משרד הפנים

פעולות הביקורת

במשרד הפנים ובמוסד לביטוח לאומי בדק משרד מבקר המדינה את הפעולות הנעשות למימוש דרישות חוק הגנת הפרטיות והפסיקה בדבר הגנת הפרטיות ואבטחת המידע במאגרי המידע שבאחריותם. כן נבדקה איכות הנתונים במשרד הפנים.

הגנת הפרטיות - אבטחת מידע ואיכותו במאגרי מידע ממשלתיים

תקציר

התפתחות עולם המחשבים מאפשרת לאחסן מידע רב במערכות מחשב. חוק יסוד: כבוד האדם וחירותו קובע כי "כל אדם זכאי לפרטיות ולצנעת חייו". על פי חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), מידע מוגדר "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו". היות שמאגרי מידע מכילים פרטים אישיים, ועלולה להיות פגיעה בפרטיות האדם בין בשוגג בין במזיד אם נתוניו נמסרים לאחר, נדרש לאבטח את המידע. על פי חוק הגנת הפרטיות, אבטחת מידע היא "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין".

פעולות הביקורת

בחודשים מאי-נובמבר 2008, לסירוגין, בדק משרד מבקר המדינה את הפעולות הנעשות במשרד הפנים ובמוסד לביטוח לאומי (להלן - הביטוח הלאומי) למימוש דרישות חוק הגנת הפרטיות והפסיקה בדבר הגנת הפרטיות ואבטחת המידע במאגרי מידע שבאחריותם. כמו כן נבדקה איכות הנתונים במרשם האוכלוסין.

עיקרי הממצאים

רשות האוכלוסין, ההגירה ומעברי הגבול במשרד הפנים

רשות האוכלוסין, ההגירה ומעברי הגבול במשרד הפנים (להלן - רשות האוכלוסין) מופקדת על מאגרי מידע של ניהול מרשם האוכלוסין. מאגרי המידע הללו ובכללם המרשם מנוהלים באופן ממוחשב במערכת "אביב", המופעלת באמצעות חברה פרטית לשירותי מחשוב שמשרד הפנים התקשר עמה בשנת 1993[1]. המערכת הוגדרה על ידי הרשות לאבטחת מחשבים במשרד ראש הממשלה כמערכת מידע קריטית בעלת מידע בלתי מסווג, ומנהלה מונחה מקצועית על ידיה.

לא מונה ממונה לאבטחת מידע לא במשרד הפנים ולא ברשות האוכלוסין, בניגוד לדרישות חוק הגנת הפרטיות והתקשי"ר.

בשנים 2006-2007 הוצעה למכירה על ידי אלמוני באתר אינטרנט תכנה המכילה נתונים ממרשם האוכלוסין הכוללים קשרי משפחה בין אזרחים. בישיבת ועדת הפנים והגנת הסביבה של הכנסת במרס 2007 ביקש יו"ר הוועדה חקירה משטרתית בעניין[2]. בעקבותיה פנה משרד הפנים למשטרה בבקשה שתחקור בעניין. בינואר 2008 שלח משרד הפנים למשטרה, לבקשתה, רשימה של 20 לקוחות שמקבלים קובצי עדכון גדולים ממערכת "אביב", שייתכן שהמידע זלג מאחד מהם. במרס 2008 סגרה המשטרה את תיק התלונה בטענה שלא ניתן לחקור כל כך הרבה חשודים, ולכן העבריין לא נודע[3]. בין המסמכים שמסר משרד הפנים למשטרה היה סיכום בדיקה שבו נכללו כעשרה גופים שקיבלו עדכוני מרשם בהיקפים גדולים, ואחד מהם אף זוהה כמקבל נתונים בצורה דומה למבנה המאגר שהופץ באינטרנט. אפילו גוף זה לא נחקר על ידי המשטרה. לא נמצא שמשרד הפנים והמשטרה שיתפו פעולה בחקירה. שיתוף פעולה כזה היה עשוי להניב תוצאות חיוביות. יש לראות בחומרה את כישלונה של רשות האוכלוסין בהגנת פרטיותם של אזרחי המדינה

במרס 2008 הוחל במערך המחשוב של מרשם האוכלוסין ברישום יומן שימוש (להלן - לוג[4]) לשם מעקב אחר שאילתות שהציגו עובדי משרד הפנים ולקוחות חיצוניים. בבדיקת נתוני הלוג בחודשים מרס-יולי 2008 מצא משרד מבקר המדינה כי הוצגו שאילתות באמצעות הרשאות הגישה של 78 ממשתמשי המערכת, כשאלה שהו בחו"ל בלי שהייתה להם לכאורה גישה למערכת. נוסף על כך, נמצא שהוצגו שאילתות באמצעות הרשאות הגישה של חמישה משתמשים שלפי הרישומים במערכת "אביב" נפטרו לפני מועדי ביצוע השאילתות.

---

1 בעניין מערכת "אביב" ראו דוח ביקורת מיוחד של מבקר המדינה (פברואר 2006), **הסכם להספקת שירותי מידע ממאגרי מרשם האוכלוסין**. כן ראו מבקר המדינה, **דוח שנתי 48** (1998), "הקמת מערכת לניהול האוכלוסין - 'פרויקט אביב'", עמ' 590, ו**דוח שנתי 54ב** (2004) בפרק "פנקס הבוחרים לכנסת השש-עשרה: מהימנות הנתונים", עמ' 705.

2 **ישיבת ועדת הפנים והגנת הסביבה** מיום 7.3.07, פרוטוקול מס' 127, דברי היו"ר ח"כ אופיר פינס-פז.

3 בעניין אחריות המשטרה להודיע על סגירת תיקים למתלוננים ראו **דוח שנתי 55ב** של מבקר המדינה (2005) בפרק "סדרי סגירת תיקים פליליים בשל היעדר עניין לציבור ופיתוח פתרונות חלופיים", עמ' 353.

4 לוג (LOG) "יומן" מנוהל אוטומטית על ידי המחשב ובו נרשמות הפעולות הנעשות בו כגון משך השימוש במחשב, סיום השימוש בו, שינויים בנתונים, ניסיונות לבצע פעולה חריגה או בלתי מורשית.

באוגוסט 2008, כעשר שנים מאז מוחשב מרשם האוכלוסין, הוגש לראשונה לרשות האוכלוסין דוח סקר סיכונים על מערכת "אביב". בסקר הסיכונים עלו ליקויים בתחומים אלה: ניהול הסמכאות, הפעלת מערכות שליטה ובקרה, כלי ניהול ייעודיים, הצפנת הנתונים, עדכון גרסאות מערכות הפעלה ובדיקת נתוני קלט ממקורות חיצוניים. הליקויים מצביעים על פרצות העלולות להוביל לדליפת נתונים רגישים או לשיבוש הפעילות השוטפת בעקבות ניסיונות תקיפה או טעויות אנוש שלא יתגלו.

מדוח מבקרת הפנים מאפריל 2008 על לשכת אילת עולה כי במשך שנים ניצל לרעה מְנהל מינהל האוכלוסין באילת את מעמדו ואת הגישה הבלתי מוגבלת כמעט שהייתה לו למשאבי מערכת "אביב", בין השאר, למעשים אלה: הנפקת דרכונים שלא כדין וביצוע מניפולציות בתאריכים שונים במרשם. בעקבות הדוח פותח במערכת "אביב" מנגנון בקרה בשם "הרשאת מנהל", שחייבה לקבל אישור ממוחשב של עובד מטה הרשות להשלמת תהליך הנפקת דרכון או לעדכון רטרואקטיבי של המען. השינוי שהוחל בו ביוני 2008 גרם לעיכובים בטיפול בתושבים, מפני שעובדי המטה לא היו תמיד זמינים לאשר את הפעולות. ביולי 2008 הוענקו גם למנהלי לשכות ולסגניהם חלק מההרשאות. הענקת "הרשאת מנהל" לבעלי תפקידים בלשכות רוקנה מתוכן את הבקרה ואת ההשקעה ליישומה.

הועלו כ-200,000 רשומות של אזרחים פעילים שנולדו בארץ בשנות החמישים של המאה העשרים, שחסרים בהן מספרי הזהות של האב והאם. הדבר מקשה על בדיקות ייחוס הנדרשות לקביעת זכאויות (כגון יורשים), התחייבויות או מגבלות התלויות בבני משפחה. עוד הועלו כמיליון רשומות של תושבים פעילים שבהן רשום תאריך עלייה ולא נרשם מאיזו ארץ עלו, וכ-65,000 רשומות של תושבים פעילים שבהן רשומה ארץ העלייה ולא נרשם תאריך העלייה. בכ-550 רשומות של עולים נמצא שתאריך העלייה קדם לתאריך הלידה.

המוסד לביטוח לאומי

בביטוח הלאומי קיים ליקוי מבני מתמשך בעניין אבטחת מידע. הוועדה העליונה לאבטחת מידע בראשות סמנכ"ל משאבי אנוש דאז התכנסה לראשונה בספטמבר 2006 ופעלה במשך כתשעה חודשים. הממונה על אבטחת מידע כפוף ישירות לסמנכ"ל תקשורת ומערכות מידע (תמ"מ). מתוקף תפקידו של הממונה על אבטחת מידע הוא נדרש לבקר חלק מפעילות מערכות המידע של הארגון שהן בסמכותו של סמנכ"ל תקשורת ומערכות מידע (תמ"מ), וכפיפות זו פוגעת באי-תלותו. נוסף על כך, הוא אינו מקבל עליו את מרותו של הקב"ט בהתאם לכללי שירות הביטחון הכללי מ-2004. מן הראוי שהנהלת הביטוח הלאומי תגדיר מבנה יעיל לניהול אבטחת המידע במוסדה ותפעל באופן מידי ליישומו.

ביוני 2005 התחייב הביטוח הלאומי בפני בג"ץ[5] לרשום את כל הפעילות של כל משתמשי התקשורת בביטוח הלאומי. בספטמבר 2006 החליטה הוועדה העליונה לתקשורת ולמערכות מידע לרכוש את תכנת "האינטלינקס" (IntellinX) שמאפשרת לעשות זאת. אף שהיה ידוע למנהל החטיבה לאבטחת מידע עוד באוגוסט 2006 מהן

---

5 בג"ץ 8070/98 האגודה לזכויות האזרח בישראל נ' משרד הפנים ואח', תקדין.

