בפרטיות ובזכויות מוגנות אחרות של התובעים ושל הציבור בכללותו. פגיעה זו נעשית על ידי הנתבעות אשר נוכח מעמדן ואופי שירותן, מחויבות שלא לפגוע בזכויות המוגנות של הציבור.

107. אשר על כן, לא די במתן פיצויים לתובעים, אשר מטרתן תיקון הנזקים שנגרמו והשבת המצב לקדמותו, התובעים מבקשים למנוע פגיעה עתידית בהם ובניזוקים פוטנציאליים אחרים, וזאת על ידי מתן צווים אשר ימנעו את המשך אספקת השירותים הנתבעות מציעות ומספקות. זאת על מנת למנוע את הצורך לחזור ולהגיש תביעות נוספות כגן זו בכל פעם שהשירותים שהנתבעות מספקות יפגעו בפרטיותם או בפרטיות אחרים.

### **החלת עקרונות המשפט הציבורי על הנתבעות**

108. התובעים יטענו כי לאור העובדה כי הדין אינו נותן מענה מלא למציאות הטכנולוגית המתפתחת היום, יש להחיל עקרונות ונורמות מן המשפט הציבורי על השירותים שהנתבעות מציעות ועל פעילותן וזאת נוכח מעמדן ואופי השירותים שהן מציעות ומספקות.

109. התובעים יטענו כי קיים אינטרס ציבורי כללי ממדרגה ראשונה ביחס לשירותים שהנתבעות מספקות, אשר מצדיק החלת סטנדרט ציבורי על תחומי הפעילות של הנתבעות. כל זאת לאור האופי המעין ציבורי של הפעילות שהן מספקות ושל תחום ההתמחות שלהן שבדרך כלל הינו נחלת רשויות המדינה וזרועותיה הביטחוניות.

110. לא תתכן כלל מחלוקת כי הנתבעות הינן חברות העוסקות בתחומי ביטחון: הן קרובות וקשורות לזרועות הבטחון במדינה, רבים מעובדיהן הם יוצאי יחידות מודיעין בצבא, והמדינה מתייחסת למוצרים של הנתבעות כאל נשק החייב ברישיון ופיקוח לפי החוק לפיקוח על ייצוא ביטחוני. יצוין, כי ההתקשרות עם גורמי הממשל במקסימום לרוב נעשתה מתוקף הרישיון שקיבלה מאת משרד הביטחון האחראי על מתן רישיונות לחברות ישראליות לייצוא נשק, והעסקה הייתה מפורקת בהתאם להוראות החוק.

111. את אופיין הציבורי של הנתבעות אפשר ללמוד גם מהמקרה שאירע לאחרונה עת שעובד מפוטר של הנתבעות ניסה למכור את המערכת לצד שלישי, בלי אישור הנתבעות ובלי אישור משרד הביטחון. המדינה התייחסה אל המקרה בחומרה רבה והיא ניהלה מעקב באמצעות השב"כ כנגד העובד עד שנתפס והוגש נגדו כתב אישום חמור במיוחד. סעיפי האישום שהוכללו בכתב האישום מעידים יותר מכל על האופי בטחוני/ציבורי של השירות שהנתבעות מספקות.

112. באופן תאורטי, הנתבעות יכולות להפעיל את המערכת כנגד כל אדם החי בתוך מדינת ישראל או מחוצה לה, ובכך לנהל מעקב מתמשך אחריו ולקבל מידע על פרטים רגישים ביותר הקשורים

לחיו האישיים של האדם תחת מעקב. לא יעלה על הדעת לאפשר כוח כזה בידי חברה פרטית מבלי להחיל עליה פיקוח ממשלתי וליישם עליה נורמות וחובות מהמשפט הציבורי. הרי רק מדינות וגופים מורשים על פי חוק ובמקרים חריגים ביותר מוסמכים בצל הגבלות ותנאים לפגוע בפרטיות של אדם. הנתבעות, חברות פרטיות, המחפשות למקסם רווחיהן בכל דרך, אינן אמורות לפעול באופן חופשי מבלי להחיל עליהם אמות מידה החלות על מדינות וגופים ממשלתיים שבידיהן כוח דומה!

