

## **הרצאתה של השופטת ד"ר מיכל אגמון-גונן על מאגרי מידע בעידן המודרני**

**במסגרת יום עיון בנושא: ביג דאטה**

**המכללה למינהל 26.3.17**

**יותר מדי מידע נאסף על אזרחים: מתי יש להשתמש בו, מתי למחוק אותו ואיך להגן עליו ?**

ישנם המון מאגרי מידע המכילים מידע על כל אחת ואחד מאתנו. בעידן המודרני כמעט ואין אפשרות להימנע מכך. השאלה באיזה אופן יש לנהל את מאגרי המידע כדי לצמצם פגיעה אפשרית בכל אלו שפרטים לגביהם מצויים במאגרים. כיום, למרות צעדים חשובים בכיוון, עדיין אין תשובה אחת כוללת ומספקת. על כך בחרתי לדבר אתכם היום.

בעידן הדיגיטלי משאיר כל אדם שובל מידע דיגיטלי לעתים מבלי שהוא מודע לכך (פרופ' בירנהק טבע מונח זה בספרו "הזכות לפרטיות"). כל שימוש בכרטיס אשראי או כרטיס מועדון לקוחות מביא לשמירת מידע אודות מי שעשה בו שימוש, ופעמים רבות מבלי שיש ללקוח שליטה על כך, או אפשרות למנוע את העברת המידע. כך גם בעת שימוש בטלפונים סלולריים ובמכשירי ניווט דיגיטליים. לעידן הדיגיטלי יתרונות רבים, אך יש להיות ערים לכך שבהשארת אותו שובל מידע דיגיטלי, נמסר מידע הנכלל באותו מרחב אישי, שהאדם, לו היה עליו לבחור בכך, היה מעדיף שלא למסור. כלומר, במאגרי מידע נמצאים נתונים שבחרנו להעביר, בין באופן מכוון, ובין כתוצאה משימוש בתוכנות או אפליקציות.

לצד זאת קיימת אינפורמציה המגיעה למאגרי מידע שלא מהאדם עצמו. כך למשל נתונים המגיעים לבנקים ממרשם האוכלוסין, או מהרשות לאכיפה ולגבייה. עסקתי בנושא במסגרת פסק דיני בעניין אי.די.איי חברה לביטוח (עת"מ 11-02-24867).

האפשרות לאסוף מידע, עלתה בניסוי שנעשה בעקבות התבטאות של השופט סקאליה המנוח, שבהרצאה במכון האמריקאי למשפט ולימודי תלמוד אמר:

**"פרטיות באינטרנט זה לא דבר כל כך חשוב. הטענה שצריך להגן על כל רסיס של מידע אישי היא מטופשת. יש מידע מסוים שצריך להיות מוגן. אבל כל עוד אני אזרח שומר חוק, אין סיבה שארצה לשמור על הפרטיות של מידע טריוויאלי, כמו כתובתי או הרגלי הקניות שלי בסופרמרקט."**

פרופ' ג'ואל ריינדברג, מרצה למשפטים באוניברסיטת פורדהם בניו יורק ומומחה לפרטיות, הרים את הכפפה שזרק סקאליה. הוא הטיל על תלמידיו, במסגרת סמינריון בנושא משפט וטכנולוגיה, משימה: לאסוף כל פיסת מידע אישי שהם מוצאים אודות השופט במקורות גלויים באינטרנט. בניגוד לחברות ענק של מאגרי מידע אישי, כמו אקסיום (Acxiom) וצ'ויספוינט

(Choicepoint), התלמידים לא הורשו לגשת למקורות מידע שאינם חשופים לציבור. בניגוד לרשויות ביטחון כמו ה-FBI וה-NSA ומקבילותיהן בישראל, התלמידים לא צוידו בכלים רבי עוצמה של ציתות, ניטור וכריית מידע.