דרישות החמרה לעבודתה התקינה של התכנה, לא נערכה החטיבה בהתאם לכך, דבר המעכב את השימוש בה. אי-אפשר להציג בתכנה שאילתות על המידע ולכן היא לא סיפקה לביקורת הפנימית את הכלים הדרושים לעבודתה, אף שהפעלתה תוכננה להתחיל במוסד לביטוח לאומי ב-2007.

סיכום והמלצות

עידן המידע מעמיד יכולות זמינות לרכז מידע, להעביר אותו במהירות ממקום למקום, להצליבו עם מידע אחר, לנתחו, למיין אותו ולהסיק מסקנות. מידע זה מצוי בידי גופים ציבוריים ופרטיים רבים, והם מחויבים בשמירתו. ללא מנגנוני אבטחה ובקרה מהותיים יש חשש ממשי לניצולו לרעה. עובדה זו מאיימת על הפרט בגלל האפשרות לחשוף בריש גלי את המידע האישי שנוגע לו. ואכן, בעטיים של מחדלים באופן השימוש במידע ובמאגרי מידע ובשמירה עליהם דלף בשנים האחרונות מידע אישי על תושבים ועל קבוצות אוכלוסיה שלמות - בניגוד לחוק הגנת הפרטיות.

על מנת לשפר את המצב יש לנקוט את הצעדים האלה: (א) על רשות האוכלוסין להכין נוהלי אבטחת מידע, להקפיד על יישומם ולאייש את התפקידים הנחוצים למילוי דרישות חוק הגנת הפרטיות. (ב) במוסד לביטוח לאומי יש להפעיל ולנצל את כל המערכות לאבטחת מידע אשר הפעלתן תוכננה כבר ב-2007. (ג) יש לערוך סקר סיכונים, להגדיר מדיניות אבטחת מידע ולהסדיר את המבנה הארגוני הנחוץ לאבטחת מידע במוסד לביטוח לאומי בכלל, ואת שיתוף הפעולה בין הקב"ט למנהל החטיבה לאבטחת מידע בפרט. (ד) מן הראוי להגביר את המודעות של העובדים לחובת השמירה על נוהלי העבודה בעניין אבטחת מידע. לשם מניעת חריגות מההוראות והנהלים ראוי שיפורסמו במסגרת פנים ארגונית העברות שעברו העובדים ואמצעי המשמעת שננקטו כלפיהם, תוך שמירת פרטיותם, וראוי שנושא המשמעת יוצג בקביעות בהנהלות הארגונים.

♦

מבוא

התפתחות עולם המחשבים מאפשרת לאחסן מידע רב במערכות מחשב. מאגר מידע מוגדר בחוק הגנת הפרטיות התשמ"א-1981 (להלן - חוק הגנת הפרטיות), כ"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב למעט - (1) אוסף לשימוש אישי שאינו למטרת עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף". על פי חוק הגנת הפרטיות, מוגדר מידע "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו". היות שמאגרי מידע מכילים פרטים אישיים, ועלולה להיות פגיעה בפרטיות הזולת בין בשוגג בין במזיד אם נתוניו נמסרים לאחר, יש לאבטח את המידע על פי חוק הגנת הפרטיות. אבטחת מידע היא "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין".

שלמות המידע מוגדרת כ"זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין".

אבטחת מידע מקוימת בשתי שיטות מקבילות ומשולבות: אבטחה פיזית הכוללת פעולות שיש לבצע בחמרה ובתשתיות על מנת למנוע פגיעה פיזית במאגר המידע ואבטחה לוגית על ידי הפעלה של מנגנוני תכנה ייעודיים, לדוגמה: שם משתמש וססמה המוזנים כתנאי כניסה למחשב. שתי השיטות ניתנות לשילוב באמצעי כמו "כרטיס חכם", שהוא אמצעי פיזי לזיהוי משתמש שדורש בו בזמן הזנת ססמה.

בתקופה מאי-נובמבר 2008, לסירוגין, בדק משרד מבקר המדינה את הפעולות שעשו משרד הפנים והמוסד לביטוח הלאומי (להלן - הביטוח הלאומי) למימוש דרישות חוק הגנת הפרטיות והפסיקה בדבר הגנת הפרטיות ואבטחת המידע על תושבים במאגרי מידע שבאחריותם. כמו כן נבדקה איכות הנתונים במרשם האוכלוסין.

המסגרת הנורמטיבית

מספר חוקים עוסקים בהגנת הפרטיות ובצנעת הפרט. סעיף 7(א) לחוק יסוד: כבוד האדם וחירותו קובע כי "כל אדם זכאי לפרטיות ולצנעת חייו". פגיעה בזכות זו מותרת רק בחוק ההולם את ערכיה של מדינת ישראל, שנועד לתכלית ראויה ובמידה שאינה עולה על הנדרש או מכוח הסמכה מפורשת בחוק. בחוק הגנת הפרטיות נקבע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". עוד נקבע כי "לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל, או כמחזיק של מאגר מידע אלא לצורך ביצוע עבודתו... המפר הוראות סעיף זה, דינו מאסר - 5 שנים". על פי חוק הגנת הפרטיות, האחריות לאבטחת מידע חלה על בעלים, על מחזיק או על מנהל של מאגר מידע. חוק הגנת הפרטיות מחייב גופים שונים, וביניהם כל הגופים הציבוריים המוגדרים בו, למנות ממונה על אבטחת מידע וקובע כי כל מאגר מידע המפורט בסעיף 8(ג) בחוק זה חייב להירשם אצל רשם מאגרי המידע במשרד המשפטים. כמו כן נקבעה החובה לקיום רישום בדבר מסירת מידע באופן קבוע גם בגוף המוסר וגם בגוף המקבל. פרק ד' לחוק הגנת הפרטיות מסדיר מסירת מידע בין גופים ציבוריים וקובע לכך מגבלות. נושא זה הוסדר בהרחבה בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 (להלן - תקנות הגנת הפרטיות) שבהן מפורטים ההוראות לניהול מאגר מידע, נהלים להעברת מידע בין גופים ציבוריים וסדרי ניהול מאגר המכיל מידע מוגבל וכללי השימוש בו.

במאי 2004 הוגשה עתירה לבית המשפט העליון על ידי האגודה לזכויות האזרח בעניין מסירת מידע לגופים ציבוריים ולבנקים[6]. בעתירה ביקשו העותרים לאסור על המדינה לאפשר גישה ישירה למאגר המידע על פי חוק מרשם האוכלוסין על ידי חיבור מחשב משרד הפנים למחשבים של משרדים אחרים ולהורות כי הדרך היחידה לקבלת המידע תהיה בקשה פרטנית. בית המשפט קבע כי "האיזון הראוי מחייב להגביל את מסירת המידע לעובדי ציבור בתקנות או בהנחיות מנהליות". בעקבות פסק הדין תוקנו תקנות הגנת הפרטיות וכן חוק מרשם האוכלוסין, התשכ"ה-1965. בתקנות הגנת הפרטיות נקבעה חובה להקים בכל גוף ציבורי ועדה שתפקידה לדון ולהחליט אם ובאיזו מידה להיעתר לבקשות למסירת מידע מהגוף הציבורי ולאשר הגשת בקשות של גוף ציבורי לקבלת מידע מגוף ציבורי אחר. כמו כן על הוועדה לקבוע הוראות בעניין הרשאות והגבלות הנוגעות לגישה למאגר המידע.

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - חוק הסדרת הבטחון), מטיל חובה על גוף ציבורי למנות ממונה ביטחון (להלן - קב"ט) האחראי במסגרת תפקידו לפעולות

---

6 ראו הערת שוליים 5 לעיל, בג"ץ 8070/98.

אבטחה אלה: "פעולות אבטחה פיזית" לרבות שמירה על רכוש; "פעולות לאבטחת מערכות מחשבות חיוניות" הכוללות את כל הפעולות הנדרשות לשמירה על המערכות הממוחשבות, על המידע בהן ופעולות למניעת פגיעה בהן; "פעולות לאבטחת מידע" לשם שמירה על מידע מסווג ומניעת פגיעה בו. חוק זה קובע כי גופים ציבוריים המנויים בתוספת הרביעית לו ובכללם משרד הפנים חייב במינוי אחראי לארגון ולביצוע פעולות לאבטחת מערכות ממוחשבות חיוניות ולפיקוח עליהן.

סעיף 117 לחוק העונשין, התשל"ז-1977, קובע: "עובד הציבור שמסר, ללא סמכות כדין, ידיעה שהגיעה אליו בתוקף תפקידו לאדם שלא היה מוסמך לקבלה, וכן מי שהגיעה אליו ידיעה בתוקף תפקידו כעובד הציבור, ולאחר שחדל מהיות עובד הציבור מסרה, ללא סמכות כדין, לאדם שלא היה מוסמך לקבלה, דינו מאסר שלוש שנים". עובד הציבור שהתרשל בשמירת ידיעה שהגיעה אליו בתוקף תפקידו או שעשה מעשה שיש בו כדי לסכן את בטיחותה של ידיעה כאמור, דינו מאסר שנה אחת.

האגף הבכיר לביקורת המדינה במשרד ראש הממשלה פרסם בספטמבר 2005 "נוהל מסגרת לאבטחת מידע" (להלן - נוהל המסגרת) המקיף 38 נהלים שונים ומפרט הלכה למעשה את העקרונות והכללים לאבטחת מידע במשרדי הממשלה. הוא כולל את הפרקים האלה: קביעת מדיניות ומיפוי מידע; הגורם האנושי ואבטחת המידע; אבטחה לוגית; אבטחה פיזית; גיבוי, שחזור והתאוששות; אבטחת תקשורת ושימושי אינטרנט; אבטחת מידע במחשבים המנותקים מרשתות המשרד. לפי נוהל המסגרת, לתחום אבטחת מידע בגוף ציבורי אחראי "הממונה על אבטחת מידע", והוא הגורם המוסמך ליישום המדיניות בעניין במשרד. באחריותו של הממונה לבקר את הפעילויות הממוחשבות המתבצעות על מנת לוודא שהמשרד עומד בדרישות אבטחת המידע הנובעים מהחוקים, מהתקנות ומהנהלים העוסקים בנושא זה.

לפי התקשי"ר, במשרדי הממשלה מנהל מאגר מידע אחראי לאבטחת המידע במאגר שעליו הופקד. מנהל מאגר מידע ימנה עובד אחראי לאבטחת המידע.