113. התובעים יטענו, כי השימוש הנעשה במערכת פגסוס משפיע על כלל הציבור בצורה ניכרת. הכוונה כאן היא לציבור החי במדינת ישראל וגם מחוץ לה בכל אותן המדינות שרכשו את המערכת מאת הנתבעות. בכך הנתבעות נושאות חובה כלפי ציבורים הללו לפעול באופן מידתי, סביר ובתום לב, וכן להימנע מפגיעה בזכויות חוקתיות מוגנות ובעיקר הזכות לפרטיות ובזכות לשם טוב. חובות הללו חלות על הנתבעות באופן מובהק.

114. להמחשת הנקודה, נחזור על סעיפי כתב האישום שהוגש לאחרונה כנגד עובד לשעבר של הנתבעת מס' 1: ניסיון לפגיעה ברכוש שהיה בו כדי לפגוע בביטחון המדינה, גניבה בידי עובד, וביצוע פעולת שיווק ביטחוני ללא רישיון שיווק ביטחוני. סעיפים אלה מעידים כי על אף שמדובר בחברות פרטיות, בשל רגישות תחום הפעילות שלהן ואפיו הציבורי ומידת המוסכנות הטמונה במוצרים המפותחים על ידי הנתבעות, יש להחיל עליהן נורמות מן המשפט הציבורי.

115. העובדה כי פעילותן של הנתבעות חוסה תחת חוק הפיקוח על ייצוא ביטחוני אף היא מלמדת על אופיין הדואלי של הנתבעות שעל אף היותן חברות פרטיות, מדובר בחברות מיוחדות בעלות מאפיינים של גופים ציבוריים וניתן לראותן כגוף דו מהותי. לחלופין, וגם באם לא מדובר בגוף דו מהותי, התובעים יטענו כי איסור הפגיעה בפרטיות חל גם על גופים פרטיים ובוודאי חלה על הנתבעות המקבלות רישיון מהמדינה לעסוק בתחומן.

116. התובעים יטענו, כי בידי הנתבעות פוטנציאל אדיר לפגוע בפרטיותם של אנשים. כפי שהוכח לעיל מההתנהגויות ומדפוסי הפעולה שהנתבעות אימצו, הנתבעות נכשלו לעמוד בנורמות הנדרשות מהן בנוגע לאופן השימוש בשירותים אותם הן מספקות. התובעים יטענו, כי הנתבעות הפרו ברגל גסה עקרונות אלה הן בכובען כמעוול ראשי והן בכובען כשותפות למעוול ובעלות תרומה מכרעת.

117. התובעים יוסיפו ויטענו, כי המשך הפעלת השירותים של הנתבעות יאפשר לנתבעות ולקוחותיה להמשיך ולפגוע בזכות לפרטיות של התובעים ושל רבים אחרים בכל רחבי העולם ובתוך מדינת ישראל.

#### **הפגיעה בפרטיות והפרת המשפט הבינלאומי**

118. התובעים יוסיפו ויטענו כי מעשיהן/מחדליהן של הנתבעות והפגיעה בזכות לפרטיות של התובעים מהווה הפרה של סעיף 17 לאמנה הבינלאומית בדבר זכויות אזרחיות ומדיניות משנת 1966 שישראל אישרה ובכך הפכה להיות חלק מהמשפט הפנימי. סעיף 17 לאמנה קובע כי:



1. לא יהיה אדם נתון להתערבות שרירותית או בלתי-חוקית בצנעת הפרט שלו, במשפחתו, בביתו או בכתובתו, או לפגיעות בלתי חוקיות בכבודו או בשמו הטוב.

2. לכל אדם הזכות להגנת החוק נגד התערבויות או פגיעה כאלה.

119. החובה לכבד הזכות לפרטיות אינה רק נחלתם של גופים ציבוריים או ממשלות. גופים פרטיים, ועל אחת כמה וכמה חברות כגן הנתבעות שיש להן אופי ציבורי מובהק, גם הן חייבות לכבד זכות זו ולתת את הדין על הפרתה. עקרון זה התבסס בשנים האחרונות ובמיוחד לאחר שהאו"ם פירסם את ה-Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and remedy" Framework בשנת 2011.

120. עקרונות אלה מטילים על המדינה ורשויותיה, וכן על הנתבעות, לכבד ולהימנע מלפגוע בזכויות אדם. לגבי עסקים וגופים פרטיים, העיקרון המרכזי כפי שנקבע בסעיף 11 מעקרונות המנחים קובע כי:

"Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."