למרות האמצעים הדלים, הפיקו התלמידים דו"ח בן 15 עמודים, עשיר בפרטים אישיים אודות השופט. בכנס בנושא הגנת הפרטיות שנערך בפורדהם, חשף רייזנברג את קיומו (אך לא את תוכנו) של הדו"ח, שכולל מידע כגון כתובת ביתו של סקאליה, מספר הטלפון שלו, העדפותיו הקולניריות והקולנועיות, שווי ביתו, כתובת המייל של אשתו ותמונות של נכדיו מפייסבוק.

**השופט סקאליה הגיב בזעם על הגילויים ואמר "התרגיל של פרופ' רייזנברג אולי לא מפר חוק, אבל מהווה דוגמה לשיקול דעת עלוב ולקוי". רייזנברג לא נעלב, אלא כתב בתגובה: "התרגיל מוכיח, כי גם מי שחושב שאין לו מה להסתיר עשוי להיות מופתע מהיקף המידע אודותיו ברשת".**

ואכן, המידע רב, ואגור במאגרי מידע רבים ושונים. ככלל, ככל שנעשה שימוש במידע שנמסר למטרה לשמה הוא נמסר, השימוש מותר. הבעיה מתעוררת כאשר נעשה במידע שימוש אחר, והיא מתעצמת כי לעתים איננו יודעים כלל כי קיים לגבינו מידע מסוים.

רשויות השלטון וגופים פרטיים מקימים מאגרי מידע לצרכים שונים. בעידן הדיגיטלי, בו לרבות מפעילויות היום יום יש את אותן שובל מידע דיגיטלי, מידע רב נכלל במאגרים מסוג זה. במקרים רבים, אין לאדם ברירה אלא לספק את אותו מידע אם ברצונו לקבל מוצר או שירות, בין פרטי, בין ציבורי. פעמים אחרות הוא אינו כלל המקור למידע זה.

שימוש באותו מידע שלא למטרה לשמה הוא נמסר, מהווה פגיעה בפרטיות. הסדרת מאגרי מידע ככלל מוסדרת בחוק הגנת הפרטיות ומחייבת לרשום מאגרי מידע בתנאים מסוימים. בנוסף קיים חוק בעניין המאגר הביומטרי, והוראות ספציפיות לגבי בנקים, חברות ביטוח, הלבנת הון, רשומות רפואיות, מידע גנטי ועוד. יש להדגיש כי חוק הגנת הפרטיות אינו מחייב רישום מאגר שהמידע בו נמסר ע"י האנשים עצמם.

סעיף 8 לחוק הגנת הפרטיות קובע כי בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

- (1) מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;
- (2) יש במאגר מידע רגיש;

- (3) המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמים או בהסכמתם למאגר זה ;
- (4) המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23 ;
- (5) המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג.

לכאורה, הרבה מהדוגמאות כמו ויז או פנגו, מדובר במידע שאנו מסרנו את הסכמנו למסירתו, ומאגרים אלו אינם מפוקחים. בעבר, כשנקבעה הוראה זו המאגרים היו כאלה שהפרטים נמסרים ע"י הלקוח, תוך שהוא מודע למסירתם. כיום, כאשר עצם השימוש ביישומים שונים מביא לאגירת מידע, יתכן כי יש לשקול שנית שאלה זו.

לא אפרט בשאלה מהי פרטיות כיוון שההרצאה הבאה עוסקת בכך. עם זאת, בהנחה שמדובר במידע פרטי, כזה שלא היינו רוצים שיעשה בו שימוש, לבד מהמטרה לשמה מסרנו את אותו מידע, הרי שמאגרי מידע בעצם קיומם מסכנים את הפרטיות. הכמות הופכת בעניין זה לאיכות. היינו, כמות המידע האגור במאגרי המידע השונים, והעובדה שמדובר במידע דיגיטלי הופכים את הסכנה לשימוש לרעה במידע, שימוש שאינו למטרה לשמה נועד ומכאן לפגיעה בפרטיות לחמורה יותר.