הגנת הפרטיות ואבטחת מידע במשרד הפנים

1. עד אפריל 2008 היה משרד הפנים באמצעות מינהל האוכלוסין מופקד על מרשם האוכלוסין. באפריל 2008 התקבלה החלטת ממשלה בדבר הקמת רשות האוכלוסין, ההגירה ומעברי הגבול במשרד הפנים (להלן - רשות האוכלוסין) במקום מינהל האוכלוסין. לפי החלטה זו כל הפעילות שהואצלה עד אז על ידי שר הפנים למשטרת ישראל בהתאם לסמכויות המוקנות לו בחוק הכניסה לישראל, התשי"ב-1952, שעניינו סדרי כניסה לישראל, תיעשה על ידי משרד הפנים.

רשות האוכלוסין מופקדת על ניהול מרשם האוכלוסין. מאגרים אלה מנוהלים במערכת "אביב", המופעלת באמצעות חברה פרטית לשירותי מחשוב שמשרד הפנים התקשר עמה בשנת 1993[7] (להלן - הספק). המערכת הוגדרה על ידי הרשות לאבטחת מחשבים במשרד ראש הממשלה (להלן - רא"ם) כמערכת מידע קריטית בעלת מידע בלתי-מסווג ומנהלה מונחה מקצועית על ידיה.

---

7 בעניין מערכת "אביב" ראו דוח ביקורת מיוחד של מבקר המדינה (פברואר 2006), **הסכם להספקת שירותי מידע ממאגרי מרשם האוכלוסין**. כן ראו **דוח שנתי 48 של מבקר המדינה** (1998), "הקמת מערכת לניהול האוכלוסין - 'פרויקט אביב'", עמ' 590 **ודוח שנתי 54ב של מבקר המדינה** (2004) בפרק "פנקס הבוחרים לכנסת השש-עשרה: מהימנות הנתונים", עמ' 705.

מאגרי מרשם האוכלוסין מכילים נתונים שנרשמו במהלך פעולות הרשות מכוח החוקים בתחומי האזרחות, השבות, מרשם האוכלוסין, הכניסה לישראל והיציאה ממנה. מאגרי מרשם האוכלוסין משרתים את משרד הפנים לכמה מטרות, ובהן: רישום המעמד האישי והפרטים האישיים האחרים של אזרחי ישראל ותושביה; הפקת תעודות זהות, דרכונים ומסמכים רשמיים אחרים; מתן רישיונות לישיבה בארץ; מתן אישורי כניסה לארץ; הפקת פנקס הבוחרים ורישוי כלי ירייה.

במרשם האוכלוסין יש כמה סוגים של משתמשים: משתמשי מערכת "אביב", שהם בעיקר עובדים פנימיים של רשות האוכלוסין, שצופים בנתונים ומעדכנים רשומות של תושבים, תיירים ועובדים זרים; לקוחות חיצוניים[8] המשתמשים במערכת "אביבים" רק להצגת שאילתות על נתוני מערכת "אביב"; מקבלי שירותי API[9], בעיקר לקוחות חיצוניים; עובדים פנימיים וחיצוניים המתחזקים את מערכת "אביב". כמו כן מקבלים לקוחות חיצוניים נתונים שנשלפים במיוחד בעבורם. בשנת 2008 היו למרשם האוכלוסין כ-275 לקוחות חיצוניים פעילים[10].

2. **נוהל "גורמי אבטחת מידע - הגדרות ותפקידים"**: נוהל המסגרת מגדיר את סמכויות בעלי התפקידים השונים בתחום אבטחת מידע במשרדי הממשלה. בנוהל "תכנית הכשרה של אחראים על אבטחה וביקורת של המידע" נקבע, כי המנהלים הכלליים של משרדי הממשלה יוודאו קיום תכנית עבודה שנתית ואמצעים לאבטחה ולביקורת על המידע במשרדיהם, בהתאם להוראות התקשי"ר; בכל משרד ימונה עובד לתפקיד "אחראי על אבטחה וביקורת של המידע", שיטמיע שיטות, כלים ונהלים לשמירת הזמינות, השלמות, המהימנות, השרידות והסודיות של המידע.

הביקורת העלתה כי לא מונה ממונה לאבטחת מידע לא במשרד הפנים ולא ברשות האוכלוסין, בניגוד לדרישות חוק הגנת הפרטיות והתקשי"ר.

משרד הפנים השיב בדצמבר 2008 כי נוהל המסגרת לא הועבר לידיעת מערך המחשוב, אך ייתכן כי הועבר למשרד הראשי.

משרד מבקר המדינה מעיר כי יש למנות ממונה על אבטחת מידע ברשות האוכלוסין ובמשרד הפנים. כמו כן בהיעדר נוהל מאושר לאבטחת מידע של רשות האוכלוסין מן הראוי שהרשות תבחן לאמץ את נוהל המסגרת כנוהל מחייב לאבטחת מידע, בהתאמות המתחייבות.

3. **זליגת מידע ממרשם האוכלוסין**: מידע זלג ממשרדים ממשלתיים והגיע לגופים פרטיים שעשו בו שימוש בניגוד לחוק הגנת הפרטיות. בשנים 2006-2007 הציע אלמוני למכירה באתר אינטרנט תכנה המכילה נתונים ממרשם האוכלוסין הכוללים קשרי משפחה בין אזרחים. בישיבת ועדת הפנים והגנת הסביבה של הכנסת במרס 2007 ביקש יו"ר הוועדה חקירה משטרתית בעניין[11], ומשרד הפנים פנה למשטרה בבקשה שתחקור בעניין.

בינואר 2008 שלח משרד הפנים למשטרה, לבקשתה, רשימה של כ-20 לקוחות שמקבלים קובצי עדכון גדולים ממערכת "אביב", וייתכן שמקור זליגת המידע היה אחד מהם. במרס 2008 סגרה המשטרה את תיק החקירה בטענה שלא ניתן לחקור כל כך הרבה חשודים ולכן העבריין לא נודע.

---

8 כגון משרדי ממשלה, רשויות מקומיות, ביטוח לאומי ואחרים.

9 Application Program Interface - ממשק להעברת נתונים דו-כיוונית בתקשורת מחשבים בין היישום אצל הלקוח ובין היישום במערכת "אביב".

10 לקוחות שקיבלו שרותי מרשם בשנת 2008.

11 **ישיבת ועדת הפנים והגנת הסביבה** מ-7.3.07, פרוטוקול מס' 127, דברי היו"ר ח"כ אופיר פינס-פז.

בין המסמכים שמסר משרד הפנים למשטרה היה סיכום בדיקה על נתוני המאגר שהופץ באינטרנט, שהכין הספק, בו נכללו כעשרה גופים שקיבלו עדכוני מרשם רבים, ואחד מהם אף זוהה כמקבל נתונים בצורה דומה למבנה המאגר שהופץ באינטרנט. משרד מבקר המדינה העלה שגוף זה לא נחקר על ידי המשטרה. סגן ראש מפלג הונאה ירושלים, שהיה אחראי לחקירה, הסביר לנציג משרד מבקר המדינה כי סיכום הבדיקה נשקל לפני החלטת המשטרה להפסיק את החקירה.

הביקורת העלתה כי לפי הסכם בין משרד הפנים לבין הלקוחות החיצוניים, יש למשרד זכות לחקור את מצב אבטחת המידע אצל הלקוחות. ראש מערך המחשוב ברשות האוכלוסין מסר למשרד מבקר המדינה כי משרד הפנים לא בדק בעצמו את דבר זליגת המידע אצל לקוחות חשודים כדי לא להפריע למשטרה בחקירתה.

לא נמצא שמשרד הפנים והמשטרה שיתפו פעולה בחקירה. שיתוף פעולה כזה היה עשוי להניב תוצאות חיוביות. לדעת משרד מבקר המדינה יש לראות בחומרה את כישלונה של רשות האוכלוסין בהגנת ושמירת פרטיותם של אזרחי המדינה.

4. **יומן שימוש בשאילתות**: רק במרס 2008 הוחל במערך המחשוב של מרשם האוכלוסין ברישום יומן שימוש (להלן - לוג[12]) לשם מעקב אחר שאילתות שהוצגו בידי עובדי משרד הפנים ובידי לקוחות חיצוניים. הלוג מאפשר לרשות האוכלוסין לוודא שגישת המשתמשים למידע על תושבים היא רק לצורכי עבודת המשתמש.

משרד מבקר המדינה העלה, כי עד מועד סיום הביקורת לא היה נוהל לבדיקת הלוג והורשו להשתמש בלוג לאיתור חריגים רק אנשי ביקורת ובקרה במשרד הפנים כגון המבקרת הפנימית. עוד נמצא שלא נקבעו סנקציות ברוח חוק הגנת הפרטיות נגד מי שמנצל את המערכת לרעה. לדעת משרד מבקר המדינה, יש לאפשר לממונים על אבטחת מידע אצל הלקוחות החיצוניים לבקר את פעילות המשתמשים במרשם ויש לקבוע סנקציות נגד המנצלים את השימוש במערכת לרעה.

בבדיקה של משרד מבקר המדינה על נתוני הלוג בתקופה מרס-יולי 2008 נמצא כי הוצגו שאילתות באמצעות הרשאות הגישה של 78 ממשתמשי המערכת, כשאלה שהו בחו"ל ולכאורה לא הייתה להם גישה למערכת. כמו כן הוצגו שאילתות באמצעות הרשאות הגישה של חמישה משתמשים שלפי הרישומים במערכת "אביב" נפטרו לפני מועדי ביצוע השאילתות. עוד העלתה הביקורת שפרטי חשבון משתמש של אחד ממפעילי הספק עדיין היו בשימוש שלוש שנים לאחר שעזב את החברה.

המקרים המתוארים לעיל מלמדים שמשתמשים מסרו את סמאותיהם לשימוש אחרים בניגוד לכללי השימוש במערכת "אביב" ובניגוד לחוק הגנת הפרטיות או לחילופין שהמשתמשים לא שמרו עליהן כיאות והן נגנבו או שהייתה חדירה למערכת על ידי זר.

משרד מבקר המדינה בדק מקרים של ריבוי שאילתות לגבי אותו אדם בתקופה מרס עד יולי 2008 והעלה ש-25 משתמשים הרבו בהצגת שאילתה על שלושה אנשים מפורסמים, דבר המעורר חשש לביצוע שאילתות שלא לצורכי עבודתם.