121. על מנת להבהיר את הנקודה ולהמחשתה, האם מישהו יכול למשל לערער או לפקפק בכך שחברות ענק כגון "פיסבוק", "גוגל" ואחרות מחויבות בכיבוד הזכות לפרטיות של האנשים ברחבי העולם כולו? האם יעלה על הדעת לקבל את הטענה כי החברות הללו אינן ציבוריות ואינן גופים מעין ממשלתיים ועל כן אינן מחויבות בכיבוד זכויות אדם כגון הזכות לפרטיות ובהתאם הן יכולות לעשות ולעוול ולפגוע בזכות לפרטיות ככל העולה על רוחן? בוודאי כי התשובה על שאלה זו הינה שלילית.

122. באשר למדינה, העיקרון המרכזי כפי שבא לידי ביטוי בסעיף 1 של העקרונות המנחים קובע כי:

"States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication."

123. התובעים יטענו כי חובה זו לשמור ולכבד את הזכות לפרטיות של התובעים ואחרים מוטלת גם על בית משפט נכבד זה, וכי חובה זו מחייבת מתן סעד לתובעים כנגד מעלליהן של הנתבעות.

124. יצויין כי טיעון זה אינו נובע מתחום המשפט הבינלומי גרידא. הזכות לפרטיות מעוגנת במספר מקורות במשפט הישראלי, ויש לה למעמד חוקתי לאחר שנקבע בסעיף 7 לחוק יסוד: כבוד האדם וחירותו כי:

7. (א) כל אדם זכאי לפרטיות ולצנעת חייו.

(ב) אין נכנסים לרשות היחיד של אדם שלא בהסכמתו.

(ג) אין עורכים חיפוש ברשות היחיד של אדם, על גופו, בגופו או בכליו.

(ד) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו.

125. משמעותו של עיגון חוקתי זה היא שעיקרון השמירה על הפרטיות צריך להיות עקרון מנחה לבית המשפט כאשר בית המשפט עוסק במלאכת פרשנות החוק ובעת מתן הסעדים הנדרשים.

## ה. הסעדים

### פיצוי כספי עבור הפגיעה בכל תובע

126. התובעים יבקשו מבית המשפט הנכבד לחייב את הנתבעות, ביחד ולחוד, בפיצוי כספי כתוצאה מהנזקים אשר נגרמו לתובעים.

127. התובעים יבקשו לקבל פיצוי בסך של 451,000 ₪ כל אחד וזאת בגין הנזקים שנגרמו כתוצאה מהפגיעה בפרטיות וואו הפרת חוק המחשבים וואו הפרת חובה חקוקה על ידי הנתבעות וואו התרשלות שהנתבעות.

128. בנוסף, התובעים יבקשו לשלם להם פיצוי לכל אחד בסך של 50,000 ש"ח ללא הוכחת נזק בהתאם לסעיף 29א לחוק הגנת הפרטיות.

129. בסך הכל, נכון למועד הגשת תובענה זו, הדרישות הכספיות שהתובעים דורשים לשלם להם עומדות על סך 2,505,000 ש"ח.

130. בנוסף, בית המשפט הנכבד מתבקש לחייב את הנתבעות בפיצוי לדוגמא, מכוח סמכותו הטבעה ולפי שיקול דעתו, זאת בהתחשב בנסיבות המיוחדות של מקרה זה ועל מנת ליצור הרתעה בעתיד מפני המשך דפוס ההתנהגות כפי שתואר לעיל שגורם להפרות קשות לזכותם של אנשים לפרטיות.

צו מניעה קבוע



131. במקרה דנן, ולאור המקובץ לעיל, התובעים יטענו כי לא די בתשלום פיצויים לתובעים. הפיצויים המבוקשים נועדו לתקן חלק מהנזקים שנגרמו בעבר בעוד שהצו נועד למנוע את המשך מתן השירותים שהנתבעות מספקות והפוגע בתובעים ובזכותם לפרטיות. על כן, בית המשפט הנכבד מתבקש למנוע את הפגיעה המתמשכת והעתידית העלולה להיגרם כתוצאה מהשירותים שהנתבעות מציעות ומספקות, על מנת למנוע את הצורך לחזור ולהגיש תביעות כגון זו בעתיד, בין אם על ידי התובעים ובין אם על ידי אחרים.