הסכנה במאגרי המידע קיימת מעצם מסירת המידע, ומחריפה בשל אפשרות לקיומן של טעויות או ניצול לרעה של הגישה למידע. מאגרי המידע טומנים בחובם את החשש שהמדינה, גופים כלכליים ומסחריים ואפילו הסביבה החברתית יתייחסו לבני אדם על פי פרט בודד או לפי אפיון שלאדם כמעט אין שליטה עליו. כך, כשמישהו מאופיין בדרך מסוימת, כמו למשל כמי שאינו מחזיר חובות, או מי שמסתבך בעסקיו, גם אם אפיון זה מקורו, למשל, בטעות של הבנק, או בהחזרת שיק טכנית, הדבר עלול לפגוע בנו. בעיקר כאשר המידע נצבר ונשמר ומתקבלות החלטות על סמך המידע הזה שמשפיעות על זכויות וחובות שלנו. יש לזכור, כי מאגרי המידע אינם חסינים מפני פריצות מבחוץ, וודאי שאינם חסינים לשימוש לרעה ע"י מי שמורשה לראות את המידע.

בעש"ס 6843/01 בן דוד נ' נציב שירות המדינה, פ"ד נ"ו (2002) 918 (2) נדון עניינו של מפקח בכיר באגף מס הכנסה שהורשע בשימוש במאגרי המידע באגף לסיפוק סקרנותו. הנשיאה ביניש התייחסה לסכנה לפרטיות במאגרי המידע) בעמ 923 'לפסק הדין):

**"ההישגים הטכנולוגיים של העידן המודרני הביאו עימם כתוצאת לוואי אפשרויות נרחבות לפגיעה בפרטיות...חזונו האפוקליפטי של ג'ורג' אורוול בדבר " האח הגדול "עלול על נקלה להפוך למציאות חיים אם לא יישומו הגבולות לנגישות למאגרים ולשימוש בהם מעבר למטרה המוגבלת שלשמה ניתנה הסמכות למופקדים על מאגר המידע."**

למעשה, מאגרי המידע מתרבים ועמם האפשרות להצליב מידע ולאסוף מידע מתרחבות מאד, והדבר עלול להביא לפגיעה מעשית באדם. כבוד האדם, פרטיותו, ובעיקר האוטונומיה שלו, ויכולתו לשלוט בחייו, מחייבים שליטה שלה או שלו במידע האגור לגביהם. כלומר, יש לוודא, כי במידע ייעשה שימוש אך ורק למטרה לשמה הוא נמסר, ובנוסף, צריכה להיות שקיפות מקסימלית. היינו, יש לאפשר לכל אדם לדעת איזה מידע כלול לגביו במאגרי מידע שונים. יש לדאוג כי מאגרי המידע הדיגיטליים לא יביאו לאבדן הפרטיות, כבוד האדם והאוטונומיה.

בסביבה דיגיטלית, כל פריט מידע ניתן לשמירה ועיבוד בקלות יחסית. כמות המידע הנאגר והאפשרויות לגזור ממנו מסקנות עצומים בהיקפם. הגברת היכולות הטכנולוגיות לחיפוש מידע, לצד מידע הנאגר מעצם שימוש בתוכנות יומיומיות כמו ויז או פנגו, מביאים לכך שנאגר מידע אינסופי לגבי כל אחת ואחד מאתנו. הדבר מאפשר בקלות יחסית, לחפש ולדלות מידע, דבר המסכן את הפרט.

לאור ריבוי המידע, וריבוי מאגרי המידע, התפתח בעשורים האחרונים משטר משפטי של הגנת מידע בכלל ומאגרי מידע בפרט, המסדיר את השימוש במידע הנאגר. כפי שצינתי אצלנו ההוראות הכלליות נמצאות בחוק הגנת הפרטיות ואחרות בחוקים ספציפיים. חלק מההסדרה נוגעת לשימוש במידע הנאגר. הנחת היסוד היא כי למאגרי מידע ישנם יתרונות רבים, ולמעשה, כפי שצינתי, כיום כמעט לא ניתן לנהל חיים מסודרים, מבלי שייאגר מידע לגבי כל אחת ואחד מאיתנו. לאור זאת, ההגנה על האוטונומיה, כבוד האדם, הפרטיות, מחייבים הגנה על המידע; בחינת דיוק, עדכון ורלבנטיות המידע; והתחייבות ואכיפתה כי ייעשה שימוש במידע רק למטרה לשמה נמסר.