---

12 לוג (LOG) - "יומן" המנוהל אוטומטית ע"י המחשב ובו נרשמות הפעולות הנעשות בו כגון שימוש בו, סיום השימוש בו, רישום שינויים בנתונים, ניסיונות לבצע פעולה חריגה או בלתי-מורשית.

בתשובתו הודיע משרד הפנים, כי בעקבות ממצאי הביקורת עשה את הפעולות המתקנות האלה: שלח מכתב לכל נציגי הלקוחות המזהיר מפני חריגה בנושא זה; השווה בין קובץ משתמשי המערכת הפעילים לבין קובץ הנפטרים והכין תכנה הבודקת את החריגות אחת לחודש. כמו כן פנה ללקוחות החיצוניים ולמנהל אגף לשכות ברשות לבדיקת המקרים.

משרד מבקר המדינה מעיר, שיש לראות בחומרה את המחדלים שנמצאו בתחום השימוש בשאילתות. הצעדים שמשרד הפנים נקט לתיקון המצב הינם חלקיים בלבד ועליו ועל האחראים לאבטחת מידע אצל כל לקוח חיצוני שיש לו גישה למאגר המידע, בין היתר, לבדוק אם כל השאילתות היו לצורכי העבודה. אם יימצא שמשתמשים אלה הציגו שאילתות שלא לצורכי עבודה, יש לנקוט נגדם בצעדים משמעתיים או להגיש תלונה במשטרה.

5. **סקר סיכונים במערכת "אביב"**: נוהל מסגרת "סקרי סיכונים - ניהול ועריכה" עוסק במודעות לסיכונים ולאיומים אפשריים על מערכי המידע והמחשוב, בהערכתם בצורה נאותה ובניהולם לאורך זמן. הערכת סיכונים מוגדרת בנוהל זה כ"הערכת פגיעותם של מידע ושל אפשרויות לעיבוד מידע, הערכת איומים והשפעות עליהם והערכת היתכנות התממשותם". ניהול סיכונים מוגדר כ"תהליך הזיהוי, הבקרה והמזעור או סילוק של סיכוני אבטחה העלולים להשפיע על מערכות מידע. במסגרת ניהול סיכונים מתבצע סקר סיכונים, שמטרתו לאתר את הסיכונים לארגון ולהעריך את חומרתם, זאת על מנת לאפשר קבלת החלטה מבוססת באיזה סיכונים לטפל, ובאיזה סדר עדיפות, עלות ולוח זמנים."

באוגוסט 2008, כעשר שנים מאז מוחשב מרשם האוכלוסין, הוגש לראשונה דוח סקר סיכונים על מערכת "אביב" שנעשה בידי חברה חיצונית. מהדוח עולה כי "מערך המחשוב ומערכות המידע של מערכת 'אביב' במשרד הפנים לוקה בחסר במספר תחומים מהותיים החושפים את המערכת לסיכונים - חלקם סיכונים מהותיים בתחום אבטחת המידע ותפעול המערכות". להלן פירוט:

בבדיקת מערכת התקשורת נמצא כי נעשה שימוש מוגבל בכלי לניטור ולמניעה, ולכן ניסיונות תקיפה או טעויות אנוש יתגלו רק לאחר מעשה ורק אם ייעשה מעקב אחר אירועים כאלו. נמצאו מספר שרתים שלא הותקנה בהם מערכת הפעלה עם עדכוני אבטחה ולכן הם היו חשופים להתקפות של פורצים וכתוצאה מכך לשאיבת מידע בלתי-מבוקרת. עוד התברר כי לא קיימת רשת תקשורת ייעודית לניהול; התקשורת עם הסניפים מבוצעת בתשתית בזק והומלץ להצפין את הקווים הללו; אין מערכות טכנולוגיות מתקדמות של שליטה ובקרה, של כלי ניהול תקשורת ושל רכיבי הצפנה; לא נבדקים נתונים שנקלטים מגופים חיצוניים, דבר המאפשר "להזריק" קוד עוין למערכת ולשבש אותה או לגנוב ממנה מידע. נמצאו משתמשים שהיו להם הרשאות מְנהל שלא לצורך; נמצאו משתמשים שלא הוחלה עליהם מדיניות הססמאות; נמצאו מספר שירותי תקשורת פתוחים שאין בהם צורך. אלה מגדילים את הסבירות לחדירה של בלתי-מורשים ולחבלה.

הממצאים הפיסיים העלו כי אין נהלים ברורים וכתובים לכניסת מבקרים למתחם מערך המחשוב. נמצא כי כניסה בלתי-מאושרת למתחם בשעות הפעילות מאפשרת איסוף מידע או התקנת רכיבי איסוף ברשת המחשוב. מתחם משרד הפנים אינו מוגן על ידי מערכת אוטומטית לכיבוי אש, ולכן אם תפרוץ בו אש, היא עלולה להגיע גם לשרתים.

הביקורת העלתה ליקוי נוסף באבטחה הפיזית של המתקן המרכזי הנמצא במתחם הראשי של משרד הפנים: לפעמים הדלת החיצונית של המתקן הושארה ביודעין פתוחה ללא השגחה. יוטעם כי דלת חיצונית פתוחה של חדר שרתים המכיל את מרשם האוכלוסין של מדינת ישראל מהווה סיכון ביטחוני ובטיחותי כאחד.

משרד מבקר המדינה מעיר כי הבדיקה במסגרת סקר הסיכונים לא הייתה שלמה מפני שרשות האוכלוסין הגבילה את היקפה. הבדיקה נעשתה רק בסביבת הייצור[13]. עוד נמצא כי במסגרת סקר הסיכונים לא אישרה רשות האוכלוסין בדיקות חדירה למערכת. סקר סיכונים למערכת "אביב", שהיא מערכת מידע עיקרית של משרד הפנים, בוצע לראשונה רק ביוני 2008, אף שנתונים ממרשם האוכלוסין פורסמו כבר ב-2006 באינטרנט וקיים חשש שזלגו ישירות מן המערכת.

מערכת רישום ביקורת הגבולות

1. משטרת ישראל אחראית לרישום היציאות והכניסות במעברי הגבול של המדינה. הנתונים נרשמים במערכת ממוחשבת (להלן - מערכת רישום ביקורת גבולות)[14]. למידע זה חשיבות הן במישור ביטחון המדינה והן במישור של הגנת הפרטיות. באמצעות מאגרים נלווים נמנעת בין היתר כניסתם או יציאתם של אנשים מסוכנים או יציאתם של אלה שמבוקשים על ידי רשויות השלטון. למשטרת ישראל הסדרים עם גופים ממשלתיים, ביניהם רשות האוכלוסין, למשלוח עדכוני מערכת רישום ביקורת גבולות אליהם.

התברר שיש אי-התאמות בין נתוני רשות האוכלוסין לבין נתוני ביקורת הגבולות - חלקן נובעות משינוי שיטת הרישום של תנועות במערכת רישום ביקורת גבולות בשנת 2006, וחלקן -מפיגורים בקליטת העדכונים למערכת "אביב" או מאי-שליחת עדכונים ממערכת אחת לאחרת.

להלן דוגמאות: (א) לפני שינוי שיטת הרישום נרשמה בשיטה הישנה "דחיית מעבר" עקב סירוב לכניסה של אדם במעבר כשתי תנועות - כאילו נכנס ויצא באותו יום, ואילו בשיטה החדשה נרשם האירוע כתנועה אחת בלבד. מערכת "אביב" לא הותאמה לקליטה תקינה של התנועות החדשות, ולמעשה נרשם בה בטעות שהאדם נכנס לישראל.

(ב) יש אפשרות לשלוח לגופים הממשלתיים תנועת עדכון אחת על תושב אחד שיש לו שני מסמכי נסיעה: אחד של מדינת ישראל ואחד של מדינה זרה. במקרה הזה דורש משרד הפנים לקבל רק נתונים על המסמך הישראלי עם רישום מספר הזהות. למשרד מבקר המדינה התברר שתושבת ארעית נכנסה לארץ עם דרכון אוקראיני; במערכת רישום ביקורת גבולות נעשה קישור למספר הזהות שלה בארץ, ואילו למשרד הפנים נשלח עדכון לפי מספר הדרכון הזר ולא לפי מספר הזהות. במשרד הפנים לא נרשמה כניסתה לארץ כתושבת עד שהיא נכחה בלשכת משרד הפנים ובוצע "קישור" בין תנועת הדרכון הזר למספר הזהות. יצוין כי פעולת הקישור גורמת להופעת תנועת כניסה במערכת "אביב" ולא במערכת "אביבים" המיועדת ללקוחות חיצוניים, ולכן מוצגת תמונה מעוותת של תנועות המעבר לגבי לקוחות אלו.

בהתייחס לממצאי הביקורת השיבה משטרת ישראל בדצמבר 2008 כי אי-ההתאמות בין מערכת רישום ביקורת גבולות למערכת "אביב" נובעות ברובן המכריע מאי-התאמת מערכת "אביב" של משרד הפנים לפורמט הדיווח החדש של מערכת רישום ביקורת גבולות. כמו כן ציינה משטרת ישראל כי משרד הפנים נמנע מלעדכן את מערכותיו ודרש לקבל את המידע בפורמט הישן. משרד הפנים עשה זאת למרות שהוסבר לו שהיעדר מידע עדכני יפגע באמינות הנתונים שיקבל. אשר לתושב שיש לו שני מסמכי נסיעה, משרד הפנים השיב למשרד מבקר המדינה כי אינו יכול להסתמך על נתוני ביקורת

---

13 סביבת ייצור הנה חלק מסביבת עבודה וכוללת: תכנה, בסיס נתונים, משתמשים ועוד.

14 בעניין מערכת ביקורת גבולות ראו **דוח שנתי 47 של מבקר המדינה** (1997), "ביקורת גבולות", עמ' 580.

הגבולות לקישור נתוני דרכון ישראלי לרישום נתוני דרכון זר של אותו אדם כי קישור שאינו נכון יכול להביא לנזקים בלתי הפיכים, לכן מעדיף המשרד לטפל לבד בקישוריות בין הנתונים.

יש להטעים כי אי-ההתאמות בין מרשם האוכלוסין ובין הרישום במערכת ביקורת הגבולות פוגעות במהימנות הנתונים במערכות אלה וגם במהימנות הנתונים במערכות אחרות שמתעדכנות לפיהן. כמו כן נגרמים עיכובים בטיפול בתושבים בלשכות רשות האוכלוסין מאחר שיש לאמת ולתקן את רישומי הכניסות והיציאות באופן ידני לפני מתן שירותים מסוימים. לדעת משרד מבקר המדינה, יש לפתור את בעיית אי-ההתאמות בין המערכות בין היתר על ידי שילובן זו בזו או על ידי מיזוגן למערכת אחת.