132. התובעים מבקשים מבית המשפט להוציא צו מניעה קבוע נגד שתי הנתבעות המורה להן:

א. להימנע באופן מוחלט, בין אם במישרין (לרבות באמצעות חברות בת, חברות אם, או חברות אחיות, בארץ ובחו"ל) ו/או באמצעות צדדים שלישיים, ממכירת מערכת "פגסוס", או כל מערכת אחרת שהנתבעות פיתחו ושיפתחו בעתיד כדוגמת מערכת "פגסוס", לממשלת מקסיקו הפדראלית, וכל רשות או גוף אכיפה, לרבות מדינות במקסיקו.

ב. להפסיק לאלתר ובאופן מוחלט, כל פעולת תמיכה, תחזוקה, שדרוג, סיוע, בין במישרין ובין באמצעות צדדים שלישיים, לרבות באמצעות חברות בת, חברות אם, או חברות אחיות, בארץ ובחו"ל, למערכת פגסוס או כל מערכת אחרת שהנתבעות כבר סיפקו לממשלת מקסיקו הפדראלית, וכל רשות או גוף אכיפה, לרבות מדינות במקסיקו.

133. כן מבקשים התובעים מבית המשפט להוציא צו קבוע נגד שתי הנתבעות המורה להן:

א. לאסור על לקוחותיהן, או כל משתמש אחר במערכת "פגסוס", או כל מערכת אחרת שהנתבעות פיתחו ושיפתחו בעתיד כדוגמת מערכת "פגסוס", לפרוץ למכשירי הטלפון של התובעים ולהימנע מאיסוף נתונים ממכשירי התובעים ו/או העברתם ו/או עיבודם.

ב. לגרום להשבתת ו/או הפסקת הפריצה למכשירי הטלפון של התובעים באמצעות מערכת "פגסוס", או כל מערכת אחרת שהנתבעות פיתחו ושיפתחו בעתיד כדוגמת מערכת "פגסוס", אם פריצה כזו למכשירי הטלפון של התובעים עודנה קיימת.

134. להוציא צו מניעה האוסר על הנתבעות למכור את תוכנת פגסוס ו/או כל תוכנת ריגול דומה אחרת למשטרים ו/או מדינות בעולם, אלא לאחר שיובטח כי אותו משטר ו/או מדינה יעשו באותה תוכנה שימוש באופן שאינו סותר את החוק המקומי והבינלאומי, וכן צו המורה לנתבעות לדאוג לכך, שהן בעצמן לא יספקו שירותי תמיכה, תחזוקה, שדרוג, סיוע בתפעול והדרכות לשימוש בתוכנת פגסוס או כל תוכנת ריגול דומה, לאחר שתוכנה כאמור נמכרה לגוף שלישי, אלא לאחר שיוודאו באופן פוזיטיבי ומתמשך כי השימוש שנעשה בתוכנה, נעשה כדין ובהתאם לצווים שיפוטיים של טריבונלים משפטיים מוסמכים באותן מדינות.

135. להוציא צו מניעה קבוע האוסר על הנתבעות למכור את תוכנת פגסוס ו/או כל תוכנת ריגול דומה אחרת למשטרים ו/או מדינות הידועות בהפרות שיטתיות של זכויות אדם.

136. וכן האוסר עליה לתמוך ו/או לתחזק ו/או לשדרג ו/או לסייע בתפעול תוכנת פגסוס או כל תוכנה דומה

### סוף דבר :

137. לבית המשפט הנכבד הסמכות העניינית והמקומית לדון בתביעה זו.
138. בהתאם לסעיפים 40 (1) ו- 51(א)(2) לחוק בתי המשפט, נוכח סכום הפיצויים המבוקש, לבית המשפט הנכבד הסמכות העניינית לדון בתביעה.
139. בהתאם לתקנה 3(א)(1) לתקנות סדר הדין האזרחי, תשמ"ד- 1984, נוכח מקום מושבם של הנתבעות, לבית המשפט הנכבד הסמכות המקומית לדון בתביעה.
140. אשר על כן, בית המשפט הנכבד, מתבקש לזמן את הנתבעות לדין ולחייבן לשלם לתובעים סך של 2,505,000 ש"ח בצירוף ריבית והפרשים כדין.
141. בנוסף, בית המשפט הנכבד מתבקש ליתן צווי מניעה כאמור בסעיפים 131-136 לעיל.
142. כמוכן, בית המשפט הנכבד מתבקש לחייב את הנתבעות בתשלום הוצאות משפט ושכר טרחת עורכי דין בצירוף מע"מ כדין.

ירושלים, 30.8.2018



מחמד דחלה, עורך דין



עלאא מחאנה, עורך דין