אני סבורה כי לאור השינויים המהותיים בהיקפי המידע הנמסר, בין אם במודע, בין אם לאו הם כאלו, המחייבים הסדרה פרטנית יותר, והגברת סמכויות ותקציב האכיפה. פעילות זו מרוכזת כבר היום ברשות למשפט, טכנולוגיה ומידע במשרד המשפטים (שהוקמה בשנת 2006). תחומי האחריות של הרשות נקבעו בחוקים שונים והם כוללים, בין היתר:

- פיקוח על בעלי מאגרי מידע ובעלי רישיונות, כולל סמכויות חיפוש ותפיסה.
- טיפול בתלונות.
- חקירת עבירות פליליות.
- הטלת קנסות מינהליים.
- רישום מאגרי מידע ומתן רישיונות לשירותי נתוני אשראי, שירותי מידע על עוסקים ולגורמים מאשרים.
- קביעת הנחיות שוק שיספקו לבעלי מאגרי מידע ובעלי רישיונות סטנדרט פעולה מקובל.
- העלאת מודעות הציבור לזכות לפרטיות במידע, הן בקרב בעלי מאגרי המידע והן בקרב נושאי המידע.

כיוון שלרשות יש את המומחיות ייתכן כי הגיעה השעה לשקול חקיקת חוק מאגרי מידע, שהממונה עליו תהיה הרשות, והוא יכלול הוראות שונות, בנושאים המצויים בטיפול כבד היום, ובנושאים נוספים, תוך התייחסות לאתגרים החדשים בתחום זה. חוק המאגר ביומטרי קבע הקמת רשות חדשה עם ראש רשות חדש. בין שאר תפקידי הרשות הוא לדאוג לבטיחות מאגר המידע, אפשרויות שימוש בנתונים וכיו"ב. יתכן כי יש מקום להקים רשות עצמאית, אולם אני סבורה כי את נושאי הרוחב לעניין מאגרי המידע יש לרכז במקום אחד שיצבור מומחיות לעניין זה. כיון שההתפתחות הטכנולוגית היא מהירה, יש לקבוע בחוק עקרונות על, ולהשאיר עניינים רבים ככל האפשר לתקנות, ואף לנהלים של הרשות. כך למשל, בחודש שעבר פורסמה הנחייה חדשה של רמו"ט, המחייבת גופים שונים לאפשר לציבור גישה למידע אישי דיגיטלי – כתוב, מוקלט או מצולם. על פי ההנחיה, כל גורם השומר מידע כזה, בין אם מטעמים הקבועים בחוק, ובין אם למטרות מסחריות שונות, מחויב לאפשר לכל אדם גישה למידע האישי אודותיו, באופן מהיר ונוח.