2. משרד התחבורה מחזיק ומעדכן מאגר ממוחשב של תמונות הנהגים במדינת ישראל. משרד הפנים קיבל עדכונים ממאגר התמונות עד שנת 2007, לפי הסכם שנחתם בין המשרדים. הביקורת העלתה כי למרות קיום מאגרי תמונות של תושבי ישראל במשרדים הנ"ל טרם הוסדר השימוש אף באחד מהם במערכת רישום ביקורת הגבולות לשם זיהוי אלה שעוברים בגבולות ולגילוי זיופים.

3. משרד החוץ מנפיק דרכונים רשמיים (כגון דרכונים דיפלומטיים) לממלאי תפקידים מסוימים; גם בנציגויות המשרד בחו"ל מונפקים מסמכי נסיעה בעבור אזרחים ישראליים. התברר כי חלק מהנתונים על הנפקות אלה אינו מועבר למשרד הפנים ולמערכת רישום ביקורת גבולות, לכן אין אפשרות אוטומטית לוודא את מקוריות המסמכים. עקב כך עלולים האזרחים להיתקל בעיכובים בלתי-מוצדקים בעת מעברם בגבולות המדינה כשנבדקת מקוריות מסמכיהם.

4. לארגון אינטרפול מאגר מידע על כ-14 מיליון דרכונים גנובים ומבוטלים ברחבי העולם. אין במערכת רישום ביקורת גבולות מישק מקוון למאגר זה, ולכן ניסיונות כניסה או יציאה עם מסמך נסיעה בלתי-תקין לאו דווקא יאותרו. בעיה זו הועלתה בדוח ביקורת פנימי של משרד הפנים מאפריל 2008 (ראו להלן) שבו הומלץ שגם מדינת ישראל תשלח עדכונים על דרכונים ישראליים גנובים ומבוטלים למאגר האינטרפול כדי למנוע את ניצולם לרעה במעברי גבול בחו"ל.

עד מועד סיום הדוח, דצמבר 2008, לא הייתה התקדמות בנושא זה.

5. **הטיפול בדוח מבקרת הפנים של משרד הפנים**: החלטת ממשלה מספר 303 מפברואר 1964 קובעת כי "לא יוצא דרכון לעולה אזרח ישראלי, הנמצא בישראל פחות משנה, אלא במקרים מיוחדים, כאשר קיימות סיבות מצדיקות, ובאישור שר הפנים או מי שהוסמך על ידו". מדוח מבקרת הפנים מאפריל 2008 עולה כי במשך שנים ניצל לרעה מְנהל מינהל האוכלוסין באילת את מעמדו ואת הגישה הכמעט בלתי-מוגבלת שהייתה לו למשאבי מערכת "אביב", הנפיק דרכונים שלא כדין ועשה מניפולציות בתאריכים שונים במרשם.

בעקבות הדוח פותח במערכת "אביב" מנגנון בקרה להפרדת סמכויות בשם "הרשאת מנהל". לפי הנוהל, כשעובד בלשכה מתחיל תהליך הנפקת תעודות מעבר מסוימות כגון דרכון בעבור תושב השוהה בחו"ל או כשעובד מתחיל תהליך עדכון למפרע של המען לתאריך הקודם בשישה חודשים ויותר ליום העדכון, להשלמתם יש לקבל אישור ממוחשב של עובד מטה הרשות. שינוי זה בתהליכים הוחל בסוף יוני 2008 ומיד גרם לעיכובים בטיפול בתושבים מפני שלא תמיד היו עובדי המטה זמינים לאשר את הפעולות. ביולי 2008 דרש מנהל אגף בכיר לשכות ממנהל מערך המחשוב בידיעת מנהל רשות האוכלוסין להעניק את הסמכות "הרשאת מנהל" גם למנהלי לשכות ולסגניהם כדי לאפשר טיפול יותר גמיש ומהיר בתושבים. באותו חודש הוענקו למנהלי הלשכות ולסגניהם חלק מההרשאות.

6. עדכוני כניסות ויציאות של ביקורת הגבולות נקלטים ברשות האוכלוסין באיחור של כשלושה ימים מהרישום במערכת רישום ביקורת גבולות. אם תושב מתייצב בלשכת רשות האוכלוסין כדי לקבל שירות, ולפי רישומי מערכת "אביב" טרם נרשם שנכנס לארץ, יש אפשרות להזין כניסה על פי נוהל "הוספת/עדכון תנועה בביקורת הגבולות" שכולל תהליך רישום תנועה מסוג "נוכח בלשכה". החל מיולי 2008 הייתה אמורה השלמת הביצוע לחייב "הרשאת מנהל" למנהלי לשכות, לסגניהם ולאלה שהסמיכו המנהלים.

הביקורת העלתה כי עדיין יש לעובדי לשכות רשות האוכלוסין אפשרות להזין תנועות כניסה ויציאה ידניות מסוגים אחרים בלי צורך באישור של עובד אחר.

בנוהל "הוספת/עדכון תנועה בביקורת הגבולות" אף צוין שאת העדכון "נוכח בלשכה" ניתן לבצע רק 72 שעות לאחר כניסתו לארץ של האזרח, משך הזמן שבו מתעדכן הקובץ. הוראה זו עשויה להפחית את מספר המקרים של אי-ההתאמות בשיוך תנועות כניסה ויציאה, ואולם תושב הזקוק לטיפול מיידי עלול להיפגע ממנה. לדעת משרד מבקר המדינה, כדי למנוע עיכובים למטופלים, על רשות האוכלוסין להחיש את קליטת רישומי התנועות ממערכת רישום ביקורת גבולות.

עוד העלתה הביקורת שכל עובד בעל סמכות אישור שמבצע בעצמו את העדכונים הנ"ל, אינו זקוק לאישור של עובד אחר כדי להשלים את הפעולה. דבר זה אינו עולה בקנה אחד עם כללי בידוק, כאשר בהיעדר הפרדת סמכויות התאפשרו חלק מהפעולות החריגות שנקט מנהל לשכת אילת בניצול סמכותו לרעה. הענקת "הרשאת מנהל" לבעלי תפקידים בלשכות רוקנה מתוכן את הבקרה ואת ההשקעה ליישומה.

הביקורת העלתה כי לא נקבע ברשות האוכלוסין גוף שעליו להפיק ולבדוק דוחות בקרה תקופתיים ודוחות משנים קודמות גם בעניין תושבים שלגביהם נרשמו תנועות כניסה מסוג "נוכח בלשכה" וגם בעניין תושבים שלגביהם נרשמו תנועות כניסה ידניות אחרות.

לדעת משרד מבקר המדינה, על רשות האוכלוסין לשקול לשלב את האישור הנוסף גם בפעולות רגישות אחרות כגון עדכוני דת, אזרחות ותאריך לידה.

איכות נתוני מרשם האוכלוסין

משרד מבקר המדינה בדק את איכות חלק מהנתונים שנמצאו במרשם האוכלוסין בחודש אוגוסט 2008. הקובץ הכיל כ-9.75 מיליון רשומות, ביניהן 7.97 מיליון רשומות (82%) פעילות. הביקורת העלתה את הליקויים האלה:

נמצאו כ-13,000 רשומות פעילות עם שם פרטי חסר. המשרד השיב כי מצב של שם פרטי חסר נוצר כאשר נולד ילד ולא ניתן לו שם בבית החולים, וההורים לא באו לרשום אותו אחר כך או חלילה כאשר הילד נפטר בסמוך ללידה.

לדעת משרד מבקר המדינה, מן הראוי שלאחר פרק זמן מסוים לאחר רישום ללא שם פרטי - שייקבע - תישלח להורי הילוד תזכורת על אי-רישום שמו ועל הצורך לעדכן את נתוני התושב בהתאם או לכל הפחות ייעשה בירור למציאת מקור התקלה.

משרד מבקר המדינה העלה שיבושים בנתונים המקשרים בין בני זוג. לכאורה, המעמד האישי של אחד מהם או של שניהם לא עודכן, כדלקמן:

מצב אישי שנרשם לתושב	סטטוס תיק התושב	מצב אישי שנרשם לבן הזוג	סטטוס תיק בן הזוג	ליקוי/ משמעות	מספר המקרים שנמצאו
נשוי/אה	פעיל	גרוש/ה	פעיל או נפטר	תושב נשוי-פעיל אמור להיות נשוי לבן זוג נשוי-פעיל.	725
נשוי/אה	פעיל	נשוי/אה	נפטר	תושב נשוי-פעיל אמור להיות נשוי לבן זוג נשוי-פעיל.	944
אלמן/נה	פעיל	אלמן/נה	פעיל או נפטר	מעמד בן הזוג של אלמן אמור להיות נפטר.	128
אלמן/נה	פעיל	גרוש/ה	פעיל או נפטר	מעמד בן הזוג של אלמן אמור להיות נפטר.	67
אלמן/נה	פעיל	נשוי/אה	פעיל	מעמד בן הזוג של אלמן אמור להיות נפטר.	120
רווקה	פעיל	גרוש או נשוי	פעיל או נפטר	מעמד הרווקה אמור היה להשתנות לנשואה או לגרושה.	2
פוליגם (אישה)	פעיל	כל מצב	פעיל או נפטר	אישה נשואה בו-זמנית לשני בני זוג.	1
נשואה לשני בני זוג	פעיל	נשוי	פעיל	אישה נשואה בו-זמנית לשני בני זוג.	117 (234 בני זוג)
כל מצב	פעיל	כל מצב	פעיל	מספר זהות בן הזוג אינו תקין.	1,182

הועלו כ-200,000 רשומות של אזרחים פעילים שנולדו בארץ בשנות ה-50, שחסרים בהן מספרי הזהות של האב והאם. הדבר מקשה על בדיקות ייחוס הנדרשות לקביעת זכאויות (כגון יורשים), התחייבויות או מגבלות התלויות בבני משפחה. עוד הועלו כמיליון רשומות של תושבים פעילים שבהן רשום תאריך עלייה ולא נרשם מאיזו ארץ עלו, וכ-65,000 רשומות של תושבים פעילים שבהן רשומה ארץ העלייה ולא נרשם תאריך העלייה. בכ-550 רשומות של עולים נמצא שתאריך העלייה קדם לתאריך הלידה.

בתשובתו למשרד מבקר המדינה ציין משרד הפנים שהשיבושים קדמו למערכת הממוחשבת הנוכחית, ומבצע לתיקון נתונים כה רבים מחייב החלטה ברמה אסטרטגית.

יודגש שבבדיקה חוזרת של הנתונים שעשה משרד מבקר המדינה, נמצא כי יותר מ-14,000 שיבושים (כ-1%) אירעו בתקופת המערכת הנוכחית. יש לציין כי רישום נתונים שגויים לגבי פרטים אישיים כגון שם, כתובת ומעמד עלול לגרום לעיכובים בטיפול בתושבים, לקביעת זכאות לא נכונה לסיוע ולאי-גביית חובות על ידי מגוון גופים ממשלתיים[15]. מן הראוי שרשות האוכלוסין תיערך לבדיקת אמינות הנתונים ולתיאום טיוב הנתונים השוטפים וההיסטוריים עם המשתמשים החיצוניים במאגר מרשם האוכלוסין; כן ראוי שתקבע אחראי להכנת נוהל שעניינו בקרת איכות לנתוני המרשם וביקורת שוטפת עליהם.

15 בעניין תשלומים לזכאים ראו דוח שנתי 56ב של מבקר המדינה (2006) בפרק "הבקרה על תשלומים לזכאים שנעשים בסיוע מערכות ממוחשבות", עמ' 153.

הגנת הפרטיות ואבטחת מידע במוסד לביטוח לאומי

המוסד לביטוח הלאומי (להלן - הביטוח הלאומי) משלם בכל חודש מאות אלפי קצבאות ותשלומים שונים למבוטחים. לצורך הניהול והתפעול של מערכת התשלומים והתמיכה בה משתמש הביטוח הלאומי במערכות מידע ייעודיות.

1. **הוועדה העליונה לאבטחת מידע בביטוח הלאומי:** בפרוטוקול הוועדה העליונה לאבטחת מידע מדצמבר 2006 נכתב, כי מטרתה לשמור על נכסי המידע של הביטוח הלאומי ולאפשר את פעולתו התקינה. כמו כן תפקידיה הם לטפל בהתוויית מדיניות ובהנחיות לאבטחת מידע; להתוות תכנית לפיקוח ובקרה על יישום המדיניות; להכין תכנית להטמעה והסברה של אבטחת המידע בביטוח הלאומי.

בדיון ועדת אבטחת מידע מיולי 2007 נסקרו האמצעים הטכנולוגיים שברשות הביטוח הלאומי. מנהל החטיבה לאבטחת מידע הציג את הפתרונות הטכנולוגיים שנרכשו, ובכללם תכנת "אינטלינקס" (ראו להלן) המקליטה מסכים באופן רציף כך שכל המידע המוקלט נשמר לאורך זמן, ויש לה עוד שני יתרונות בהפעלת מבחני קבלה ושחזור נתונים; מערכת לניהול זהויות משתמשים והרשאות. הפעלתה של תכנת ה"אינטלינקס" הייתה מתוכננת בספטמבר 2007.

הביקורת העלתה כי עד דצמבר 2008, מועד סיום הביקורת, תכנת ה"אינטלינקס" שפועלת בביטוח לאומי אינה נותנת תשובות לשאילתות על המידע ולכן לא סיפקה ליחידת ביקורת הפנימית את הכלים הדרושים לעבודתה.

2. **מימוש אחריות קב"ט הביטוח הלאומי בתחום אבטחת המידע:** בשנת 2003 הוסף הביטוח הלאומי לתוספת לחוק להסדרת הביטחון, ומכוח זה הוחלו עליו כללי שירות הביטחון הכללי (אבטחת מידע), התשס"ד-2004, אשר קובעים את האחריות ואת הסמכות של ממונה הביטחון לפעולות אבטחה. ב-2004 הוכן תיק מדיניות אבטחת מידע שהופץ למנכ"ל דאז, מר יגאל בן שלום, ולגורמים שונים בביטוח הלאומי. המנכ"ל אישר את התיק והוציא הנחייה שבה העניק לקב"ט את הסמכות ואת האחריות לאבטחת המידע.

במועד ביקורת המעקב, באוקטובר 2008 לא התקיים שיתוף פעולה בין הקב"ט למנהל החטיבה לאבטחת מידע. הקב"ט לא הוזמן לישיבות עבודה, לא שותף בפרויקטים של אבטחת מידע ולכן לא היה יכול לממש את סמכותו. נוסף על כך, לא בוצע השינוי הארגוני הנדרש בעקבות שינוי חוק הסדרת הביטחון, כללי שירות הביטחון הכללי וההנחיות שנקבעו בתיק מדיניות אבטחת המידע, נוכח אי-שיתוף הפעולה של הממונה על אבטחת המידע.

הביקורת העלתה כי כתוצאה מאי-שיתוף הפעולה בין הקב"ט למנהל החטיבה לאבטחת המידע לא אפשר מנהל החטיבה לקב"ט לבצע מבחני חדירות למערכת; הוא לא קיבל את רשימת שמות העובדים במוקד הטלפוני בצפת לצורך בדיקות סיווג ביטחוני (ראו להלן); הוא לא קיים פעולות הדרכה וימי עיון בענייני ביטחון מידע בביטוח הלאומי, כמתבקש.

חלוקת הסמכויות, קשרי העבודה וקשרי הגומלין בין קב"ט הביטוח הלאומי ויחידת אבטחת מידע עלו בחריפות בישיבה שנערכה בינואר 2007 בפרוטוקול הישיבה נכתב כי במצב ששרר באותה עת היו שני גופים: אגף הביטחון האחראי לאבטחה הפיזית, הכפופה למנכ"ל הביטוח הלאומי, והחטיבה לאבטחת מידע, האחראית לאבטחה הלוגית, הכפופה לסמנכ"ל תקשורת ומערכות מידע.

בחוות דעת של הקב"ט מינואר 2007 הוא ציין כי עליו לאשר כל שינוי בארכיטקטורה, בתפיסה ובמדיניות, כולל אבטחת המידע במחשבים הניידים שבארגון, ואילו החטיבה לאבטחת מידע אחראית ליישום ולביצוע. עוד הודיע כי פעולות שיבוצעו ללא אישור הקב"ט, בלי לדווח לו ובלי לתאם אתו ייחשבו עברת ביטחון. הוא פירט מספר פעולות שהוגדרו על ידו כפרצה אבטחתית: פתיחת תכנת ה-Outlook למחשבים ניידים; מתן אפשרות לעובדים להתחבר מהבית למחשבי הביטוח הלאומי; אי-ביצוע בדיקה ביטחונית ליועצים ולעובדים בחטיבה לאבטחת מידע; ביצוע פעולות במוקדים טלפוניים בלי עדכון אגף הביטחון. בסיכום המסמך טען הקב"ט, כי מצב אבטחת המידע בביטוח הלאומי בכי רע, קיימת פרצה אבטחתית ולהערכתו "האסון בוא יבוא".

בביטוח הלאומי קיים ליקוי מבני מתמשך בעניין אבטחת מידע. הוועדה העליונה לאבטחת מידע בראשות סמנכ"ל משאבי אנוש דאז התכנסה לראשונה בספטמבר 2006 ופעלה במשך כתשעה חודשים. הממונה על אבטחת מידע כפוף ישירות לסמנכ"ל תקשורת ומערכות מידע (תמ"מ), מתוקף תפקידו של הממונה על אבטחת מידע הוא נדרש לבקר חלק מפעילות מערכות המידע של הארגון שהן תחת סמכותו של סמנכ"ל תקשורת ומערכות מידע (תמ"מ), כפיפות זו פוגעת באי-תלותו. נוסף על כך, הוא אינו מקבל עליו את מרותו של הקב"ט בהתאם לכללי שירות הביטחון הכללי מ-2004. מן הראוי שהנהלת הביטוח הלאומי תגדיר מבנה יעיל לניהול אבטחת המידע במוסדה ותפעל באופן מיידי ליישומו.

בתשובתו מדצמבר 2008 הודיע הביטוח הלאומי כי שיתוף הפעולה בין הקב"ט למנהל החטיבה לאבטחת מידע הוסדר. סמנכ"ל תמ"מ הנחה את מנהל החטיבה לאבטחת מידע כי הקשר בין הביטוח הלאומי לרא"ם יקוים אך ורק באמצעות הקב"ט; הקב"ט יזומן לכל דיון במינהל תמ"מ הנוגע לנושאים שבתחום אחריותו. כמו כן מנכ"לית הביטוח הלאומי, הגב' אסתר דומיניסיני, קבעה כי הקב"ט ומנהל החטיבה לאבטחת מידע יפעלו בשיתוף פעולה ובהתייעצות בכל הנושאים הנוגעים לאבטחת מידע בביטוח לאומי.

מבירור שערך משרד מבקר המדינה עם הקב"ט בינואר 2009 עולה כי ההסדר שתואר בתשובת הביטוח הלאומי עדין לא יושם.

3. הגנת הפרטיות ואבטחת המידע טופלו בידי מבקר הפנים של הביטוח הלאומי במספר מקרים. בפרוטוקול ישיבה מנובמבר 2003 "בנושא כניסת עובדים לפרטי אנשים במערכת הממוכנת" צוינה "התופעה הרווחת בקרב עובדי הסניפים... נכנסים... לפרטים של אנשים כגון: מפורסמים, עובדי הביטוח הלאומי, קרובי משפחה ועוד... מסקרנות/רכילות/נקמנות ועוד... מדובר בעבירה פלילית לכל דבר". כמו כן הועלו הצעות למיגור התופעה שכללו יצירת קובץ אנשים מפורסמים; יצירת קובץ עובדי הביטוח הלאומי; יידוע העובדים כי כניסה לפרטי אנשים לא לשם עבודה היא עברה פלילית.

משרד מבקר המדינה העלה כי כבר בינואר 2007 רוכזו נושאים לביקורת אבטחת מידע במוסד על ידי האגף לביקורת פנים: קביעת מדיניות אבטחת המידע וסמכויות; מדיניות אבטחה כוללת; ניהול הרשאות. אלה הנושאים לבדיקה ברמת היישום: מתן הרשאות לפי צורכי העבודה; מעקב אחר פעולות וניטורן; מבחני חדירה תקופתיים למערכות; קליטת קבצים חדשים; פיקוח ובקרה על הגישה לבסיס הנתונים; אבטחה בסביבות הניסוי ובדיקת המערכת; פיקוח ובקרה על "קבצים שטוחים[16]"; זמינות של נאמן האבטחה ועובדיו לפתרון בעיות המתעוררות בסניפים ובמטה; ניהול יומן תקלות; ניהול מערך בקרה והתרעות בנושא אבטחה; פתיחת מספר מסופים באותה סמסה; העברת סמאות בין משתמשים; עקיפת ההרשאות באמצעות מסכים או מקשים פונקציונאליים.