העקרונות עליהם יש לעמוד הם בראש ובראשונה צמצום מאגרי המידע למינימום הנדרש, שכן ההנחה היא שאין מאגר מידע חסין (לעניין זה ראו הוויכוח שהיה לאחרונה, והוכרע בימים אלו לגבי תעודות זהות ודרכונים חכמים). היינו, יש לצמצם ככל הניתן את המידע הנשמר במאגרים. יש לבחון את היתרונות במאגר מידע ואת המחיר אם המידע ידלוף. כך, למשל, וויז זוכרת נסיעות, ויכולה לשאול אותך בבוקר האם את נוסעת לעבודה. האם שווה לשמור זאת במאגר, שאם יפרץ יזוהו התנועות הקבועות של מיליוני משתמשים, ככולל מקומות אחרונים אליהם נסע. ומדובר במיליוני משתמשים, או שעדיף לוותר ולבחור בכל בוקר מרשימת המועדפים "עבודה". איני מביעה עמדה בשאלה זו לגופה. בהחלט ישנם נימוקים טובים להסדיר זאת במישור הפרטי תוך הגברת המודעות. להשאיר בידי הפרט את הבחירה באילו יישומים להשתמש ומה המחיר בשימוש זה מבחינת אפשרויות כריית המידע על ידי גורמים אחרים. אולם אלו שאלות שצריכות להעסיק את הרשויות. האם אין מקום לקבוע חובת רישום ופיקוח על מאגרי מידע דוגמת וויז? האם מדובר בכלל במאגר מידע? אם כן, מה הם הפרטים שיש מקום לשמור במאגר כאמור. כך צריך לעשות לגבי כל פריט מידע ולהשתדל שישמר כמה שפחות מידע, אם אין בשמירתו יתרונות. ההפך נכון, ברשומה רפואית, שם יש חשיבות רבה לכל הפרטים, אך הכלל צריך להיות מינימום המידע הנדרש למטרה לשמה הוא נאגר.

העקרון השני הוא כי על המידע שנאגר יש לשמור. אשר להגנה על המידע, טובי המוחות עסוקים בשאלות אלו בכל העולם. ועדת החוקה, חוק ומשפט של הכנסת החלה ביום שלישי (10.1.2017) לדון בתקנות להגנה על מאגרי מידע שהגישה שרת המשפטים איילת שקד

התקנות נועדו לקבוע הסדר מעודכן, מקיף ומפורט יותר מזה הקיים כיום בתקנות הגנת הפרטיות, לעניין ההגנה הפיזית והלוגית על מאגרי מידע ולעניין סדרי הניהול וכללי העבודה בקשר למאגרי מידע של גופים ציבוריים ופרטיים. על פי האמור:

"ההסדר כולל מנגנונים וכלים פנים ארגוניים הממחישים את חובותיהם ואחריותם של ארגונים בתחום אבטחת מידע אישי ומטרתם להנחיל עקרונות אבטחת מידע כדי להגן על זכויות נושאי המידע במאגרים מפני שימוש לרעה על-ידי גורמים מחוץ לארגון והן על-ידי עובדי הארגון. בהיבט האחריות הארגונית, התקנות מודולריות ומחילות חובות ברמה הולכת וגדלה ככל שפעילות עיבוד המידע בארגון משמעותית יותר."

בשל המגוון הרחב של גופים שמעבדים מידע במסגרת מאגרי מידע, התקנות המוצעות מבחינות בין ארבעה סוגי מאגרים: מאגר ברמת אבטחה גבוהה; מאגר ברמת אבטחה בינונית; מאגר ברמת אבטחה בסיסית; מאגר המנוהל בידי יחיד. את רמת הרגישות של המאגרים מוצע לקבוע בהתאם לשילוב של מספר פרמטרים: היקף מורשי הגישה למידע שבמאגר, כמות האנשים שאודותיהם יש מידע במאגר וסוג המידע המעובד במאגר. ההנחה היא שנוסף על רגישות המידע, גם היקף החשיפה של המידע למספר רב יותר של מורשי גישה, כמו גם היקף רחב יותר של אנשים שאודותיהם יש מידע במאגר, מגבירים את סיכוני אבטחת המידע שהמאגר מעורר, ועל כן מוצדק לדרוש מהמאגר רמת אבטחה גבוהה יותר. לפיכך, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה ככל שהמאגר הוא מאגר שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותית יותר ורמת האבטחה הנדרשת בו היא גבוהה יותר.

אני סבורה כי התקנת תקנות כאמור בהחלט תקדם את ההגנה על המאגרים הדיגיטליים, אך יש לשקול אם לא נדרשת גם חקיקה שתחיל תקנות אלו על מאגרים רבים יותר.