---

16 קובץ שטוח - קובץ טקסט פשוט המכיל בדרך כלל נתון אחד בשורה או מספר נתונים המופרדים בסימן קבוע כגון פסיק. לדוגמה: שם פרטי, שם משפחה, כתובת, מספר טלפון וכו'.

לדעת משרד מבקר המדינה, יש לראות בחומרה שכבר בנובמבר 2003 התריעה מבקרת הפנים על המחדלים באבטחת המידע בפני הנהלת הביטוח הלאומי. עד דצמבר 2008 לא נעשו סקר סיכונים ומבחני חדירה על ידי חברה חיצונית, לא הוגדרה מדיניות אבטחת מידע ולא הוסדר המבנה הארגוני של אבטחת מידע בביטוח הלאומי על ידי ההנהלה.

מעקב אחר משתמשי-קצה בעזרת תכנת "אינטלינקס"

לתכנת "אינטלינקס" יכולת ניטור של פעילות לא מורשית או בלתי-חוקית במערכת ואפשר לקיים באמצעותה מעקב איכותי וכמותי אחר הפעילות העסקית של הארגון במערכת מחשב מרכזי (MainFrame).

ביוני 2005, בעקבות התחייבות הביטוח הלאומי בפני בג"ץ[17] לרשום את כל הפעילות של כל משתמשי התקשורת בביטוח הלאומי, הוקמה ועדה מקצועית לבחינת תכנות שבהן אפשר להשתמש כדי לקיים את ההתחייבות הזו. הוועדה מצאה כי ה"אינטלינקס" היא היחידה שנותנת מענה לדרישות ואף פנתה לחברת ייעוץ בעניין זה.

באוגוסט 2006 דיווח מנהל החטיבה לאבטחת מידע כי "הניסוי הסתיים בהצלחה רבה, המוצר הוכיח את עצמו בצורה מעוררת השתאות". באותו חודש שלח נציג חברת "אינטלינקס" למנהל חטיבת אבטחת מידע רשימה ובה פריטי החמרה הנדרשים עבור תכנה זו ובכלל זה גודלם של דיסקי האחסון הנדרשים לעבודה השוטפת. בנובמבר 2006 אישרה ועדת המכרזים לרכוש את התכנה ובדצמבר 2006 נחתם הסכם עם חברת "אינטלינקס" על רכישתה ב-250,000 דולר של ארה"ב. התכנה אמורה הייתה להתחיל לפעול החל בספטמבר 2007.

מעיון בפרוטוקול ישיבה שכנסה מבקרת הפנים בנושא תכנת ה"אינטלינקס" מיולי 2008 עולה, שמבקרת הביטוח הלאומי דיווחה "כי המערכת הקיימת אינה מספקת לביקורת את הכלים הדרושים בעבודתה". מנהל החטיבה לאבטחת מידע ציין, כי "בפועל, המערכת אינה מנתחת את הנתונים ואינה מציפה חריגים. הבעייתיות עיקרה במיעוט שטחי הדיסקים לאחסון".

ממסמך שהוציאה יחידת הביקורת הפנימית באוגוסט 2008 עולה, כי "מאז ועד היום לא התאפשר לעבוד מול התכנה. ביקשנו מספר 'שליפות' ובשני מקרים ספציפיים קיבלנו מידע אך מאז לא ניתן היה לקבל מידע נוסף... במטרה להגיע לפתרונות יזמנו דיון עם אנשי אבטחת מידע ומנהלת האגף האחראית. על פי תוצאות הדיון, גם כיום לא ניתן לקבל המידעים המבוקשים".

בהתייחסו להערת משרד מבקר המדינה השיב הביטוח הלאומי כי התכנה נרכשה בדצמבר 2006 והחל מינואר 2007 הוחל ביישום הפתרון כפי שהותווה על ידי המוסד בשיתוף היצרן. בינואר 2008 החלה התכנה לפעול במלוא ההיקף, אולם אז התברר כי העדר שטחי דיסקים פגע באפשרויות ניתוח ההקלטות שמבצעת תכנת ה"אינטלינקס" **אך לא בביצוע ההקלטות** (ההדגשה במקור).

אף שהיה ידוע למנהל החטיבה לאבטחת מידע כבר באוגוסט 2006 מהי החמרה הנדרשת לעבודתה התקינה של התכנה, הוא לא נערך בהתאם, דבר שעיכב את השימוש בה. כאמור העלתה הביקורת כי עד סיומה בנובמבר 2008 לא היה אפשר להציג שאילתות על המידע; לכן לא סיפקה התכנה ליחידת הביקורת הפנימית את הכלים הדרושים לעבודתה.

---

17 ראו הערת שוליים 5 לעיל, בג"ץ 8070/98.

הטיפול בעברות מידע בביטוח הלאומי

לצורך הרתעה והתראה מוקדמת מיד עם הכניסה למערכת המידע בביטוח הלאומי מוצגת אזהרה בכותרת אדומה בכל המחשבים בזו הלשון: "כל כניסה למערכת המידע תעשה לצרכי עבודה בלבד. כל שימוש אחר הוא בגדר עבירה פלילית שדינה מאסר! הפעילות הנעשית במסוף מוקלטת!", כך שעובדים לא יוכלו להלין כי לא ידעו שאסור להשתמש במידע שלא לצרכי עבודה.

מינואר 2005 טופלו בהליכי משמעת ובהליכים פליליים 13 עובדים שהיו חשודים בהוצאת מידע: שמונה טופלו על ידי נציבות שירות המדינה בעיקר בגין הוצאת מידע מהביטוח הלאומי; שניים הגיעו לטיפול של בית הדין למשמעת של עובדי המדינה; שלושה הועברו לחקירת משטרה, בעיקר בחשד למכירת מידע.

מבדיקת החשדות עלה כי הגישה למידע נעשתה מאינטרסים אישיים, מסקרנות ולעתים לצורך מסירת מידע לאחר. בחלק מהמקרים לא היה צורך לאותו עובד להציג את השאילתות שמהתשובות להן שלף את המידע. קבלת ההחלטה להעמיד עובד לדין משמעתי וההליכים בדין המשמעתי נמשכים לעתים זמן רב. לדוגמה, תיק שהועבר לנציבות שירות המדינה בסוף נובמבר 2005 הועבר לתביעה רק באפריל 2006, ועד נובמבר 2008 לא התקבלה ההחלטה בעניינו.

מאחד התיקים עולה חשד להוצאת מידע ולמכירתו על ידי עובד הביטוח הלאומי. העובד הושעה מתפקידו מאוקטובר 2004 ובעת סיום הביקורת עדיין התנהל נגדו הליך פלילי. מדוח אחר ממאי 2005 עולה כי התעורר חשד שהעובד טיפל בתיקים בניגוד לנוהלי הביטוח הלאומי ואף מכר מידע שאותו שלף מתשובה לאחת השאילתות במחשב. חקירת המשטרה העלתה כי העובד אכן מסר מידע לגורמים מחוץ לביטוח הלאומי. במאי 2005 הרשיעו בית המשפט וגזר עליו שמונה חודשי מאסר על תנאי למשך שלוש שנים, 200 שעות שירות לציבור ופיקוח שירות המבחן למשך שנה. בית הדין למשמעת של עובדי המדינה גזר על העובד באוגוסט 2006 נזיפה חמורה, פיטורים משירות המדינה החל מנובמבר 2006 ופסילה משירות המדינה לתקופה של שלוש שנים מיום גזר הדין. ביולי 2006 התעורר חשד שעובדת שנהגה לרשום פרטי אנשים השוהים בחו"ל מכרה מידע שהשיגה בתשובה לשאילתה שהיא מורשית לשאול. היא הועמדה לדין ובנובמבר 2007 גזר עליה בית המשפט 12 חודשי מאסר בפועל, 12 חודשי מאסר על תנאי, קנס של 10,000 ש"ח או שישה חודשי מאסר תמורתו. באפריל 2008 גזר בית הדין למשמעת של עובדי המדינה על העובדת פסילה משירות המדינה לתקופה של 15 שנים ונזיפה חמורה.

בספטמבר 2006 כתבה מבקרת הביטוח הלאומי למנכ"ל בעניין חקירת משטרה בגין חשד למכירת מידע, כי לנושא אבטחת המידע נדרשים היערכות נוספת ודגש רב יותר.

בספטמבר 2007 הודיע נציב שירות המדינה (להלן - הנציב) לעובדת הביטוח הלאומי על "העברה מתפקיד" עקב חקירה פלילית נגדה בחשד לביצוע עברות של מרמה והפרת אמונים והוצאת מסמך ממשמורת על-ידי עובד ציבור. במכתבו התייחס הנציב לטענתה כי "שליפת המידע נעשתה בתום לב ומתוך יצר סקרנות" באמרו "לעניין הקלון הטמון במעשים המיוחסים לך, הרי שעבירות של גילוי בהפרת חובה ופגיעה בפרטיות משתייכות לסוג העבירות אשר מטבען מבססות עבירה של מרמה והפרת אמונים של עובד ציבור, שהינה עבירת קלון מובהקת וזאת אף כאשר מדובר באירוע חד-פעמי". כמו כן ציין הנציב את הפסיקה המחמירה של בית המשפט העליון בנושא שליפת מידע ממאגרי מידע ממשלתיים והחליט על העברתה לתפקיד אחר שבו לא תהיה לה גישה למאגרי מידע עד תום ההליכים הפליליים או המשמעתיים שיינקטו נגדה.

לדעת משרד מבקר המדינה, כדי להגביר את המודעות של העובדים לצורך בשמירה על נוהלי העבודה בנושא אבטחת מידע ולשם מניעת הישנות של חריגות מהוראות הנהלים, ראוי שהביטוח הלאומי יפרסם במסגרת פנים ארגונית את העבירות שעברו עובדיו ואת אמצעי המשמעת שננקטו כלפיהם וכן יציג את נושא המשמעת בקביעות בפני הנהלתו.