אשר לשני התנאים האחרים: עדכון ורלבנטיות המידע, ושימוש בו למטרה לשמה הוא נמסר, אני רוצה להדגים זאת באמצעות חוק נתוני אשראי. הנושא המרכזי של חוק זה הוא מתן רשות לשירות נתוני האשראי לאסוף ולמסור נתוני אשראי על יחידים בנוגע להיסטוריית האשראי שלהם. מידע שממנו ניתן להסיק על אמינות העמידה שלהם בהתחייבויותיהם הכספיות. המידע השלילי נאסף ונמסר מבלי שאותם יחידים נתנו את הסכמתם לכך. אין ספק, כי מסירת מידע על עמידתו של היחיד בהתחייבויותיו הכספיות, ובמיוחד מידע על אי עמידתו בהתחייבויותיו, ללא הסכמתו, מעוררת בעיות בתחום הגנת הפרטיות. מול הפגיעה בפרטיות הלקוח עומדת זכותו של הנושא והאינטרס הציבורי בכלל, לפיו יוכל נתן אשראי לסמוך על כך שהוא פועל במשטר בו לקוחות עומדים בהתחייבויות שלקחו על עצמם, אחרת לא יינתן אשראי, או שמחירו יעלה מאד.

על מנת להבטיח פגיעה מינימלית בלקוחות, מקבלי האשראי ובזכויותיהם, קובע חוק נתוני אשראי כמה מנגנונים שנועדו להבטיח את מהימנות המידע, הן במובן זה שהמידע יהיה אמין ושמקורו אינו בטעות או בתקלה, והן במובן זה שאכן יהא בו כדי להצביע על המסקנה שמבקשים להסיק מאותו מידע בדבר עמידתו של פלוני בהתחייבויותיו הכספיות. כך, למשל, קובע החוק, בסעיף 22, מגבלה של פרק זמן לגבי שמירת המידע. החוק אף קובע, בסעיף 29ג, חובת מסירת הודעה ללקוח על קבלת החלטה לגביו בהתבסס על דו"ח אשראי, והוא מסדיר מנגנון לתיקון או מחיקה של מידע שגוי. החוק מתיר לכלול בדו"ח אשראי נתונים בדבר אי תשלום חובות המבוססים, בין היתר, על נתונים מלשכת ההוצאה לפועל. ואולם, מסירת דו"ח כאמור מותנית בכך שהדו"ח יכול גם נתונים חיוביים מתאגיד בנקאי לגבי אותו לקוח. בנוסף, דו"ח אשראי יכול לכלול נתונים בדבר אי תשלום חובות, רק אם נפתחו כנגד פלוני לפחות שלושה תיקי פסק דין או לפחות חמישה תיקי שטרות.

איזון דומה מצוי בחוק המרשם הפלילי. חוק המרשם הפלילי מבחין בין שני סוגים של מאגרי מידע: האחד מיועד למי שהורשעו בדין או שניתנה לגביהם החלטה שיפוטית אחרת (סעיף 1א) לחוק המרשם הפלילי); והשני מיועד ל-"רישומים אחרים" הדרושים למטרה לצרכי עבודתה (סעיף 1ג) לחוק המרשם הפלילי) – ובכלל זה תיקי חקירה שנסגרו (ראו: סעיף 11א). ההנחה היא שמידע בדבר תיקי חקירה שנסגרו מחוסר בראיות עשוי לשמש את המשטרה בעתיד, בחקירות אחרות נגד אותו אדם ואף נגד אחרים. אמנם לפי סעיף 3 לחוק המרשם הפלילי, המרשם הוא חסוי – ואולם סעיף 11א לחוק מאפשר למסור מידע בדבר החלטה על סגירת תיק חקירה לשורה ארוכה של גורמים. בין היתר כוללת רשימה זו את היועץ המשפטי לממשלה, תובע משטרה ופרקליט משטרה, השב"כ, גורמים שונים בצה"ל, קציני מבחן וקציני פיקוח, נציבות בתי הסוהר, ועדת שחרורים לפי חוק שחרור על תנאי ממאסר, התשס"א-2001, וכיוצא באלה. יתירה מזאת, נוהג מקובל בשוק העבודה הוא להציב כתנאי לקבלה למקום עבודה אישור על היעדר רישום פלילי – ובליט ברירה מועמדים רבים מאפשרים למעסיקים פוטנציאליים לעיין במרשם הפלילי בעניינם. מטבע הדברים, מסירת מידע בגין סגירת תיק מחמת חוסר בראיות מספיקות, באופן המותיר ספק לגבי חפותו של אדם, עלולה להכתימו כמי שמעורב בפלילים ולהסב פגיעה קשה לשמו הטוב ולפרנסתו.