מרכז המידע הטלפוני בביטוח הלאומי

בנובמבר 2006 נפתח מוקד לשרות הציבור בצפת. לצורך הגנת פרטיותם על הפונים למוקד הטלפוני להקיש קוד ורק לאחר מכן הם מופנים למוקדן לקבלת שירות. המוקדנים מקבלים את המידע על הפונה דרך מערכת מידע "דלפק קדמי" הכוללת בין היתר, פרטים לגבי חשבון הבנק, אחוזי הנכות ומעמדו האישי של הפונה. כמו כן המוקדנים נדרשים לחתום על התחייבות לשמירת סודיות ולעבור בדיקת התאמה אצל קב"ט הביטוח הלאומי. הם אינם יכולים להיכנס למחשב ללא "כרטיס חכם"[18] לצורך זיהוים, אך נמצא שהתחילו לעבוד במוקד קודם קבלת "כרטיס חכם" אישי על ידי שימוש "בכרטיס חכם" של עובד אחר, כך שלא היה אפשר לדעת מי הוא הנציג המטפל (ראו להלן).

משרד מבקר המדינה מעיר כי יש לראות בחומרה את העסקת המוקדנים ללא "כרטיס חכם" אישי שמאפשר את זיהוים, דבר המונע לחלוטין את יכולת המעקב אחר מוסרי המידע ומהווה פגיעה קשה באבטחת המידע של הארגון.

בדצמבר 2006 הודיע מנהל החטיבה לאבטחת מידע ללשכת היועץ המשפטי של הביטוח הלאומי כי מוקד צפת משמש את החברה החיצונית למתן שירותי טלפוני גם לחברות נוספות; ההפרדה בין המוקדים שהובטח שתוסדר עד סוף נובמבר 2006 אינה קיימת, והדבר "מהווה סיכון של פגיעה בפרטיות המבוטחים שלנו". עוד ציין כי אם לא יסיימו את הפרדת המוקדים באופן מוחלט, החל מינואר 2007 תיסגר לחלוטין התקשורת בין המוקד לבין הביטוח הלאומי.

בינואר 2007 הודיע מנהל החטיבה לאבטחת מידע למנכ"ל הביטוח הלאומי דאז, מר יגאל בן שלום, כי פעילות של הביטוח הלאומי במוקד צפת מתקיימת יחד עם פעילות של חברה פרטית וציין ש"קיים פוטנציאל רב מאוד לפגיעה בהגנה על הפרטיות של מבוטחינו... אין באפשרותי לתת פתרון לאבטחת המידע ולהגנה על פרטיות המבוטחים בהעדר פתרון חד משמעי של הפרדה מוחלטת של הפעילות החיצונית מפעילות הביטוח הלאומי באתר ויישום כל ההוראות שנקבעו בזמנו להפעלת האתר... למיטב דעתי המקצועית, בתצורה הנוכחית של המוקד הביטוח הלאומי רומס ברגל גסה את חוק הגנת הפרטיות ואת הפרטיות של מבוטחיו!".

ב-17.10.07 פנתה הוועדה לפניות הציבור של הכנסת למנכ"ל הביטוח הלאומי דאז, מר יגאל בן שלום, לקבלת תשובות בעניין המוקד הטלפוני של הביטוח הלאומי. ב-21.10.07 הביע מנהל החטיבה לאבטחת מידע את דעתו למנכ"ל, לבקשת הוועדה, וציין כי "הגדרתי את הדרישות הטכנולוגיות שיאפשרו את שמירת סודיות ופרטיות המבוטחים. הגדרות אלה כללו דרכי מניעה שיטוט חופשי של עובדים במידע. לצערי <u>אף לא אחת מההמלצות יושמה</u>!!!". (ההדגשה במקור)

ב-31.10.07 כתב מנהל החטיבה לאבטחת מידע למבקרת הפנימית מכתב בנושא "מוקד צפת" שבו צרף דוגמת תכתובת פנימית מאותו יום בין שתי עובדות במוקד צפת, שממנה עולה כי עובדת אחת מסרה את הסיסמה שלה לעובדת אחרת לצורך עבודה למשך יומיים והוסיפה "נא דאגי בדחיפות להסדיר מתן סיסמה למי מהעובדות במוקד בצפת על מנת שיפסק השימוש בסיסמה של... כמו כן נא דאגי להסדיר מתן סיסמאות לכניסה למערכת קשר". הממונה ציין גם כי עד אותו יום לא יושמו השינויים הטכנולוגיים בהרשאות העובדים במוקד צפת כדי שתימנע מהם האפשרות לחיטוט במידע והוסיף ש"במצב הקיים היום, אנו בבחינת פורעי חוק שכן כל המידע של הביטוח הלאומי מצוי בקצות אצבעותיהם של עובדי חברה פרטית... נוסף על כך, ציין כי מנהלי המוקד פועלים להספיק לקיים שיחות[19] רבות ככל האפשר, ולעתים - בניגוד להסכם ובניגוד להוראות של הביטוח הלאומי.

---

18 כרטיס המזהה לכאורה את המפעיל באופן פיזי וחד חד-ערכי במחשב שבו הוא עובד.

19 הדבר יגדיל את הכנסות החברה הפרטית.

בינואר 2008 כתבה המשנה ליועץ המשפטי של הביטוח הלאומי למחלקת הבג"צים בפרקליטות המדינה בהתייחסות לעתירה לבג"צ[20], כי "מיקור חוץ כאמור חייב התמודדות עם בעיות של אבטחת מידע, הן חמרה והן תכנה, וכך התעורר גם נושא הגישה למידע אישי על ידי עובדי הגוף המפעיל את המוקד, שאינם עובדי הביטוח הלאומי". היא הוסיפה ש"בשל הצורך הדחוף להפעיל מיד את המוקד בצפת, הזמן הרב שחלף מאז שהוכשרו נציגי השירות... לא ניתן היה לתת שירות זמין ומקצועי מיד עם ההפעלה... ובעיקר - הצעדים הטכנולוגיים שנועדו להגנה על סודיות המידע לא מומשו". בסיום מכתבה המליצה "גם מבחינת הצד המקצועי, ובעיקר בשל בעיות הבטחת מידע וההגנה על הפרטיות, ראוי ששירות מסירת המידע הטלפוני יבוצע על ידי עובדי הביטוח הלאומי. אם לא יעשה כך, יש צורך להסדיר את עניין מסירת המידע בדרך של תיקון חקיקה, ובשלב ביניים על ידי קבלת הסכמת הפונים, וכן יש להסדיר את עניין הזיהוי באמצעות כרטיס חכם, ולקבוע הסדרים להגבלת גישה למידע באמצעות הקשת מספרי זהות ללא פניה טלפונית, כמו גם הגבלת הגישה למערכות במקביל ממספר מחשבים".

הביטוח הלאומי השיב למשרד מבקר המדינה כי עם כניסתה לתפקיד של מנהלת המוקדים הטלפוניים החדשה בנובמבר 2008 ננקטו הפעולות שלהלן: היא הנחתה את המוקדים בצורה שאינה משתמעת לשתי פנים שחל איסור להעביר סמה מעובד לעובד; התקבלה רשימת השמות של עובדי המוקד בצפת וניתנו להם הרשאות מסודרות; נופו כל העובדים לשעבר במוקד צפת ובוטלו סיסמאות שהיו בתוקף גם לאחר שסיימו את עבודתם בחברה; כל העובדים בצפת עברו בדיקת קב"ט ובדיקת רישום פלילי; הופסקה עבודתם של עובדים שהיה להם רישום פלילי; "מזה כשנה" לפני פתיחת קורס חדש לנציגי שירות מועברת רשימת המשתתפים לקב"ט לאישורו, ולאחר מכן - לממונה אבטחת מידע לקבלת הרשאות; עם קליטתם של עובדי המוקדים בדימונה וברחובות כעובדי המוסד נבדקו גם הם בדיקות ביטחוניות.

משרד מבקר המדינה מעיר כי מאחר שבעבר נגנב מידע ונמכר לגורמי חוץ ואף היו ניסיונות של מתחזים להוצאת מידע ממאגרי הביטוח הלאומי, שיפור השירות ללקוחות אינו יכול לבוא על חשבון אבטחת המידע.

סיכום

עידן המידע מעמיד יכולות זמינות לרכז מידע, להעביר אותו במהירות ממקום למקום, להצליבו עם מידע אחר, לנתחו, למיין אותו ולהסיק מסקנות. מידע זה מצוי בידי גופים ציבוריים ופרטיים רבים, והם מחויבים בשמירתו. ללא מנגנוני אבטחה ובקרה מהותיים יש חשש ממשי לניצולו לרעה. עובדה זו מאיימת על הפרט בגלל האפשרות לחשוף בריש גלי את המידע האישי שנוגע לו. ואכן, בעטיים של מחדלים באופן השימוש במידע ובמאגרי מידע ובשמירה עליהם דלף בשנים האחרונות מידע אישי על תושבים ועל קבוצות אוכלוסיה שלמות - בניגוד לחוק הגנת הפרטיות.

---

20 בג"ץ 11193/07 "כן לזקן" נ' המוסד לביטוח לאומי ואח' - מרכז מידע טלפוני בצפת (חברת טלאול).

על מנת לשפר את המצב יש לנקוט את הצעדים האלה: (א) על רשות האוכלוסין להכין נוהלי אבטחת מידע, להקפיד על יישומם ולאייש את התפקידים הנחוצים למילוי דרישות חוק הגנת הפרטיות. (ב) במוסד לביטוח לאומי יש להפעיל ולנצל את כל המערכות לאבטחת מידע אשר הפעלתן תוכננה כבר ב-2007. (ג) יש לערוך סקר סיכונים, להגדיר מדיניות אבטחת מידע ולהסדיר את המבנה הארגוני הנחוץ לאבטחת מידע במוסד לביטוח לאומי בכלל, ואת שיתוף הפעולה בין הקב"ט למנהל החטיבה לאבטחת מידע בפרט. (ד) מן הראוי להגביר את המודעות של העובדים לחובת השמירה על נוהלי העבודה בעניין אבטחת מידע. לשם מניעת חריגות מההוראות והנהלים ראוי שיפורסמו במסגרת פנים ארגונית העברות שעברו העובדים ואמצעי המשמעת שננקטו כלפיהם, תוך שמירת פרטיותם, וראוי שנושא המשמעת יוצג בקביעות בהנהלות הארגונים.