כאן מתעוררת שאלה מעניינת. החוק קובע כי מי שהתיק נגדו נסגר בהעדר ראיות יישאר במרשם לטובת רשויות החקירה. ואולם, כפי שציינתי, מקומות עבודה רבים דורשים להמציא להם את אותו מידע, שהפרט, על פי החוק זכאי לקבלו. היינו, מרגע שקיים מאגר מידע, לעתים לא די לקבוע שיש להשתמש בו למטרה מסוימת, אלא ייתכן שיש לקבוע איסור על אחרים לבחון את אותו מידע. כך, לגבי מקום עבודה פוטנציאלי, בהחלט ייתכן כי חומר כזה אינו רלבנטי, כי המקורות לחשד אינם מהימנים, ומעסיק פוטנציאלי אינו יודע לבחון זאת. די כי במסגרת סכסוך

עסקי או משפחתי יגיש מאן דהוא תלונה על חברו וזו תישאר במאגר המידע, ותפגע בו בצמתים שונים בחייו. כלומר, גם כשהחוק קובע כי ייעשה שימוש במידע למטרה מסוימת, יש לשקול לקבוע איסור לגורמים אחרים, כגון מעסיקים פוטנציאליים לבקש את המידע. ככל שהמידע רגיש יותר, הוראה מעין זו חשובה יותר.

[ברע"פ 8464/14 מדינת ישראל נ' ניר עזרא \(פורסם בנבו, 15.12.2015\)](#)  
השאירו בצריך עיון האם ניתן להרשיע בעבירה פלילית על חוק המחשבים, מי שנכנס למחשב כדין, אך עשה שימוש שלא כדין במידע.

אני מאמינה שצריך להסתכל על חצי הכוס המלאה. על היתרונות שבטכנולוגיה, המביאים עמם את אותו שובל מידע דיגיטלי, את המידע הרב במאגרי המידע. על כן יש לדאוג לרכז את החקיקה והאכיפה בנושאים אלו ככל שניתן, ולקבוע עקרונות בכמה מישורים:

ראשית, יש לוודא כי תישמר כמות המידע המינימלית הנדרשת, היינו, כי כל ידע שאין צורך להחזיק בו לאורך זמן אכן יימחק;

שנית, יש להגן באופן רציני על מאגרי מידע, לחייב בכך כל מי שמחזיק מאגר מידע ולהקצות משאבים לאכוף זאת.

שלישית, יש לדאוג כי מי שמחזיק מאגר מידע יכלול בו רק מידע נכון רלבנטי ומעודכן, ויעדכן את מי שיש לגביו מידע במאגר בעניין זה, תוך אפשרות לפנות ולתקן מידע זה. ככל שמדובר במאגרים של רשויות הביטחון יש צורך בהסדרה מיוחדת.

ולבסוף, יש לדאוג כי יעשה במידע שימוש רק למטרה לשמה הוא נמסר. שימושים אחרים יש לאסור ולהטיל סנקציות חריפות בין אזרחיות (תביעות אזרחיות אישיות או ייצוגיות), בין מנהליות ואף פליליות במקרים המתאימים. דוגמא עדכנית לכך ניתן לראות בחוק המאגר הביומטרי. אני סבורה כי יש לקבוע הוראות דומות אחידות לגבי כלל מאגרי המידע.